



Guida per l'utente

AWS Security Hub



AWS Security Hub: Guida per l'utente

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

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

Table of Contents

Che cos'è AWS Security Hub?	1
Vantaggi del Security Hub	2
Accesso al Security Hub	2
Servizi correlati	4
Versione di prova gratuita, utilizzo e prezzi di Security Hub	4
Visualizzazione dei dettagli di utilizzo e dei costi stimati	4
Dettagli prezzi	5
Concetti di Security Hub	6
Consigli prima di abilitare Security Hub	13
Integrazione con AWS Organizations	13
Utilizzo della configurazione centrale	13
Configurazione AWS Config	14
Abilitazione AWS Config	15
Attivazione della registrazione delle risorse in AWS Config	15
Abilitazione del Security Hub	18
Verifica delle autorizzazioni necessarie	18
Abilitare l'integrazione di Security Hub with Organizations	18
Abilitazione manuale di Security Hub	20
Script di abilitazione per più account	21
Passaggi successivi dopo aver abilitato Security Hub	22
Configurazione centrale	23
Vantaggi della configurazione centralizzata	24
Chi dovrebbe usare la configurazione centrale?	25
Termini e concetti relativi alla configurazione centrale	25
Inizia a usare la configurazione centrale	31
Prerequisiti per la configurazione centrale	31
Avvia la configurazione centralizzata	33
Scelta del tipo di gestione	36
Specificazione delle impostazioni per gli account autogestiti	37
Scelta del tipo di gestione degli account e delle unità organizzative	38
Come funzionano le politiche di configurazione	40
Considerazioni politiche	40
Tipi di politiche di configurazione	41
Associazione delle politiche tramite applicazione ed ereditarietà	43

Test di una politica di configurazione	45
Creazione e associazione di politiche di configurazione	46
Visualizzazione delle politiche di configurazione	52
Stato di associazione di una configurazione	55
Le cause più comuni del fallimento dell'associazione	56
Aggiornamento delle politiche di configurazione	57
Eliminazione e dissociazione delle politiche di configurazione	62
Eliminazione delle politiche di configurazione	62
Dissociazione di una configurazione dagli account e dalle unità organizzative	64
Configurazione contestuale	66
Configurazione di uno standard di sicurezza nel contesto	66
Configurazione di un controllo di sicurezza nel contesto	67
Smetti di usare la configurazione centrale	67
Gestione degli account degli amministratori e dei membri	71
Gestione degli account con AWS Organizations	71
Gestione manuale degli account tramite invito	72
Gestione degli account con AWS Organizations	73
Integrazione del Security Hub con AWS Organizations	74
Attivazione automatica del Security Hub nei nuovi account	81
Abilitazione manuale di Security Hub in nuovi account	83
Dissociazione degli account dei membri dell'organizzazione	85
Disabilitazione dell'integrazione con AWS Organizations	87
Gestione degli account tramite invito	89
Aggiungere e invitare account membri	90
Rispondere a un invito	94
Dissociazione degli account dei membri	96
Eliminazione degli account dei membri	98
Dissociarsi dal proprio account amministratore	99
Transizione a AWS Organizations	100
Azioni consentite per gli account	102
Restrizioni e raccomandazioni	109
Numero massimo di account membri	109
Account e Regioni	109
Restrizioni alle relazioni amministratore-membro	110
Coordinamento degli account degli amministratori tra i vari servizi	110
Effetto delle azioni dell'account sui dati del Security Hub	111

Security Hub disattivato	111
Account membro dissociato dall'account amministratore	111
L'account membro viene rimosso da un'organizzazione	112
L'account è sospeso	112
L'account è chiuso	112
Aggregazione tra regioni	114
Come funziona l'aggregazione tra regioni	115
Aggregazione per account amministrativi e membri	116
Configurazione centrale e aggregazione tra regioni	117
Abilitazione dell'aggregazione tra regioni	118
Abilitazione dell'aggregazione tra regioni (console)	119
Abilitazione dell'aggregazione tra regioni (API Security Hub,) AWS CLI	119
Visualizzazione delle impostazioni di aggregazione tra regioni	120
Visualizzazione della configurazione di aggregazione tra regioni (console)	120
Visualizzazione dell'attuale configurazione di aggregazione tra regioni (API Security Hub,) AWS CLI	121
Aggiornamento della configurazione	121
Aggiornamento della configurazione di aggregazione tra regioni (console)	122
Aggiornamento della configurazione di aggregazione tra regioni (API Security Hub,) AWS CLI	122
Interruzione dell'aggregazione tra regioni	124
Interruzione dell'aggregazione tra regioni (console)	124
Interruzione dell'aggregazione tra regioni (API Security Hub,) AWS CLI	124
Risultati	126
Creazione e aggiornamento dei risultati	127
Uso di BatchImportFindings	128
Uso di BatchUpdateFindings	132
Gestione e revisione dei dettagli e della cronologia dei risultati	137
Filtraggio e raggruppamento dei risultati (console)	138
Informazioni di ricerca disponibili	141
Revisione della cronologia dei risultati	142
Esame dei dettagli del ritrovamento	144
Intervenire in base ai risultati	146
Impostazione dello stato dei risultati del flusso di lavoro	146
Invio dei risultati a un'operazione personalizzata	149
Formato dei risultati	150

Sintassi ASFF	150
ASFF e consolidamento	230
Esempi ASFF	291
Informazioni dettagliate	441
Visualizzazione e filtraggio dell'elenco di approfondimenti	441
Visualizzazione dei risultati e dei risultati di informazione dettagliata	442
Visualizzazione e azione dei risultati delle analisi (console)	442
Visualizzazione dei risultati delle analisi (API Security Hub, AWS CLI)	443
Visualizzazione dei risultati per un risultato approfondito (console)	444
Informazioni dettagliate gestite	445
Informazioni personalizzate	455
Creazione di informazioni personalizzate (console)	456
Creazione di un'analisi personalizzata (programmatica)	457
Modifica di un'analisi personalizzata (console)	459
Modifica di un'analisi personalizzata (programmatica)	460
Creazione di nuove informazioni personalizzate da un'analisi gestita (console)	461
Eliminazione di un'analisi personalizzata (console)	462
Eliminazione di un'analisi personalizzata (programmatica)	462
Automazioni	464
Regole di automazione	464
Come funzionano le regole di automazione	465
Criteri e azioni delle regole disponibili	467
Creazione di regole di automazione	473
Visualizzazione delle regole di automazione	478
Modifica delle regole di automazione	480
Eliminazione delle regole di automazione	483
Esempi di regole di automazione	485
Risposta e correzione automatizzate	492
Tipi di EventBridge integrazione	494
EventBridge formati di eventi	496
Configurazione di una regola per l'invio automatico dei risultati	498
Configurazione e utilizzo di azioni personalizzate	505
Integrazioni di prodotti	510
Gestione delle integrazioni di prodotti	510
Visualizzazione e filtraggio dell'elenco delle integrazioni (console)	511

Visualizzazione delle informazioni sulle integrazioni dei prodotti (API Security Hub, AWS CLI)	512
Abilitazione di un'integrazione	512
Disabilitazione e abilitazione del flusso di risultati di un'integrazione (Console)	513
Disabilitazione del flusso di risultati da un'integrazione (API Security Hub, AWS CLI)	513
Abilitazione del flusso di risultati da un'integrazione (API Security Hub, AWS CLI)	514
Visualizzazione dei risultati di un'integrazione	514
Servizio AWS integrazioni	515
Panoramica delle integrazioni dei AWS servizi con Security Hub	515
AWS servizi che inviano i risultati a Security Hub	516
AWS servizi che ricevono risultati da Security Hub	532
Integrazioni di prodotti di terze parti	534
Panoramica delle integrazioni di terze parti con Security Hub	535
Integrazioni di terze parti che inviano i risultati a Security Hub	545
Integrazioni di terze parti che ricevono risultati da Security Hub	561
Integrazioni di terze parti che inviano e ricevono risultati da Security Hub	568
Utilizzo di integrazioni di prodotti personalizzate	569
Requisiti e raccomandazioni per l'invio di risultati da prodotti per la sicurezza personalizzati	570
Aggiornamento dei risultati da prodotti personalizzati	571
Esempio di integrazioni personalizzate	571
Standard e controlli	572
Autorizzazioni IAM per standard e controlli	573
Controlli e punteggi di sicurezza	574
AWS Config regole e controlli di sicurezza	575
AWS Config Risorse necessarie per i risultati del controllo	576
Pianificazione dell'esecuzione dei controlli di sicurezza	617
Generazione e aggiornamento dei risultati del controllo	618
Stato di conformità e stato di controllo	633
Definizione dei punteggi di sicurezza	635
Riferimento agli standard	637
AWS FSBP	638
CIS AWS Foundations Benchmark	652
NIST SP 800-53 Rev. 5	670
PCI DSS	684
AWS Standard di etichettatura delle risorse	687

Standard gestiti dai servizi	691
Visualizzazione e gestione degli standard di sicurezza	705
Abilitazione e disabilitazione degli standard	706
Visualizzazione dei dettagli di uno standard	713
Abilitazione e disabilitazione dei controlli in standard specifici	718
Riferimento ai controlli	725
Account AWS controlli	813
AWS Certificate Manager controlli	815
Controlli API Gateway	819
AWS AppSync controlli	825
Comandi Athena	829
AWS Backup controlli	833
CloudFormation controlli	840
CloudFront controlli	843
CloudTrail controlli	853
CloudWatch controlli	863
AWS CodeArtifact controlli	909
CodeBuild controlli	911
AWS Config controlli	916
Controlli Amazon Data Firehose	918
Controlli di rilevamento	919
AWS DMS controlli	920
Controlli Amazon DocumentDB	934
Controlli DynamoDB	939
Controlli Amazon ECR	946
Controlli Amazon ECS	950
Controlli Amazon EC2	963
Controlli di Amazon EC2 Auto Scaling	1018
Controlli di Amazon EC2 Systems Manager	1027
Controlli Amazon EFS	1031
Controlli Amazon EKS	1036
ElastiCache controlli	1043
Controlli Elastic Beanstalk	1048
Controlli Elastic Load Balancing	1052
Controlli Amazon EMR	1066
Controlli Elasticsearch	1068

EventBridge controlli	1077
Controlli Amazon FSx	1081
AWS Global Accelerator controlli	1082
AWS Glue controlli	1084
GuardDuty controlli	1086
controlli IAM	1091
AWS IoT controlli	1126
Controlli Kinesis	1135
AWS KMS controlli	1137
Controlli Lambda	1142
Controlli Amazon Macie	1148
Controlli Amazon MSK	1149
Controlli Amazon MQ	1151
Comandi Neptune	1156
Controlli Network Firewall	1164
OpenSearch Controlli del servizio	1173
AWS Private Certificate Authority controlli	1183
Controlli Amazon RDS	1184
Controlli Amazon Redshift	1220
Controlli Route 53	1235
Controlli Amazon S3	1238
SageMaker controlli	1262
Controlli di Secrets Manager	1266
Controlli del Service Catalog	1273
Controlli Amazon SES	1274
Controlli Amazon SNS	1277
Controlli Amazon SQS	1281
Controlli Step Functions	1283
Controlli Transfer Family	1286
AWS WAF controlli	1288
Visualizzazione e gestione dei controlli di sicurezza	1296
Visualizzazione consolidata dei controlli	1296
Punteggio di sicurezza complessivo per i controlli	1297
Categorie di controllo	1298
Abilitazione e disabilitazione dei controlli in tutti gli standard	1301
Abilitazione automatica di nuovi controlli negli standard abilitati	1305

Parametri di controllo personalizzati	1312
Controlli che potrebbe essere necessario disabilitare	1331
Visualizzazione dei dettagli di un controllo	1336
Filtraggio e ordinamento dei controlli	1339
Visualizzazione e adozione di misure in base ai risultati del controllo	1340
Dashboard	1366
Widget disponibili per la dashboard di riepilogo	1366
I widget sono mostrati per impostazione predefinita	1366
Widget nascosti per impostazione predefinita	1368
Filtraggio della dashboard di riepilogo	1369
Creazione e salvataggio di set di filtri	1370
Aggiornamento o eliminazione dei set di filtri	1371
Personalizzazione della dashboard di riepilogo	1371
Creazione di risorse con CloudFormation	1373
Security Hub e AWS CloudFormation modelli	1373
Scopri di più su AWS CloudFormation	1373
Iscrizione agli annunci del Security Hub	1375
Formato dei messaggi Amazon SNS	1381
Sicurezza	1383
Protezione dei dati	1383
Gestione dell'identità e degli accessi	1384
Destinatari	1385
Autenticazione con identità	1386
Gestione dell'accesso con policy	1389
Come funziona Security Hub con IAM	1392
Esempi di policy basate su identità	1400
Ruoli collegati ai servizi	1406
AWS politiche gestite	1410
Risoluzione dei problemi	1421
Convalida della conformità	1425
Resilienza	1426
Sicurezza dell'infrastruttura	1426
Endpoint VPC (AWS PrivateLink)	1427
Considerazioni sugli endpoint VPC di Security Hub	1427
Creazione di un endpoint VPC di interfaccia per Security Hub	1427
Creazione di una politica degli endpoint VPC per Security Hub	1428

Sottoreti condivise	1429
Registrazione di chiamate API	1430
Informazioni su Security Hub in CloudTrail	1430
Esempio: voci del file di registro di Security Hub	1431
Assegnazione di tag alle risorse	1433
Nozioni fondamentali sull'etichettatura	1433
Utilizzo di tag nelle policy IAM	1435
Aggiunta di tag alle risorse	1436
Revisione dei tag relativi alle risorse	1438
Modifica dei tag per le risorse	1440
Rimozione dei tag dalle risorse	1441
Quote	1444
Quote massime	1444
Quote tariffa	1444
Limiti regionali del Security Hub	1445
Restrizioni di aggregazione tra regioni	1445
Disponibilità di integrazioni per regione	1445
Integrazioni supportate in Cina (Pechino) e Cina (Ningxia)	1445
Integrazioni supportate in AWS GovCloud (Stati Uniti orientali) e (Stati Uniti occidentali)	
AWS GovCloud	1446
Disponibilità degli standard per regione	1448
Disponibilità dei controlli per regione	1448
Limiti regionali sui controlli	1448
Stati Uniti orientali (Virginia settentrionale)	1450
Stati Uniti orientali (Ohio)	1451
Stati Uniti occidentali (California settentrionale)	1452
US West (Oregon)	1454
Africa (Città del Capo)	1456
Asia Pacifico (Hong Kong)	1460
Asia Pacifico (Hyderabad)	1462
Asia Pacifico (Giacarta)	1471
Asia Pacifico (Mumbai)	1479
Asia Pacifico (Melbourne)	1480
Asia Pacifico (Osaka-Locale)	1490
Asia Pacifico (Seoul)	1497
Asia Pacifico (Singapore)	1499

Asia Pacifico (Sydney)	1501
Asia Pacifico (Tokyo)	1502
Canada (Centrale)	1504
Cina (Pechino)	1505
Cina (Ningxia)	1513
Europa (Francoforte)	1521
Europa (Irlanda)	1522
Europa (Londra)	1524
Europa (Milano)	1525
Europa (Parigi)	1529
Europa (Spagna)	1531
Europa (Stoccolma)	1542
Europa (Zurigo)	1544
Israele (Tel Aviv)	1553
Medio Oriente (Bahrein)	1564
Medio Oriente (Emirati Arabi Uniti)	1566
Sud America (San Paolo)	1575
AWS GovCloud (Stati Uniti orientali)	1577
AWS GovCloud (Stati Uniti occidentali)	1588
Disabilitazione del Security Hub	1599
Registro delle modifiche dei controlli	1601
Cronologia dei documenti	1654
.....	mdccxxix

Che cos'è AWS Security Hub?

AWS Security Hub ti offre una visione completa dello stato di sicurezza AWS e ti aiuta a valutare il tuo AWS ambiente rispetto agli standard e alle best practice del settore della sicurezza.

Security Hub raccoglie dati sulla sicurezza su tutti Account AWS i Servizi AWS prodotti di terze parti supportati e ti aiuta ad analizzare le tendenze della sicurezza e a identificare i problemi di sicurezza con la massima priorità.

Per aiutarti a gestire lo stato di sicurezza della tua organizzazione, Security Hub supporta diversi standard di sicurezza. Questi includono lo standard AWS Foundational Security Best Practices (FSBP) sviluppato da AWS e framework di conformità esterni come il Center for Internet Security (CIS), il Payment Card Industry Data Security Standard (PCI DSS) e il National Institute of Standards and Technology (NIST). Ogni standard include diversi controlli di sicurezza, ognuno dei quali rappresenta una best practice di sicurezza. Security Hub esegue controlli rispetto ai controlli di sicurezza e genera risultati di controllo per aiutarti a valutare la tua conformità rispetto alle migliori pratiche di sicurezza.

Oltre a generare risultati di controllo, Security Hub riceve anche risultati da altri prodotti, Servizi AWS come Amazon GuardDuty, Amazon Inspector e Amazon Macie, e da prodotti di terze parti supportati. Questo ti offre un'unica finestra di controllo per una serie di problemi relativi alla sicurezza. Puoi anche inviare i risultati del Security Hub ad altri Servizi AWS prodotti di terze parti supportati.

Security Hub offre funzionalità di automazione che aiutano a valutare e risolvere i problemi di sicurezza. Ad esempio, è possibile utilizzare le regole di automazione per aggiornare automaticamente i risultati critici quando un controllo di sicurezza fallisce. Puoi anche sfruttare l'integrazione con Amazon EventBridge per attivare risposte automatiche a risultati specifici.

Argomenti

- [Vantaggi del Security Hub](#)
- [Accesso al Security Hub](#)
- [Servizi correlati](#)
- [Versione di prova gratuita e prezzi di Security Hub](#)

Vantaggi del Security Hub

Ecco alcuni dei modi principali in cui Security Hub consente di monitorare il livello di conformità e sicurezza in tutto l'AWSambiente.

Riduzione dell'impegno per la raccolta e la definizione della priorità dei risultati

Security Hub riduce lo sforzo di raccogliere e assegnare priorità ai risultati di sicurezza tra gli account provenienti da prodotti integrati Servizi AWS e AWS partner. Security Hub elabora la ricerca dei dati utilizzando il AWS Security Finding Format (ASFF), un formato di ricerca standard. Ciò elimina la necessità di gestire i risultati provenienti da una miriade di fonti in più formati. Security Hub mette inoltre in correlazione i risultati dei diversi provider per aiutarti a dare priorità a quelli più importanti.

Controlli di sicurezza automatici rispetto alle best practice e agli standard

Security Hub esegue automaticamente controlli continui di configurazione e sicurezza a livello di account in base alle AWS migliori pratiche e agli standard del settore. Security Hub utilizza i risultati di questi controlli per calcolare i punteggi di sicurezza e identifica account e risorse specifici che richiedono attenzione.

Vista consolidata dei risultati per account e provider

Security Hub consolida i risultati di sicurezza su account e prodotti del provider e visualizza i risultati sulla console Security Hub. Puoi anche recuperare i risultati tramite l'API Security Hub o AWS CLI gli SDK. Con una visione olistica dello stato di sicurezza attuale, puoi individuare tendenze, identificare potenziali problemi e adottare le misure correttive necessarie.

Capacità di automatizzare la ricerca di aggiornamenti e correzioni

È possibile creare regole di automazione che modificano o sopprimono i risultati in base ai criteri definiti. Security Hub supporta anche l'integrazione con Amazon EventBridge. Per automatizzare la correzione di risultati specifici, puoi definire azioni personalizzate da intraprendere quando viene generato un risultato. Ad esempio, puoi configurare operazioni personalizzate per inviare risultati a un sistema di ticket o a un sistema di correzione automatizzato.

Accesso al Security Hub

Security Hub è disponibile nella maggior parte dei casiRegioni AWS. Per un elenco delle regioni in cui Security Hub è attualmente disponibile, consulta [Endpoint e quote del AWS Security Hub](#) nel. Riferimenti generali di AWS Per informazioni sulla gestione Regioni AWS del tuo accountAccount

AWS, consulta [Specificare quale Regioni AWS account può utilizzare nella AWS Account Management Guida](#) di riferimento.

In ogni regione, puoi accedere e utilizzare Security Hub in uno dei seguenti modi:

Console Security Hub

AWS Management Console È un'interfaccia basata su browser che è possibile utilizzare per creare e gestire AWS risorse. Come parte di tale console, la console Security Hub fornisce l'accesso all'account, ai dati e alle risorse del Security Hub. È possibile eseguire attività di Security Hub utilizzando la console Security Hub: visualizzare i risultati, creare regole di automazione, creare un'area di aggregazione e altro ancora.

API Security Hub

L'API Security Hub ti offre l'accesso programmatico all'account, ai dati e alle risorse del Security Hub. Con l'API, puoi inviare richieste HTTPS direttamente a Security Hub. Per informazioni sull'API, consulta il [AWS Security Hub API Reference](#).

AWS CLI

Con AWS CLI, è possibile eseguire comandi dalla riga di comando del sistema per eseguire le attività del Security Hub. In alcuni casi, l'utilizzo della riga di comando può essere più rapido e comodo rispetto all'utilizzo della console. La riga di comando è utile anche se si desidera creare script che eseguano operazioni. Per informazioni sull'installazione e l'uso della AWS CLI, consultare la [Guida per l'utente della AWS Command Line Interface](#).

AWS SDK

AWS fornisce SDK costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione, ad esempio Java, Go, Python, C++ e .NET. Gli SDK forniscono un accesso pratico e programmatico a Security Hub e ad altro Servizi AWS nella lingua preferita. Gestiscono anche attività come la firma crittografica delle richieste, la gestione degli errori e il tentativo automatico delle richieste. Per informazioni sull'installazione e l'utilizzo degli AWS SDK, consulta [Tools to Build on. AWS](#)

Important

Security Hub rileva e consolida solo i risultati generati dopo aver abilitato Security Hub. Non rileva e consolida retroattivamente i risultati di sicurezza generati prima dell'attivazione di Security Hub.

Security Hub riceve ed elabora i risultati solo nella regione in cui hai abilitato Security Hub nel tuo account.

Per la piena conformità ai controlli di sicurezza di CIS AWS Foundations Benchmark, è necessario abilitare Security Hub in tutte le regioni supportate AWS.

Servizi correlati

Per proteggere ulteriormente il tuo AWS ambiente, prendi in considerazione l'utilizzo di altri Servizi AWS in combinazione con Security Hub.

Per un elenco delle altre persone Servizi AWS che inviano o ricevono i risultati del Security Hub, consulta [Servizio AWS integrazioni con AWS Security Hub](#).

Security Hub utilizza regole collegate ai servizi AWS Config per eseguire i controlli di sicurezza per la maggior parte dei controlli. È necessario abilitare AWS Config e registrare le risorse in Security Hub AWS Config per generare la maggior parte dei risultati di controllo. Per ulteriori informazioni, consulta [Configurazione AWS Config](#).

Versione di prova gratuita e prezzi di Security Hub

Quando abiliti Security Hub Account AWS per la prima volta, quell'account viene automaticamente registrato a una prova gratuita di 30 giorni di Security Hub.

Quando utilizzi Security Hub durante la prova gratuita, ti viene addebitato l'utilizzo di altri servizi con cui Security Hub interagisce, come AWS Config gli articoli. Non ti vengono addebitati costi per AWS Config le regole attivate solo dagli standard di sicurezza di Security Hub.

Non ti verrà addebitato alcun costo per l'utilizzo di Security Hub fino al termine della prova gratuita.

Note

La versione di prova gratuita di Security Hub non è supportata nella regione Cina (Pechino).

Visualizzazione dei dettagli di utilizzo e dei costi stimati

Security Hub fornisce informazioni sull'utilizzo, incluso un costo stimato in 30 giorni per l'utilizzo di Security Hub. I dettagli di utilizzo includono il tempo rimanente della prova gratuita. Le informazioni

sull'utilizzo possono aiutarti a capire quali potrebbero essere i costi del Security Hub al termine del periodo di prova gratuito. Le informazioni sull'utilizzo sono disponibili anche al termine del periodo di prova gratuito.

Per visualizzare le informazioni sull'utilizzo (console)

1. Aprire la console AWS Security Hub all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, scegli Utilizzo in Impostazioni.

Il costo mensile stimato si basa sull'utilizzo del Security Hub del tuo account per i risultati e i controlli di sicurezza previsti su un periodo di 30 giorni.

Le informazioni sull'utilizzo e il costo stimato si riferiscono solo all'account corrente e alla regione corrente. In una regione di aggregazione, le informazioni sull'utilizzo e il costo stimato non includono le regioni collegate. Per ulteriori informazioni sulle regioni collegate, consulta [the section called "Come funziona l'aggregazione tra regioni"](#).

Dettagli prezzi

Per ulteriori informazioni su come Security Hub addebita i risultati acquisiti e i controlli di sicurezza, consulta i prezzi di [Security Hub](#).

Concetti di Security Hub

Questo argomento descrive i concetti e la terminologia chiave in AWS Security Hub per aiutarti a iniziare a usare il servizio.

Account

Un account Amazon Web Services (AWS) standard che contiene AWS le tue risorse. Puoi accedere AWS con il tuo account e abilitare Security Hub.

Un account può invitare altri account ad abilitare Security Hub e associarsi a quell'account in Security Hub. L'accettazione di un invito è facoltativa. Se gli inviti vengono accettati, l'account diventa un account amministratore e gli account aggiunti sono account membro. Gli account amministratore possono visualizzare i risultati nei propri account membri.

Se sei registrato AWS Organizations, l'organizzazione designa un account amministratore di Security Hub per l'organizzazione. L'account amministratore di Security Hub può abilitare altri account dell'organizzazione come account membro.

Un account non può essere contemporaneamente un account amministratore e un account membro. Un account può avere un solo account amministratore.

Per ulteriori informazioni, consulta [Gestione degli account degli amministratori e dei membri](#).

Account amministratore

Un account in Security Hub a cui è concesso l'accesso per visualizzare i risultati degli account dei membri associati.

Un account diventa un account amministratore in uno dei seguenti modi:

- L'account invita altri account a associarsi ad esso in Security Hub. Quando questi account accettano l'invito, diventano account membro e l'account che invita diventa il loro account amministratore.
- L'account è designato da un account di gestione dell'organizzazione come account amministratore di Security Hub. L'account amministratore di Security Hub può abilitare qualsiasi account dell'organizzazione come account membro e può anche invitare altri account a diventare account membro.

Un account può avere un solo account amministratore. Un account non può essere contemporaneamente un account amministratore e un account membro.

Regione di aggregazione

L'impostazione di una regione di aggregazione consente di visualizzare i risultati di sicurezza provenienti da più aree Regioni AWS in un unico pannello di controllo.

La regione di aggregazione è la regione da cui è possibile visualizzare e gestire i risultati. I risultati vengono aggregati alla regione di aggregazione delle regioni collegate. Gli aggiornamenti ai risultati vengono replicati in tutte le regioni.

Nella regione di aggregazione, le pagine degli standard di sicurezza, degli approfondimenti e dei risultati includono i dati di tutte le aree collegate.

Per informazioni, consulta [Aggregazione tra regioni](#).

Risultati archiviati

Un risultato con `RecordState` impostato su `ARCHIVED`. L'archiviazione di un risultato indica che il fornitore del risultato ritiene che il risultato non sia più pertinente. Lo stato del record è separato dallo stato del flusso di lavoro, che tiene traccia dello stato di un'indagine su un risultato.

I provider di ricerca possono utilizzare il [BatchImportFindings](#) funzionamento dell'API Security Hub per archiviare i risultati che hanno creato. Security Hub archivia automaticamente i risultati per i controlli se il controllo è disabilitato o la risorsa associata viene eliminata, in base a uno dei seguenti criteri.

- I risultati non vengono aggiornati in tre-cinque giorni (si noti che si tratta del massimo impegno e non è garantito).
- I risultati di AWS Config valutazione associati `NOT_APPLICABLE`.

Per impostazione predefinita, i risultati archiviati sono esclusi dagli elenchi dei risultati nella console Security Hub. Puoi aggiornare il filtro per includere i risultati archiviati.

Il [GetFindings](#) funzionamento dell'API Security Hub restituisce risultati attivi e archiviati. Puoi includere un filtro per lo stato del record.

```
"RecordState": [  
  {  
    "Comparison": "EQUALS",  
    "Value": "ARCHIVED"  
  }  
],
```

AWS Formato ASFF (Security Finding Format)

Un formato standardizzato per il contenuto dei risultati aggregati o generati da Security Hub. Il AWS Security Finding Format consente di utilizzare Security Hub per visualizzare e analizzare i risultati generati dai servizi di AWS sicurezza, dalle soluzioni di terze parti o dallo stesso Security Hub dall'esecuzione dei controlli di sicurezza. Per ulteriori informazioni, consulta [AWS Formato ASFF \(Security Finding Format\)](#).

Controllo

Una salvaguardia o contromisura prescritta per un sistema informatico o un'organizzazione concepita per proteggere la riservatezza, l'integrità e la disponibilità delle sue informazioni e per soddisfare una serie di requisiti di sicurezza definiti. Uno standard di sicurezza è associato a una raccolta di controlli.

Il termine controllo di sicurezza si riferisce ai controlli che hanno un unico ID e titolo di controllo per tutti gli standard. Il termine controllo standard si riferisce ai controlli con ID e titoli di controllo specifici per ogni standard. Attualmente, Security Hub supporta solo i controlli standard nelle regioni AWS GovCloud (US) Region e in Cina. I controlli di sicurezza sono supportati in tutte le altre regioni.

Operazione personalizzata

Un meccanismo Security Hub per l'invio di risultati selezionati a EventBridge. Viene creata un'azione personalizzata in Security Hub. Viene quindi collegata a una EventBridge regola. La regola definisce un'operazione specifica da eseguire quando viene ricevuta una ricerca associata all'ID operazione personalizzato. Le operazioni personalizzate possono essere utilizzate, ad esempio, per inviare una ricerca specifica, o un piccolo set di risultati, a un flusso di lavoro di risposta o di correzione. Per ulteriori informazioni, consulta [the section called "Creazione di un'azione personalizzata \(console\)"](#).

Account amministratore delegato (Organizations)

In Organizations, l'account amministratore delegato per un servizio è in grado di gestire l'utilizzo di un servizio per l'organizzazione.

In Security Hub, l'account amministratore di Security Hub è anche l'account amministratore delegato per Security Hub. Quando l'account di gestione dell'organizzazione designa per la prima volta un account amministratore di Security Hub, Security Hub chiama Organizations per rendere quell'account l'account amministratore delegato.

L'account di gestione dell'organizzazione deve quindi scegliere l'account amministratore delegato come account amministratore di Security Hub in tutte le regioni.

Risultato

La registrazione osservabile di un controllo di sicurezza o di un rilevamento correlato alla sicurezza. Security Hub genera un risultato dopo aver completato un controllo di sicurezza. Questi sono chiamati risultati del controllo. I risultati possono provenire anche da integrazioni di prodotti di terze parti.

Per ulteriori informazioni sui risultati di Security Hub, vedere [Risultati](#).

Note

I risultati vengono eliminati 90 giorni dopo l'aggiornamento più recente o 90 giorni dopo la data di creazione se non viene eseguito un aggiornamento. Per archiviare i risultati per più di 90 giorni, puoi configurare una regola EventBridge che instrada i risultati al tuo bucket Amazon S3.

Aggregazione tra regioni

L'aggregazione di risultati, approfondimenti, stati di conformità dei controlli e punteggi di sicurezza dalle regioni collegate a una regione di aggregazione. È quindi possibile visualizzare tutti i dati della regione di aggregazione e aggiornare i risultati e gli approfondimenti della regione di aggregazione.

Per informazioni, consulta [Aggregazione tra regioni](#).

Individuazione dell'ingestione

L'importazione di risultati in Security Hub da altri AWS servizi e da fornitori partner terzi.

Gli eventi di ingestione di Finding includono sia nuovi risultati che aggiornamenti dei risultati esistenti.

Informazione dettagliata

Una raccolta di risultati correlati definiti da un'istruzione di aggregazione e filtri opzionali.

Un'informazione dettagliata identifica un'area di sicurezza che richiede attenzione e intervento. Security Hub offre diverse informazioni gestite (predefinite) che non è possibile modificare. Puoi anche creare approfondimenti personalizzati sul Security Hub per tenere traccia dei problemi di

sicurezza specifici del tuo AWS ambiente e del tuo utilizzo. Per ulteriori informazioni, consulta [Informazioni dettagliate](#).

Regione collegata

Quando si abilita l'aggregazione tra aree geografiche, una regione collegata è un'area che aggrega risultati, approfondimenti, stati di conformità di controllo e punteggi di sicurezza nella regione di aggregazione.

In una regione collegata, le pagine Findings e Insights contengono solo i risultati relativi a quella regione.

Per informazioni, consulta [Aggregazione tra regioni](#).

Account membro

Un account che ha concesso l'autorizzazione a un account amministratore per visualizzare i risultati e intervenire in base ai risultati.

Un account diventa un account membro in uno dei seguenti modi:

- L'account accetta un invito da un altro account.
- Per un account dell'organizzazione, l'account amministratore di Security Hub abilita l'account come account membro.

Requisiti correlati

Un set di requisiti di settore o normativi mappati a un controllo.

Regola

Un set di criteri automatizzati utilizzati per valutare se un controllo viene rispettato. Quando viene valutata una regola, il risultato può essere positivo o negativo. Se la valutazione non è in grado di determinare se la regola ha esito negativo o positivo, la regola è in uno stato di avviso. Se la regola non può essere valutata, significa che è in uno stato non disponibile.

Controllo di sicurezza

Una point-in-time valutazione specifica di una regola rispetto a una singola risorsa che determina uno stato superato, non riuscito, di avviso o non disponibile. L'esecuzione di un controllo di sicurezza produce un risultato.

Account amministratore Security Hub

Un account dell'organizzazione che gestisce l'iscrizione a Security Hub per un'organizzazione.

L'account di gestione dell'organizzazione designa l'account amministratore di Security Hub in ciascuna regione. L'account di gestione dell'organizzazione deve scegliere lo stesso account amministratore di Security Hub in tutte le regioni.

L'account amministratore di Security Hub è anche l'account amministratore delegato per Security Hub in Organizations.

L'account amministratore di Security Hub può abilitare qualsiasi account dell'organizzazione come account membro. L'account amministratore di Security Hub può anche invitare altri account a diventare account membri.

Standard di sicurezza

Un'istruzione pubblicata su un argomento che specifica le caratteristiche, di solito misurabili e sotto forma di controlli, che devono essere soddisfatte o archiviate per conformità. Gli standard di sicurezza possono essere basati su framework normativi, best practice o policy aziendali interne. Un controllo può essere associato a uno o più standard supportati in Security Hub. Per ulteriori informazioni sugli standard di sicurezza in Security Hub, consulta [Standard e controlli](#).

Gravità

La severità assegnata a un controllo Security Hub identifica l'importanza del controllo. La severità di un controllo può essere critica, alta, media, bassa o informativa. La severità assegnata ai risultati del controllo è uguale alla gravità del controllo stesso. Per ulteriori informazioni su come Security Hub assegna la gravità a un controllo, vedere [Assegnazione della gravità ai risultati del controllo](#).

Stato del flusso di lavoro

Lo stato di un'indagine su un risultato. Viene tracciato utilizzando l'attributo `Workflow.Status`.

Lo stato del flusso di lavoro è inizialmente NEW. Se hai notificato al proprietario della risorsa che viene intrapresa un'azione per il risultato, puoi impostare lo stato del flusso di lavoro su NOTIFIED. Se il risultato non è un problema e non richiede alcuna azione, imposta lo stato del flusso di lavoro su SUPPRESSED. Dopo aver esaminato e risolto un risultato, imposta lo stato del flusso di lavoro su RESOLVED.

Per impostazione predefinita, la maggior parte degli elenchi di risultati include solo risultati con stato del flusso di lavoro NEW o NOTIFIED. Gli elenchi di risultati per i controlli includono anche i risultati RESOLVED.

Per l'operazione [GetFindings](#), puoi includere un filtro per lo stato del flusso di lavoro.

```
"WorkflowStatus": [  
  {  
    "Comparison": "EQUALS",  
    "Value": "RESOLVED"  
  }  
],
```

La console Security Hub offre un'opzione per impostare lo stato del flusso di lavoro per i risultati. I clienti (o gli strumenti SIEM, creazione di ticket, gestione degli incidenti o SOAR che lavorano per conto di un cliente per aggiornare i risultati dei provider di risultati) possono anche utilizzare [BatchUpdateFindings](#) per aggiornare lo stato del flusso di lavoro.

Consigli prima di abilitare Security Hub

I seguenti consigli possono aiutarti a iniziare a utilizzare AWS Security Hub.

Integrazione con AWS Organizations

AWS Organizations è un servizio globale di gestione degli account che consente AWS agli amministratori di consolidare e gestire centralmente più Account AWS unità organizzative (OU). Fornisce funzionalità di gestione degli account e fatturazione consolidata progettate per supportare le esigenze di budget, sicurezza e conformità. È offerto senza costi aggiuntivi e si integra con più piattaforme Servizi AWS, tra cui Security Hub GuardDuty, Amazon e Amazon Macie.

Per aiutare ad automatizzare e semplificare la gestione degli account, consigliamo vivamente di integrare Security Hub e AWS Organizations. Puoi effettuare l'integrazione con Organizations se ne hai più di una Account AWS che utilizza Security Hub.

Per istruzioni sull'attivazione dell'integrazione, consulta [Integrazione del Security Hub con AWS Organizations](#).

Utilizzo della configurazione centrale

Quando integri Security Hub and Organizations, hai la possibilità di utilizzare una funzionalità chiamata configurazione centrale per configurare e gestire Security Hub per la tua organizzazione. Consigliamo vivamente di utilizzare la configurazione centrale perché consente all'amministratore di personalizzare la copertura di sicurezza per l'organizzazione. Se del caso, l'amministratore delegato può consentire a un account membro di configurare le proprie impostazioni di copertura di sicurezza.

La configurazione centrale consente all'amministratore delegato di configurare Security Hub tra account, unità organizzative e regioni. L'amministratore delegato configura Security Hub creando policy di configurazione. All'interno di una politica di configurazione, è possibile specificare le seguenti impostazioni:

- Se Security Hub è abilitato o disabilitato
- Quali standard di sicurezza sono abilitati e disabilitati
- Quali controlli di sicurezza sono abilitati e disabilitati
- Se personalizzare i parametri per determinati controlli

In qualità di amministratore delegato, è possibile creare un'unica politica di configurazione per l'intera organizzazione o politiche di configurazione diverse per i vari account e unità organizzative. Ad esempio, gli account di test e gli account di produzione possono utilizzare politiche di configurazione diverse.

Gli account dei membri e le unità organizzative che utilizzano una politica di configurazione sono gestiti centralmente e possono essere configurati solo dall'amministratore delegato. L'amministratore delegato può designare account membri e unità organizzative specifici come autogestiti per dare al membro la possibilità di configurare le proprie impostazioni su base regionale.

Per ulteriori informazioni sulla configurazione centrale, consulta [Come funziona la configurazione centrale](#)

Configurazione AWS Config

AWS Security Hub utilizza AWS Config regole collegate ai servizi per eseguire controlli di sicurezza per la maggior parte dei controlli.

Per supportare questi controlli, AWS Config deve essere abilitato su tutti gli account, sia l'account amministratore che gli account membro, in tutti gli account in cui Regione AWS Security Hub è abilitato. Inoltre, per ogni standard abilitato AWS Config deve essere configurato in modo da registrare le risorse necessarie per i controlli abilitati.

Ti consigliamo di attivare la registrazione delle risorse AWS Config prima di abilitare gli standard Security Hub. Se Security Hub tenta di eseguire controlli di sicurezza quando la registrazione delle risorse è disattivata, i controlli restituiscono errori.

Security Hub non gestisce AWS Config per te. Se l'hai già AWS Config abilitato, puoi configurarne le impostazioni tramite la AWS Config console o le API.

Se abiliti uno standard ma non lo hai abilitato AWS Config, Security Hub tenta di creare le AWS Config regole secondo la seguente pianificazione:

- Il giorno in cui abiliti lo standard
- Il giorno dopo aver abilitato lo standard
- 3 giorni dopo l'attivazione dello standard
- 7 giorni dopo l'attivazione dello standard (e successivamente ogni 7 giorni consecutivi)

Se si utilizza la configurazione centrale, Security Hub tenta anche di creare le AWS Config regole quando si riapplica una politica di configurazione che abilita uno o più standard.

Abilitazione AWS Config

Se non l'hai AWS Config già abilitato, puoi abilitarlo in uno dei seguenti modi:

- Console o AWS CLI: è possibile abilitare manualmente AWS Config utilizzando la AWS Config console o AWS CLI. Vedi [Guida introduttiva AWS Config](#) nella Guida per gli AWS Config sviluppatori.
- AWS CloudFormation modello: se desideri abilitarlo AWS Config su un numero elevato di account, puoi abilitarlo AWS Config con il CloudFormation modello Enable AWS Config. Per accedere a questo modello, consulta i [modelli di AWS CloudFormation StackSets esempio](#) nella Guida AWS CloudFormation per l'utente.
- Script Github: Security Hub offre uno [GitHub script](#) che abilita Security Hub per più account in diverse regioni. Questo script è utile se non ti sei integrato con Organizations o se disponi di account che non fanno parte della tua organizzazione. Quando si utilizza questo script per abilitare Security Hub, si abilita automaticamente anche AWS Config per questi account.

Per ulteriori informazioni sull'abilitazione per aiutarti AWS Config a eseguire i controlli di sicurezza del Security Hub, consulta [Ottimizza AWS ConfigAWS Security Hub per gestire efficacemente la tua posizione di sicurezza sul cloud](#).

Attivazione della registrazione delle risorse in AWS Config

Quando si attiva la registrazione delle risorse AWS Config con le impostazioni predefinite, vengono registrati tutti i tipi di risorse regionali supportati presenti AWS Config nel sistema Regione AWS in cui è in esecuzione. È inoltre possibile AWS Config configurare la registrazione dei tipi di risorse globali supportati. Devi registrare le risorse globali solo in una singola regione (consigliamo che questa sia la tua regione di origine se utilizzi la configurazione centrale).

Se utilizzi CloudFormation StackSets to enable AWS Config, ti consigliamo di eseguirne due diverse StackSets. Esegui uno StackSet per registrare tutte le risorse, incluse le risorse globali, in una singola regione. Esegui un secondo StackSet per registrare tutte le risorse tranne le risorse globali in altre regioni.

Puoi anche utilizzare Quick Setup, una funzionalità di AWS Systems Manager, per configurare rapidamente la registrazione delle risorse AWS Config tra i tuoi account e le tue regioni. Durante

il processo di configurazione rapida, puoi scegliere in quale regione desideri registrare le risorse globali. Per ulteriori informazioni, consultate il [registratore di AWS Config configurazione](#) nella Guida per l'AWS Systems Manager utente.

Il controllo di sicurezza Config.1 genererà risultati non riusciti nelle regioni in cui le risorse globali non sono registrate. Questo è previsto ed è possibile utilizzare una [regola di automazione](#) per eliminare questi risultati.

Se si utilizza lo script multi-account per abilitare Security Hub, abilita automaticamente la registrazione delle risorse per tutte le risorse, incluse le risorse globali, in tutte le regioni. È quindi possibile aggiornare la configurazione per registrare le risorse globali solo in una singola regione. Per informazioni, consulta [Selezione delle risorse da AWS Config registrare](#) nella Guida per gli AWS Config sviluppatori.

Affinché Security Hub riporti in modo accurato i risultati dei controlli che si basano su AWS Config regole, è necessario abilitare la registrazione per le risorse pertinenti. Per un elenco dei controlli e AWS Config delle relative risorse, vedere [AWS Config risorse necessarie per generare i risultati del controllo](#). AWS Config consente di scegliere tra la registrazione continua e la registrazione giornaliera delle modifiche allo stato delle risorse. Se si sceglie la registrazione giornaliera, AWS Config fornisce i dati di configurazione delle risorse alla fine di ogni periodo di 24 ore in caso di cambiamenti nello stato delle risorse. Se non ci sono modifiche, non viene fornito alcun dato. Ciò può ritardare la generazione dei risultati del Security Hub per i controlli attivati dalle modifiche fino al completamento di un periodo di 24 ore.

Note

Per generare nuovi risultati dopo i controlli di sicurezza ed evitare risultati obsoleti, è necessario disporre di autorizzazioni sufficienti per il ruolo IAM collegato al registratore di configurazione per valutare le risorse sottostanti.

Considerazioni sui costi

[Per informazioni dettagliate sui costi associati alla registrazione delle risorse, consulta AWS Security Hub prezzi e prezzi.AWS Config](#)

Security Hub può influire sui costi AWS Config del registratore di configurazione aggiornando l'elemento `AWS::Config::ResourceCompliance` di configurazione. Gli aggiornamenti possono verificarsi ogni volta che un controllo Security Hub associato a una AWS Config regola modifica lo

stato di conformità, viene abilitato o disabilitato o presenta aggiornamenti dei parametri. Se utilizzi il registratore di AWS Config configurazione solo per Security Hub e non utilizzi questo elemento di configurazione per altri scopi, ti consigliamo di disattivarne la registrazione nella AWS Config console o AWS CLI. Questo può ridurre i AWS Config costi. Non è necessario registrarsi perché i controlli `AWS::Config::ResourceCompliance` di sicurezza funzionino in Security Hub.

Abilitazione del Security Hub

Esistono due modi per abilitare AWS Security Hub, mediante l'integrazione AWS Organizations o manualmente.

Consigliamo vivamente l'integrazione con Organizations per ambienti con più account e più regioni. Se disponi di un account indipendente, è necessario configurare Security Hub manualmente.

Verifica delle autorizzazioni necessarie

Dopo esserti registrato ad Amazon Web Services (AWS), devi abilitare Security Hub per utilizzarne le funzionalità e le caratteristiche. Per abilitare Security Hub, devi prima configurare le autorizzazioni che ti consentano di accedere alla console di Security Hub e alle operazioni API. Tu o il tuo AWS amministratore potete farlo utilizzando AWS Identity and Access Management (IAM) per allegare la policy AWS gestita chiamata `AWSecurityHubFullAccess` alla vostra identità IAM.

Per abilitare e gestire Security Hub tramite l'integrazione Organizations, è inoltre necessario allegare la policy AWS gestita denominata `AWSecurityHubOrganizationsAccess`.

Per ulteriori informazioni, consulta [AWS politiche gestite per AWS Security Hub](#).

Abilitare l'integrazione di Security Hub with Organizations

Per iniziare a utilizzare Security Hub con AWS Organizations, l'account di AWS Organizations gestione dell'organizzazione designa un account come account amministratore delegato di Security Hub per l'organizzazione. Security Hub viene abilitato automaticamente nell'account amministratore delegato nella regione corrente.

Scegli il metodo preferito e segui i passaggi per designare l'amministratore delegato.

Security Hub console

Per designare l'amministratore delegato del Security Hub durante l'onboarding

1. Aprire la console AWS Security Hub all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Scegli Vai a Security Hub. Ti viene richiesto di accedere all'account di gestione Organizations.

3. Nella pagina Designa amministratore delegato, nella sezione Account amministratore delegato, specifica l'account amministratore delegato. Ti consigliamo di scegliere lo stesso amministratore delegato che hai impostato per altri AWS servizi di sicurezza e conformità.
4. Scegli Imposta amministratore delegato.

Security Hub API

Richiama l'[EnableOrganizationAdminAccount](#) API dall'account di gestione Organizations. Fornisci l'Account AWSID dell'account amministratore delegato del Security Hub.

AWS CLI

Esegui il [enable-organization-admin-account](#) comando dall'account di gestione Organizations. Fornisci l'Account AWSID dell'account amministratore delegato del Security Hub.

Comando di esempio:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Per ulteriori informazioni sull'integrazione con Organizations, vedere [Integrazione del Security Hub con AWS Organizations](#).

Dopo aver designato l'amministratore delegato, ti consigliamo di continuare a configurare Security Hub con la configurazione [centralizzata](#). La console ti chiede di farlo. Utilizzando la configurazione centralizzata, è possibile semplificare il processo di attivazione e configurazione di Security Hub per l'organizzazione e garantire che l'organizzazione disponga di una copertura di sicurezza adeguata.

La configurazione centrale consente all'amministratore delegato di personalizzare Security Hub su più account e regioni dell'organizzazione anziché configurare regione per regione. È possibile creare una politica di configurazione per l'intera organizzazione o creare politiche di configurazione diverse per account e unità organizzative diversi. Le policy specificano se Security Hub è abilitato o disabilitato negli account associati e quali standard e controlli di sicurezza sono abilitati.

L'amministratore delegato può designare gli account come gestiti centralmente o autogestiti. Gli account gestiti centralmente sono configurabili solo dall'amministratore delegato. Gli account autogestiti possono specificare le proprie impostazioni.

Se non si utilizza la configurazione centrale, l'amministratore delegato ha una capacità più limitata di configurare Security Hub. Per ulteriori informazioni, consulta [Gestione degli account con AWS Organizations](#).

Abilitazione manuale di Security Hub

Devi abilitare Security Hub manualmente se disponi di un account autonomo o se non esegui l'integrazione con AWS Organizations. Gli account autonomi non possono integrarsi AWS Organizations e devono utilizzare l'abilitazione manuale.

Quando si abilita Security Hub manualmente, si designa un account amministratore di Security Hub e si invitano altri account a diventare account membro. La relazione amministratore-membro viene stabilita quando un potenziale account membro accetta l'invito.

Scegli il tuo metodo preferito e segui i passaggi per abilitare Security Hub. Quando abiliti Security Hub dalla console, hai anche la possibilità di abilitare gli standard di sicurezza supportati.

Security Hub console

1. Aprire la console AWS Security Hub all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Quando apri la console Security Hub per la prima volta, scegli Vai a Security Hub.
3. Nella pagina di benvenuto, la sezione Standard di sicurezza elenca gli standard di sicurezza supportati da Security Hub.

Seleziona la casella di controllo relativa a uno standard per abilitarlo e deseleziona la casella di controllo per disabilitarlo.

È possibile abilitare o disabilitare uno standard o i relativi controlli singoli in qualsiasi momento. Per informazioni sulla gestione degli standard e dei controlli di sicurezza, consulta [Controlli e standard di AWS sicurezza in Security Hub](#).

4. Scegliere Enable Security Hub (Abilita Security Hub).

Security Hub API

Richiama l'[EnableSecurityHub](#) API. Quando abiliti Security Hub dall'API, abilita automaticamente i seguenti standard di sicurezza predefiniti:

- AWS Foundational Security Best Practices

- Benchmark v1.2.0 delle AWS basi del Center for Internet Security (CIS)

Se non desideri abilitare questi standard, imposta `EnableDefaultStandards` su `false`.

È inoltre possibile utilizzare il `Tags` parametro per assegnare i valori dei tag alla risorsa dell'hub.

AWS CLI

Esegui il comando [enable-security-hub](#). Per abilitare gli standard predefiniti, `--enable-default-standards` includi. Per non abilitare gli standard predefiniti, includi `--no-enable-default-standards`. Gli standard di sicurezza predefiniti sono i seguenti:

- AWS Foundational Security Best Practices
- Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0

```
aws securityhub enable-security-hub [--tags <tag values>] [--enable-default-standards | --no-enable-default-standards]
```

Esempio

```
aws securityhub enable-security-hub --enable-default-standards --tags '{"Department": "Security"}
```

Script di abilitazione per più account

Note

Invece di questo script, consigliamo di utilizzare la configurazione centrale per abilitare e configurare Security Hub su più account e regioni.

Lo [script di abilitazione multi-account di Security Hub GitHub consente di](#) abilitare Security Hub tra account e regioni. Lo script automatizza anche il processo di invio e attivazione degli inviti agli account dei membri. AWS Config

Lo script abilita automaticamente la registrazione delle risorse per tutte le risorse, incluse le risorse globali, in tutte le regioni. Non limita la registrazione delle risorse globali a una singola regione.

Esiste uno script corrispondente per disabilitare Security Hub tra account e regioni.

Passaggi successivi dopo aver abilitato Security Hub

Dopo aver abilitato Security Hub, ti consigliamo di abilitare gli [standard di sicurezza e i controlli](#) di sicurezza importanti per le tue esigenze di sicurezza. Dopo aver abilitato i controlli, Security Hub inizia a eseguire i controlli di sicurezza e a generare i risultati dei controlli. Puoi anche sfruttare [le integrazioni](#) tra Security Hub Servizi AWS e altre soluzioni di terze parti per visualizzarne i risultati in Security Hub.

Come funziona la configurazione centrale

La configurazione centrale è una funzionalità di Security Hub che consente di configurare e gestire Security Hub su più Account AWS e Regioni AWS. Per utilizzare la configurazione centrale, devi prima integrare Security Hub e AWS Organizations. È possibile integrare i servizi creando un'organizzazione e designando un account amministratore delegato di Security Hub per l'organizzazione.

Dall'account amministratore delegato di Security Hub, è possibile specificare in che modo il servizio Security Hub, gli standard di sicurezza e i controlli di sicurezza sono configurati negli account e nelle unità organizzative (OU) dell'organizzazione in tutte le regioni. È possibile configurare queste impostazioni in pochi passaggi da una regione principale, denominata regione di origine. Se non utilizzi la configurazione centrale, devi configurare Security Hub separatamente in ogni account e regione.

Quando si utilizza la configurazione centrale, l'amministratore delegato può scegliere quali account e unità organizzative configurare. Se l'amministratore delegato designa un account membro o un'unità organizzativa come autogestita, il membro può configurare le proprie impostazioni separatamente in ciascuna regione. Se l'amministratore delegato designa un account membro o un'unità organizzativa come gestita centralmente, solo l'amministratore delegato può configurare l'account membro o l'unità organizzativa in tutte le regioni. È possibile designare tutti gli account e le unità organizzative dell'organizzazione come gestiti centralmente, tutti autogestiti o una combinazione di entrambi.

Per configurare gli account gestiti centralmente, l'amministratore delegato utilizza le politiche di configurazione del Security Hub. I criteri di configurazione consentono all'amministratore delegato di specificare se Security Hub è abilitato o disabilitato e quali standard e controlli sono abilitati e disabilitati. Possono essere utilizzati anche per personalizzare i parametri di determinati controlli.

Le politiche di configurazione hanno effetto nella regione di origine e in tutte le regioni collegate. L'amministratore delegato specifica la regione di origine dell'organizzazione e le regioni collegate prima di iniziare a utilizzare la configurazione centrale. L'amministratore delegato può creare un'unica politica di configurazione per l'intera organizzazione o creare più politiche di configurazione per configurare impostazioni variabili per account e unità organizzative diversi.

Questa sezione fornisce una panoramica della configurazione centrale.

Vantaggi della configurazione centralizzata

I vantaggi della configurazione centrale includono quanto segue:

Semplifica la configurazione del servizio e delle funzionalità del Security Hub

Quando utilizzi la configurazione centrale, Security Hub ti guida attraverso il processo di configurazione delle best practice di sicurezza per la tua organizzazione. Inoltre, distribuisce automaticamente le politiche di configurazione risultanti su account e unità organizzative specifici. Se disponi di impostazioni esistenti del Security Hub, come l'abilitazione automatica di nuovi controlli di sicurezza, puoi utilizzarle come punto di partenza per le tue politiche di configurazione. Inoltre, la pagina Configurazione sulla console Security Hub mostra un riepilogo in tempo reale delle policy di configurazione e degli account e delle unità organizzative che utilizzano ciascuna policy.

Configurazione su più account e regioni

È possibile utilizzare la configurazione centrale per configurare Security Hub su più account e regioni. Questo aiuta a garantire che ogni parte dell'organizzazione mantenga una configurazione coerente e una copertura di sicurezza adeguata.

Adatta configurazioni diverse in account e unità organizzative diversi

Con la configurazione centralizzata, puoi scegliere di configurare gli account e le unità organizzative della tua organizzazione in diversi modi. Ad esempio, gli account di test e gli account di produzione potrebbero richiedere configurazioni diverse. Puoi anche creare una politica di configurazione che copra i nuovi account quando entrano a far parte dell'organizzazione.

Previene la deriva della configurazione

La modifica della configurazione si verifica quando un utente apporta una modifica a un servizio o a una funzionalità che è in conflitto con le selezioni dell'amministratore delegato. La configurazione centrale impedisce questa deriva. Quando si designa un account o un'unità organizzativa come gestito centralmente, tale account o unità organizzativa è configurabile solo dall'amministratore delegato dell'organizzazione. Se si preferisce che un account o un'unità organizzativa specifici configurino le proprie impostazioni, è possibile designarlo come autogestito.

Chi dovrebbe usare la configurazione centrale?

La configurazione centrale è particolarmente utile per AWS gli ambienti che includono più account Security Hub. È progettato per aiutarti a gestire centralmente Security Hub per più account.

È possibile utilizzare la configurazione centrale per configurare il servizio Security Hub, gli standard di sicurezza e i controlli di sicurezza. Puoi anche usarlo per personalizzare i parametri di determinati controlli. Per informazioni su standard e controlli, vedere [Controlli e standard di AWS sicurezza in Security Hub](#).

Termini e concetti relativi alla configurazione centrale

La comprensione dei seguenti termini e concetti chiave può aiutarti a utilizzare la configurazione centrale di Security Hub.

Configurazione centrale

Una funzionalità di Security Hub che aiuta l'account amministratore delegato di Security Hub di un'organizzazione a configurare il servizio Security Hub, gli standard di sicurezza e i controlli di sicurezza su più account e regioni. Per configurare queste impostazioni, l'amministratore delegato crea e gestisce le politiche di configurazione del Security Hub per gli account gestiti centralmente nella propria organizzazione. Gli account autogestiti possono configurare le proprie impostazioni separatamente in ciascuna regione. Per utilizzare la configurazione centrale, è necessario integrare Security Hub e AWS Organizations.

Regione d'origine

Regione AWS Da cui l'amministratore delegato configura centralmente Security Hub, creando e gestendo le politiche di configurazione. Le politiche di configurazione hanno effetto nella regione di origine e in tutte le regioni collegate.

La regione di origine funge anche da regione di aggregazione del Security Hub, ricevendo risultati, approfondimenti e altri dati dalle regioni collegate.

Le regioni AWS introdotte a partire dal 20 marzo 2019 sono note come regioni opt-in. Una regione opt-in non può essere la regione di origine, ma può essere una regione collegata. Per un elenco delle regioni che hanno aderito, consulta [Considerazioni prima di abilitare e disabilitare le regioni](#) nella Guida di riferimento per la gestione degli AWS account.

Regione collegata

È la Regione AWS che è configurabile dalla regione di origine. Le politiche di configurazione vengono create dall'amministratore delegato nella regione di origine. Le politiche hanno effetto nella regione di origine e in tutte le regioni collegate. È necessario specificare almeno una regione collegata per utilizzare la configurazione centrale.

Una regione collegata invia inoltre risultati, approfondimenti e altri dati alla regione di origine.

Le regioni AWS introdotte a partire dal 20 marzo 2019 sono note come regioni opt-in. È necessario abilitare tale regione per un account prima di potervi applicare una politica di configurazione. L'account di gestione Organizations può abilitare le regioni opzionali per un account membro. Per ulteriori informazioni, consulta [Specificare quali Regioni AWS account può essere utilizzato dal proprio account](#) nella Guida di riferimento per la gestione degli AWS account.

Politica di configurazione del Security Hub

Una raccolta di impostazioni del Security Hub che l'amministratore delegato può configurare per gli account gestiti centralmente. Questo include:

- Se abilitare o disabilitare Security Hub.
- Se abilitare uno o più [standard di sicurezza](#).
- Quali [controlli di sicurezza](#) abilitare tra gli standard abilitati. L'amministratore delegato può farlo fornendo un elenco di controlli specifici che devono essere abilitati e Security Hub disabilita tutti gli altri controlli (inclusi i nuovi controlli quando vengono rilasciati). In alternativa, l'amministratore delegato può fornire un elenco di controlli specifici che devono essere disabilitati e Security Hub abilita tutti gli altri controlli (inclusi i nuovi controlli quando vengono rilasciati).
- Facoltativamente, [personalizza i parametri](#) per selezionare i controlli abilitati tra gli standard abilitati.

Una politica di configurazione ha effetto nella regione di origine e in tutte le regioni collegate dopo essere stata associata ad almeno un account, un'unità organizzativa (OU) o la directory principale.

Sulla console Security Hub, l'amministratore delegato può scegliere la politica di configurazione consigliata da Security Hub o creare policy di configurazione personalizzate. Con l'API Security Hub e AWS CLI, l'amministratore delegato può creare solo politiche di configurazione personalizzate. L'amministratore delegato può creare un massimo di 20 politiche di configurazione personalizzate.

Nella politica di configurazione consigliata, Security Hub, lo standard AWS Foundational Security Best Practices (FSBP) e tutti i controlli FSBP esistenti e nuovi sono abilitati. I controlli che accettano i parametri utilizzano i valori predefiniti. La politica di configurazione consigliata si applica all'intera organizzazione.

Per applicare impostazioni diverse all'organizzazione o applicare politiche di configurazione diverse a account e unità organizzative diversi, crea una politica di configurazione personalizzata.

Configurazione locale

Il tipo di configurazione predefinito per un'organizzazione, dopo l'integrazione di Security Hub e AWS Organizations. Con la configurazione locale, l'amministratore delegato può scegliere di abilitare automaticamente Security Hub e [gli standard di sicurezza predefiniti](#) nei nuovi account dell'organizzazione nella regione corrente. Se l'amministratore delegato abilita automaticamente gli standard predefiniti, tutti i controlli che fanno parte di questi standard vengono abilitati automaticamente anche con parametri predefiniti per i nuovi account dell'organizzazione. Queste impostazioni non si applicano agli account esistenti, quindi è possibile modificare la configurazione dopo che un account si unisce all'organizzazione. La disabilitazione di controlli specifici che fanno parte degli standard predefiniti e la configurazione di standard e controlli aggiuntivi devono essere eseguite separatamente in ogni account e regione.

La configurazione locale non supporta l'uso di politiche di configurazione. Per utilizzare i criteri di configurazione, è necessario passare alla configurazione centrale.

Gestione manuale degli account

Se non integri Security Hub AWS Organizations o disponi di un account autonomo, devi specificare le impostazioni per ciascun account separatamente in ciascuna regione. La gestione manuale degli account non supporta l'uso di politiche di configurazione.

API di configurazione centralizzate

Operazioni di Security Hub che solo l'amministratore del Security Hub delegato di Security Hub può utilizzare nella regione di residenza per gestire le politiche di configurazione per gli account gestiti centralmente. Le operazioni includono:

- `CreateConfigurationPolicy`
- `DeleteConfigurationPolicy`
- `GetConfigurationPolicy`
- `ListConfigurationPolicies`

- `UpdateConfigurationPolicy`
- `StartConfigurationPolicyAssociation`
- `StartConfigurationPolicyDisassociation`
- `GetConfigurationPolicyAssociation`
- `BatchGetConfigurationPolicyAssociations`
- `ListConfigurationPolicyAssociations`

API specifiche dell'account

Operazioni di Security Hub che possono essere utilizzate per abilitare o disabilitare Security Hub, standard e controlli su account-by-account base individuale. Queste operazioni vengono utilizzate in ogni singola regione.

Gli account autogestiti possono utilizzare operazioni specifiche dell'account per configurare le proprie impostazioni. Gli account gestiti centralmente non possono utilizzare le seguenti operazioni specifiche dell'account nella regione di origine e nelle regioni collegate. In tali regioni, solo l'amministratore delegato può configurare gli account gestiti centralmente tramite operazioni di configurazione e politiche di configurazione centralizzate.

- `BatchDisableStandards`
- `BatchEnableStandards`
- `BatchUpdateStandardsControlAssociations`
- `DisableSecurityHub`
- `EnableSecurityHub`
- `UpdateStandardsControl`

Per verificare lo stato dell'account, il proprietario di un account gestito centralmente può utilizzare `Get` qualsiasi `Describe` operazione dell'API Security Hub.

Se si utilizza la configurazione locale o la gestione manuale degli account, anziché la configurazione centrale, è possibile utilizzare queste operazioni specifiche dell'account.

Gli account autogestiti possono inoltre essere utilizzati e utilizzati*`Invitations`. *`Members` Tuttavia, consigliamo che gli account autogestiti non utilizzino queste operazioni. Le associazioni di policy possono fallire se un account membro ha i propri membri che fanno parte di un'organizzazione diversa da quella dell'amministratore delegato.

Unità organizzativa (OU)

In AWS Organizations and Security Hub, un contenitore per un gruppo di Account AWS. Un'unità organizzativa (OU) può contenere anche altre unità organizzative, il che consente di creare una gerarchia simile a un albero capovolto, con un'unità organizzativa principale nella parte superiore e rami di unità organizzative che si estendono verso il basso e terminano con gli account che sono le foglie dell'albero. Un'unità organizzativa può avere esattamente un genitore e ogni account dell'organizzazione può essere membro di una sola unità organizzativa.

È possibile gestire le unità organizzative in AWS Organizations o AWS Control Tower. Per ulteriori informazioni, vedere [Gestione delle unità organizzative](#) nella Guida per l'AWS Organizations utente o [Gestione di organizzazioni e account AWS Control Tower](#) nella Guida per l'AWS Control Tower utente.

L'amministratore delegato può associare le politiche di configurazione a account o unità organizzative specifici oppure alla directory principale per coprire tutti gli account e le unità organizzative di un'organizzazione.

Gestito centralmente

Un account, unità organizzativa o root che solo l'amministratore delegato può configurare in tutte le regioni utilizzando i criteri di configurazione.

L'account amministratore delegato specifica se un account è gestito centralmente.

L'amministratore delegato può anche modificare lo stato di un account da gestito centralmente a gestito automaticamente o viceversa.

Autogestito

Un account, unità organizzativa o root che gestisce le proprie impostazioni del Security Hub. Un account autogestito utilizza operazioni specifiche dell'account per configurare Security Hub separatamente in ciascuna regione. Ciò è in contrasto con gli account gestiti centralmente, che sono configurabili solo dall'amministratore delegato in tutte le regioni tramite politiche di configurazione.

L'account amministratore delegato specifica se un account è gestito automaticamente. L'account amministratore delegato può anche modificare lo stato di un account da autogestito a gestito centralmente o viceversa.

L'amministratore delegato può applicare un comportamento autogestito a un account o a un'unità organizzativa. In alternativa, un account o un'unità organizzativa può ereditare il comportamento

autogestito da un genitore. L'account amministratore delegato può essere esso stesso un account autogestito.

Associazione dei criteri di configurazione

Un collegamento tra una politica di configurazione e un account, un'unità organizzativa (OU) o una radice. Quando esiste un'associazione di policy, l'account, l'unità organizzativa o la root utilizza le impostazioni definite dalla politica di configurazione. Esiste un'associazione in uno di questi casi:

- Quando l'amministratore delegato applica direttamente una politica di configurazione a un account, a un'unità organizzativa o a una cartella principale
- Quando un account o un'unità organizzativa eredita una politica di configurazione da un'unità organizzativa principale o dalla directory principale

Un'associazione esiste fino a quando non viene applicata o ereditata una configurazione diversa.

Politica di configurazione applicata

Un tipo di associazione di criteri di configurazione in cui l'amministratore delegato applica direttamente una politica di configurazione agli account di destinazione, alle unità organizzative o alla directory principale. Gli obiettivi sono configurati nel modo definito dalla politica di configurazione e solo l'amministratore delegato può modificarne la configurazione. Se applicata a root, la politica di configurazione influisce su tutti gli account e le unità organizzative dell'organizzazione che non utilizzano una configurazione diversa tramite l'applicazione o l'ereditarietà dal genitore più vicino.

L'amministratore delegato può anche applicare una configurazione autogestita ad account specifici, unità organizzative o alla directory principale.

Politica di configurazione ereditata

Un tipo di associazione di criteri di configurazione in cui un account o un'unità organizzativa adotta la configurazione dell'unità organizzativa principale o principale più vicina. Se un criterio di configurazione non viene applicato direttamente a un account o a un'unità organizzativa, eredita la configurazione dell'elemento principale più vicino. Tutti gli elementi di una policy vengono ereditati. In altre parole, un account o un'unità organizzativa non possono scegliere di ereditare selettivamente solo parti di una politica. Se il genitore più vicino è autogestito, l'account figlio o l'unità organizzativa eredita il comportamento autogestito del genitore.

L'ereditarietà non può sovrascrivere una configurazione applicata. In altre parole, se un criterio di configurazione o una configurazione autogestita viene applicata direttamente a un account

o a un'unità organizzativa, utilizza tale configurazione e non eredita la configurazione dell'unità principale.

Root

In AWS Organizations and Security Hub, il nodo principale di livello superiore di un'organizzazione. Se l'amministratore delegato applica una politica di configurazione a root, la politica viene associata a tutti gli account e le unità organizzative dell'organizzazione, a meno che non utilizzino una politica diversa, tramite l'applicazione o l'ereditarietà, o non siano designati come autogestiti. Se l'amministratore definisce la directory principale come autogestita, tutti gli account e le unità organizzative dell'organizzazione vengono gestiti automaticamente, a meno che non utilizzino una politica di configurazione tramite l'applicazione o l'ereditarietà. Se la directory principale è gestita automaticamente e al momento non esistono criteri di configurazione, tutti i nuovi account dell'organizzazione mantengono le impostazioni correnti.

I nuovi account che entrano a far parte di un'organizzazione rientrano nella cartella principale finché non vengono assegnati a un'unità organizzativa specifica. Se un nuovo account non viene assegnato a un'unità organizzativa, eredita la configurazione principale a meno che l'amministratore delegato non lo designi come account autogestito.

Inizia a usare la configurazione centrale

L'account amministratore AWS Security Hub delegato può utilizzare la configurazione centrale per configurare Security Hub, standard e controlli per più account e unità organizzative (OU) in tuttoRegioni AWS.

Questa sezione spiega i prerequisiti per la configurazione centrale e come iniziare a utilizzarla.

Prerequisiti per la configurazione centrale

Prima di iniziare a utilizzare la configurazione centralizzata, è necessario integrare Security Hub AWS Organizations e designare una regione di residenza. Se si utilizza la console Security Hub, questi prerequisiti sono inclusi nel flusso di lavoro di attivazione per la configurazione centralizzata.

Integrazione con Organizations

È necessario integrare Security Hub and Organizations per utilizzare la configurazione centrale.

Per integrare questi servizi, è necessario innanzitutto creare un'organizzazione in Organizations. Dall'account di gestione Organizations, si designa quindi un account amministratore delegato di Security Hub. Per istruzioni, consulta [Integrazione del Security Hub con AWS Organizations](#).

Assicurati di designare l'amministratore delegato nella regione di residenza desiderata. Quando inizi a utilizzare la configurazione centrale, lo stesso amministratore delegato viene impostato automaticamente anche in tutte le regioni collegate. L'account di gestione Organizations non può essere impostato come account amministratore delegato.

Important

Quando si utilizza la configurazione centrale, non è possibile utilizzare la console di Security Hub o le API di Security Hub per modificare o rimuovere l'account amministratore delegato. Se l'account di gestione Organizations utilizza le AWS Organizations API per modificare o rimuovere l'amministratore delegato di Security Hub, Security Hub interrompe automaticamente la configurazione centrale. Inoltre, le policy di configurazione vengono dissociate ed eliminate. Gli account dei membri mantengono la configurazione che avevano prima della modifica o della rimozione dell'amministratore delegato.

Designare una regione d'origine

È necessario designare una regione d'origine per utilizzare la configurazione centralizzata. La regione d'origine è la regione da cui l'amministratore delegato configura l'organizzazione.

Per utilizzare la configurazione centrale, è necessario specificare almeno una regione collegata configurabile dalla regione di origine.

Note

La regione d'origine non può essere una regione AWS designata come regione opt-in. Per impostazione predefinita, una regione che prevede l'attivazione è disattivata. Per un elenco delle regioni che hanno aderito, consulta [Considerazioni prima di abilitare e disabilitare le regioni](#) nella Guida di riferimento per la gestione degli AWSaccount.

L'amministratore delegato può creare e gestire le politiche di configurazione solo dalla regione di origine. Le politiche di configurazione hanno effetto nella regione di origine e in tutte le regioni

collegate. Non è possibile creare una politica di configurazione che si applichi solo a un sottoinsieme di queste regioni e non ad altre.

La regione di origine è anche la [regione di aggregazione del Security Hub](#) che riceve risultati, approfondimenti e altri dati dalle regioni collegate.

Se hai già impostato una regione di aggregazione per l'aggregazione tra regioni, questa è la tua regione principale predefinita per la configurazione centrale. Puoi modificare la regione di residenza prima di iniziare a utilizzare la configurazione centrale eliminando l'aggregatore di ricerca corrente e creandone uno nuovo nella regione di residenza desiderata. Un aggregatore di risultati è una risorsa del Security Hub che specifica la regione di origine e le regioni collegate.

Per designare una regione di origine, segui i [passaggi per impostare una](#) regione di aggregazione. Se disponi già di una regione di residenza, puoi richiamare l'[GetFindingAggregator](#) API per visualizzarne i dettagli, incluse le regioni attualmente collegate.

Avvia la configurazione centralizzata

Scegli il tuo metodo preferito e segui i passaggi per iniziare a utilizzare la configurazione centralizzata per la tua organizzazione.

Security Hub console

Per configurare centralmente la tua organizzazione

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.
2. Nel riquadro di navigazione, scegli Impostazioni e configurazione. Quindi, scegli Avvia configurazione centrale.

Se stai effettuando l'onboarding su Security Hub, scegli Vai a Security Hub.

3. Nella pagina Designare un amministratore delegato, seleziona il tuo account di amministratore delegato o inserisci l'ID dell'account. Se applicabile, ti consigliamo di scegliere lo stesso amministratore delegato che hai impostato per altri servizi di AWS sicurezza e conformità. Scegli Imposta amministratore delegato.
4. Nella pagina Centralizza l'organizzazione, nella sezione Regioni, seleziona la tua regione d'origine. Devi aver effettuato l'accesso alla regione d'origine per procedere. Se hai già impostato una regione di aggregazione per l'aggregazione tra regioni, viene visualizzata come regione principale. Per modificare la regione d'origine, scegli Modifica impostazioni

della regione. Puoi quindi selezionare la tua regione d'origine preferita e tornare a questo flusso di lavoro.

5. Seleziona almeno una regione da collegare alla regione d'origine. Facoltativamente, scegli se collegare automaticamente le future regioni supportate alla regione d'origine. Le regioni selezionate qui saranno configurabili dalla regione d'origine dall'amministratore delegato. Le politiche di configurazione hanno effetto nella regione di origine e in tutte le regioni collegate.
6. Scegli Conferma e continua.
7. Ora puoi usare la configurazione centrale. Continua a seguire le istruzioni della console per creare la tua prima politica di configurazione. Se non sei ancora pronto per creare una politica di configurazione, scegli Non sono ancora pronto a configurare. Puoi creare una politica in un secondo momento scegliendo Impostazioni e configurazione nel riquadro di navigazione. Per istruzioni sulla creazione di una politica di configurazione, consulta [Creazione e associazione dei criteri di configurazione del Security Hub](#).

Security Hub API

Per configurare centralmente Security Hub

1. Utilizzando le credenziali dell'account amministratore delegato, richiama l'[UpdateOrganizationConfiguration](#) API dalla regione di origine.
2. Imposta il campo su. `AutoEnable false`
3. Imposta il `ConfigurationType` campo nell'`OrganizationConfiguration` oggetto su `CENTRAL`. Questa azione ha il seguente impatto:
 - Designa l'account chiamante come amministratore delegato del Security Hub in tutte le regioni collegate.
 - Abilita Security Hub nell'account amministratore delegato in tutte le regioni collegate.
 - Designa l'account chiamante come amministratore delegato di Security Hub per gli account nuovi ed esistenti che utilizzano Security Hub e appartengono all'organizzazione. Ciò si verifica nella regione d'origine e in tutte le regioni collegate. L'account chiamante viene impostato come amministratore delegato per i nuovi account dell'organizzazione solo se sono associati a una politica di configurazione con Security Hub abilitato. L'account chiamante viene impostato come amministratore delegato per gli account dell'organizzazione esistenti solo se hanno già abilitato Security Hub.

- Viene [AutoEnable](#) impostato su `false` in tutte le regioni collegate e viene impostato [AutoEnableStandards](#) su `NONE` nella regione di origine e in tutte le regioni collegate. Questi parametri non sono rilevanti nella home page e nelle regioni collegate quando si utilizza la configurazione centrale, ma è possibile abilitare automaticamente Security Hub e gli standard di sicurezza predefiniti negli account dell'organizzazione tramite l'uso di policy di configurazione.
4. Ora puoi usare la configurazione centrale. L'amministratore delegato può creare policy di configurazione per configurare Security Hub nell'organizzazione. Per istruzioni sulla creazione di una politica di configurazione, consulta [Creazione e associazione dei criteri di configurazione del Security Hub](#).

Esempio di richiesta API:

```
{
  "AutoEnable": false,
  "OrganizationConfiguration": {
    "ConfigurationType": "CENTRAL"
  }
}
```

AWS CLI

Per configurare centralmente Security Hub

1. Utilizzando le credenziali dell'account amministratore delegato, esegui il [update-organization-configuration](#) comando dalla regione di origine.
2. Includere il parametro `no-auto-enable`.
3. Imposta il `ConfigurationType` campo nell'`organization-configuration` oggetto su `CENTRAL`. Questa azione ha il seguente impatto:
 - Designa l'account chiamante come amministratore delegato del Security Hub in tutte le regioni collegate.
 - Abilita Security Hub nell'account amministratore delegato in tutte le regioni collegate.
 - Designa l'account chiamante come amministratore delegato di Security Hub per gli account nuovi ed esistenti che utilizzano Security Hub e appartengono all'organizzazione. Ciò si verifica nella regione d'origine e in tutte le regioni collegate. L'account chiamante

viene impostato come amministratore delegato per i nuovi account dell'organizzazione solo se sono associati a una politica di configurazione con Security Hub abilitato. L'account chiamante viene impostato come amministratore delegato per gli account dell'organizzazione esistenti solo se hanno già abilitato Security Hub.

- Imposta l'opzione di attivazione automatica su tutte le regioni collegate e imposta su [no-auto-enable](#) nella regione [auto-enable-standards](#) di origine e NONE in tutte le regioni collegate. Questi parametri non sono rilevanti nella home page e nelle regioni collegate quando si utilizza la configurazione centrale, ma è possibile abilitare automaticamente Security Hub e gli standard di sicurezza predefiniti negli account dell'organizzazione tramite l'uso di policy di configurazione.
4. Ora puoi usare la configurazione centrale. L'amministratore delegato può creare policy di configurazione per configurare Security Hub nell'organizzazione. Per istruzioni sulla creazione di una politica di configurazione, consulta [Creazione e associazione dei criteri di configurazione del Security Hub](#).

Comando di esempio:

```
aws securityhub --region us-east-1 update-organization-configuration \  
--no-auto-enable \  
--organization-configuration '{"ConfigurationType": "CENTRAL"}'
```

Scelta del tipo di gestione degli account e delle unità organizzative

Quando si utilizza la configurazione centrale, l'amministratore AWS Security Hub delegato può designare ogni account e unità organizzativa (OU) dell'organizzazione come gestiti centralmente o autogestiti. Il tipo di gestione di un account o di un'unità organizzativa determina come specificare e modificare le impostazioni del Security Hub.

Un account o un'unità organizzativa autogestiti possono configurare le proprie impostazioni del Security Hub separatamente in ciascuno Regione AWS di essi. L'amministratore delegato non può configurare le impostazioni del Security Hub per un account o un'unità organizzativa autogestiti e i criteri di configurazione non possono essere associati a tali impostazioni. Al contrario, solo l'amministratore delegato può configurare le impostazioni del Security Hub per gli account e le unità organizzative gestiti centralmente nella regione di origine e nelle regioni collegate. Le policy di configurazione possono essere associate ad account e unità organizzative gestiti centralmente.

L'amministratore delegato può cambiare lo stato di un account o di un'unità organizzativa tra gestione automatica e gestione centralizzata. Per impostazione predefinita, tutti gli account e l'unità organizzativa vengono gestiti automaticamente quando si avvia la configurazione centrale tramite l'API Security Hub. Nella console, il tipo di gestione dipende dalla prima politica di configurazione. Gli account e le unità organizzative associati alla prima policy vengono gestiti centralmente. Per impostazione predefinita, gli altri account e unità organizzative vengono gestiti automaticamente.

Se si associa una politica di configurazione a un account autogestito, la politica prevale sulla designazione autogestita. L'account viene gestito centralmente e adotta le impostazioni riportate nella politica di configurazione.

Gli account figli e le unità organizzative possono ereditare il comportamento autogestito da un genitore autogestito, allo stesso modo in cui gli account figlio e le unità organizzative possono ereditare le politiche di configurazione da un genitore gestito centralmente. Per ulteriori informazioni, consulta [Associazione delle politiche tramite applicazione ed ereditarietà](#).

Un account o un'unità organizzativa autogestiti non possono ereditare una politica di configurazione da un nodo principale o dalla radice. Ad esempio, se si desidera che tutti gli account e le unità organizzative dell'organizzazione ereditino una politica di configurazione dalla radice, è necessario modificare il tipo di gestione dei nodi autogestiti in gestione centralizzata.

Specificazione delle impostazioni per gli account autogestiti

Gli account autogestiti devono configurare le proprie impostazioni separatamente in ciascuna regione.

I proprietari di account autogestiti possono richiamare le seguenti operazioni dell'API Security Hub in ciascuna regione per configurare le proprie impostazioni:

- `EnableSecurityHub` `DisableSecurityHub` per abilitare o disabilitare il servizio Security Hub
- `BatchEnableStandardse` `BatchDisableStandards` per abilitare o disabilitare gli standard
- `BatchUpdateStandardsControlAssociationso` `UpdateStandardsControl` per abilitare o disabilitare i controlli

Gli account autogestiti possono inoltre essere utilizzati `*Invitations` e utilizzati `*Members`.

Tuttavia, consigliamo che gli account autogestiti non utilizzino queste operazioni. Le associazioni di policy possono fallire se un account membro ha i propri membri che fanno parte di un'organizzazione diversa da quella dell'amministratore delegato.

Per le descrizioni delle azioni dell'API Security Hub, consulta l'[AWS Security Hub API Reference](#).

Gli account autogestiti possono anche utilizzare la console Security Hub o AWS CLI configurarne le impostazioni in ciascuna regione.

Gli account autogestiti non possono richiamare alcuna API relativa ai criteri di configurazione e alle associazioni di policy di Security Hub. Solo l'amministratore delegato può richiamare le API di configurazione centrale e utilizzare le politiche di configurazione per configurare account gestiti centralmente.

Scelta del tipo di gestione degli account e delle unità organizzative

Scegli il metodo che preferisci e segui i passaggi per designare un account o un'unità organizzativa come gestita centralmente o autogestita.

Security Hub console

Per scegliere il tipo di gestione di un account o di un'unità organizzativa

1. Aprire la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).

Accedi utilizzando le credenziali dell'account amministratore delegato di Security Hub nella regione di residenza.

2. Scegliere Configuration (Configurazione).
3. Nella scheda Organizzazione, seleziona l'account o l'unità organizzativa di destinazione. Scegli Modifica.
4. Nella pagina Definisci configurazione, per Tipo di gestione, scegli Gestito centralmente se desideri che l'amministratore delegato configuri l'account o l'unità organizzativa di destinazione. Quindi, scegli Applica una politica specifica se desideri associare una politica di configurazione esistente alla destinazione. Scegli Inherit from my organization se desideri che il target erediti la configurazione del genitore più vicino. Scegli Autogestito se desideri che l'account o l'unità organizzativa configurino le proprie impostazioni.
5. Seleziona Successivo. Rivedi le modifiche e scegli Salva.

Security Hub API

Per scegliere il tipo di gestione di un account o di un'unità organizzativa

1. Richiama l'[StartConfigurationPolicyAssociation](#) API dall'account amministratore delegato di Security Hub nella regione di origine.
2. Per il `ConfigurationPolicyIdentifier` campo, specifica `SELF_MANAGED_SECURITY_HUB` se desideri che l'account o l'unità organizzativa controllino le proprie impostazioni. Fornisci l'Amazon Resource Name (ARN) o l'ID della politica di configurazione pertinente se desideri che l'amministratore delegato controlli le impostazioni dell'account o dell'unità organizzativa.
3. Per il `Target` campo, fornisci l' Account AWS ID, l'ID OU o l'ID root della destinazione di cui desideri modificare il tipo di gestione. Ciò associa il comportamento autogestito o la politica di configurazione specificata alla destinazione. Gli account secondari della destinazione possono ereditare il comportamento autogestito o la politica di configurazione.

Esempio di richiesta API per designare un account autogestito:

```
{
  "ConfigurationPolicyIdentifier": "SELF_MANAGED_SECURITY_HUB",
  "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Per scegliere il tipo di gestione di un account o di un'unità organizzativa

1. Esegui il [start-configuration-policy-association](#) comando dall'account amministratore delegato di Security Hub nella regione di residenza.
2. Per `configuration-policy-identifier` campo, specifica `SELF_MANAGED_SECURITY_HUB` se desideri che l'account o l'unità organizzativa controllino le proprie impostazioni. Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione pertinente se desideri che l'amministratore delegato controlli le impostazioni dell'account o dell'unità organizzativa.
3. Per il `target` campo, fornisci l' Account AWS ID, l'ID OU o l'ID root della destinazione di cui desideri modificare il tipo di gestione. Ciò associa il comportamento autogestito o la politica

di configurazione specificata alla destinazione. Gli account secondari della destinazione possono ereditare il comportamento autogestito o la politica di configurazione.

Esempio di comando per designare un account autogestito:

```
aws securityhub --region us-east-1 start-configuration-policy-association \  
--configuration-policy-identifier "SELF_MANAGED_SECURITY_HUB" \  
--target '{"AccountId": "123456789012"}'
```

Come funzionano le politiche di configurazione di Security Hub

L'account amministratore delegato può creare policy di AWS Security Hub configurazione per configurare Security Hub, standard di sicurezza e controlli di sicurezza nell'organizzazione. Dopo aver creato una politica di configurazione, l'amministratore delegato può associarla agli account, alle unità organizzative (OU) o alla directory principale. L'amministratore delegato può anche visualizzare, modificare o eliminare le politiche di configurazione.

Considerazioni sulle politiche

Prima di creare una politica di configurazione in Security Hub, considera i seguenti dettagli.

- Le politiche di configurazione devono essere associate per avere effetto: dopo aver creato una politica di configurazione, è possibile associarla a uno o più account, unità organizzative (OU) o root. Una politica di configurazione può essere associata agli account o alle unità organizzative tramite applicazione diretta o tramite ereditarietà da un'unità organizzativa principale.
- Un account o un'unità organizzativa possono essere associati a una sola politica di configurazione: per evitare conflitti di impostazioni, un account o un'unità organizzativa può essere associato a una sola politica di configurazione alla volta. In alternativa, un account o un'unità organizzativa possono essere gestiti automaticamente.
- I criteri di configurazione sono completi: i criteri di configurazione forniscono una specifica completa delle impostazioni. Ad esempio, un account figlio non può accettare impostazioni per alcuni controlli da un criterio e impostazioni per altri controlli da un altro criterio. Quando associ una politica a un account per bambini, assicurati che la politica specifichi tutte le impostazioni che desideri che l'account per bambini utilizzi.

- I criteri di configurazione non possono essere ripristinati: non è possibile ripristinare un criterio di configurazione dopo averlo associato ad account o unità organizzative. Ad esempio, se si associa una politica di configurazione che disabilita CloudWatch i controlli a un account specifico e poi si dissocia tale politica, i CloudWatch controlli continuano a essere disabilitati in quell'account. Per abilitare nuovamente CloudWatch i controlli, puoi associare l'account a una nuova politica che abilita i controlli. In alternativa, puoi modificare l'account rendendolo autogestito e abilitare ogni CloudWatch controllo nell'account.
- I criteri di configurazione hanno effetto nella regione di origine e in tutte le regioni collegate: i criteri di configurazione hanno effetto su tutti gli account associati nella regione di origine e in tutte le regioni collegate. Non è possibile creare una politica di configurazione che abbia effetto solo in alcune di queste regioni e non in altre. L'eccezione è rappresentata dai [controlli che coinvolgono risorse globali](#).

Le regioni AWS introdotte a partire dal 20 marzo 2019 sono note come regioni opt-in. È necessario abilitare tale regione per un account prima che una politica di configurazione abbia effetto su tale account. L'account di gestione Organizations può abilitare le regioni opzionali per un account membro. Per istruzioni sull'attivazione delle regioni che richiedono l'iscrizione, consulta [Specificare quali possono essere utilizzate dal Regioni AWS tuo account nella Guida](#) di riferimento per la gestione degli AWS account.

Se la tua politica configura un controllo che non è disponibile nella regione d'origine o in una o più aree collegate, Security Hub ignora la configurazione del controllo nelle regioni non disponibili ma applica la configurazione nelle regioni in cui il controllo è disponibile.

- Le policy di configurazione sono risorse: come risorsa, una policy di configurazione ha un Amazon Resource Name (ARN) e un identificatore univoco universale (UUID). L'ARN utilizza il seguente formato: `arn:partition:securityhub:region:delegated administrator account ID:configuration-policy/configuration policy UUID` Una configurazione autogestita non ha ARN o UUID. L'identificatore per una configurazione autogestita è `SELF_MANAGED_SECURITY_HUB`

Tipi di politiche di configurazione

Ogni politica di configurazione specifica le seguenti impostazioni:

- Abilita o disabilita Security Hub.
- Abilita uno o più [standard di sicurezza](#).

- Indica quali [controlli di sicurezza](#) sono abilitati tra gli standard abilitati. Puoi farlo fornendo un elenco di controlli specifici che devono essere abilitati e Security Hub disabilita tutti gli altri controlli, inclusi i nuovi controlli quando vengono rilasciati. In alternativa, puoi fornire un elenco di controlli specifici che devono essere disabilitati e Security Hub abilita tutti gli altri controlli, inclusi i nuovi controlli quando vengono rilasciati.
- Facoltativamente, [personalizza i parametri](#) per selezionare i controlli abilitati tra gli standard abilitati.

Le politiche di configurazione centralizzate non includono le impostazioni del AWS Config registratore. È necessario abilitare AWS Config e attivare separatamente la registrazione per le risorse richieste affinché Security Hub generi i risultati del controllo. Per ulteriori informazioni, consulta [Configurazione AWS Config](#).

Se si utilizza la configurazione centrale, Security Hub disattiva automaticamente i controlli che coinvolgono risorse globali in tutte le regioni tranne la regione di origine. Gli altri controlli che scegli di abilitare tramite una politica di configurazione sono abilitati in tutte le regioni in cui sono disponibili. Per limitare i risultati di questi controlli a una sola regione, puoi aggiornare le impostazioni del AWS Config registratore e disattivare la registrazione globale delle risorse in tutte le regioni tranne la regione d'origine. Quando utilizzi la configurazione centrale, non hai la copertura necessaria per un controllo che non è disponibile nella regione d'origine e in nessuna delle regioni collegate. Per un elenco dei controlli che coinvolgono risorse globali, consulta [Controlli che riguardano le risorse globali](#).

Politica di configurazione consigliata

Quando si crea una politica di configurazione per la prima volta nella console di Security Hub, è possibile scegliere la politica consigliata da Security Hub.

La policy consigliata abilita Security Hub, lo standard AWS Foundational Security Best Practices (FSBP) e tutti i controlli FSBP esistenti e nuovi. I controlli che accettano i parametri utilizzano i valori predefiniti. La politica consigliata si applica a root (tutti gli account e le unità organizzative, sia nuovi che esistenti). Dopo aver creato la politica consigliata per l'organizzazione, è possibile modificarla dall'account amministratore delegato. Ad esempio, puoi abilitare standard o controlli aggiuntivi o disabilitare controlli FSBP specifici. Per istruzioni sulla modifica di una politica di configurazione, consulta [Aggiornamento delle politiche di configurazione del Security Hub](#)

Politica di configurazione personalizzata

Invece della politica consigliata, l'amministratore delegato può creare fino a 20 politiche di configurazione personalizzate. È possibile associare una singola politica personalizzata all'intera organizzazione o diverse politiche personalizzate a diversi account e unità organizzative. Per una politica di configurazione personalizzata, è necessario specificare le impostazioni desiderate. Ad esempio, puoi creare una policy personalizzata che abiliti FSBP, il Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 e tutti i controlli di tali standard tranne i controlli Amazon Redshift. Il livello di granularità utilizzato nelle politiche di configurazione personalizzate dipende dall'ambito di copertura di sicurezza previsto in tutta l'organizzazione.

Note

Non è possibile associare una politica di configurazione che disabiliti Security Hub all'account amministratore delegato. Tale politica può essere associata ad altri account ma ignora l'associazione con l'amministratore delegato. L'account amministratore delegato mantiene la configurazione corrente.

Dopo aver creato una politica di configurazione personalizzata, è possibile passare alla politica di configurazione consigliata aggiornando la politica di configurazione in modo che rifletta la configurazione consigliata. Tuttavia, non è possibile scegliere di creare la politica di configurazione consigliata nella console Security Hub dopo la creazione della prima politica.

Associazione delle politiche tramite applicazione ed ereditarietà

Quando si attiva per la prima volta la configurazione centralizzata, l'organizzazione non ha associazioni e si comporta nello stesso modo in cui si comportava prima dell'opt-in. L'amministratore delegato può quindi stabilire associazioni tra una politica di configurazione o un comportamento autogestito e gli account, le unità organizzative o la directory principale. Le associazioni possono essere stabilite tramite applicazione o ereditarietà.

Dall'account amministratore delegato, è possibile applicare direttamente una politica di configurazione a un account, a un'unità organizzativa o alla radice. In alternativa, l'amministratore delegato può applicare direttamente una designazione autogestita a un account, a un'unità organizzativa o alla directory principale.

In assenza di un'applicazione diretta, un account o un'unità organizzativa eredita le impostazioni del genitore più vicino che ha una politica di configurazione o un comportamento autogestito. Se

Il genitore più vicino è associato a una politica di configurazione, il figlio eredita tale politica ed è configurabile solo dall'amministratore delegato della regione di origine. Se il genitore più prossimo è autogestito, il figlio eredita il comportamento autogestito e ha la possibilità di specificare le proprie impostazioni in ciascuno di essi. Regione AWS

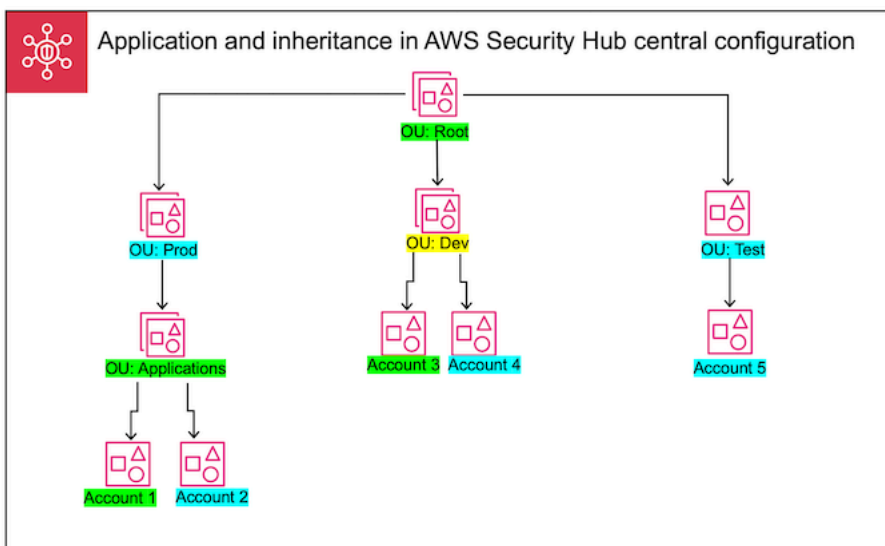
L'applicazione ha la precedenza sull'ereditarietà. In altre parole, l'ereditarietà non sostituisce una politica di configurazione o una designazione autogestita che l'amministratore delegato ha applicato direttamente a un account o a un'unità organizzativa.

Se si applica direttamente un criterio di configurazione a un account autogestito, il criterio ha la precedenza sulla designazione autogestita. L'account viene gestito centralmente e adotta le impostazioni riportate nella politica di configurazione.

Si consiglia di applicare direttamente una politica di configurazione alla radice. Se applichi una policy alla root, i nuovi account che entrano a far parte dell'organizzazione ereditano automaticamente la policy principale, a meno che non li associ a una politica diversa o non li definiate come autogestiti.

È possibile associare una sola politica di configurazione a un account o a un'unità organizzativa alla volta, tramite applicazione o ereditarietà. Questo è progettato per evitare conflitti di impostazioni.

Il diagramma seguente illustra come funzionano l'applicazione delle politiche e l'ereditarietà nella configurazione centrale.



In questo esempio, a un nodo evidenziato in verde è stata applicata una politica di configurazione. A un nodo evidenziato in blu non è stata applicata alcuna politica di configurazione. Un nodo evidenziato in giallo è stato designato come autogestito. Ogni account e unità organizzativa utilizza la seguente configurazione:

- OU:Root (verde): questa unità organizzativa utilizza la politica di configurazione che le è stata applicata.
- ou:Prod (blu) — Questa unità organizzativa eredita la politica di configurazione da OU:Root.
- ou:Applications (verde) — Questa unità organizzativa utilizza la politica di configurazione che le è stata applicata.
- Account 1 (verde): questo account utilizza la politica di configurazione che gli è stata applicata.
- Account 2 (blu): questo account eredita la politica di configurazione da OU:Applications.
- ou:Dev (giallo) — Questa unità organizzativa è gestita automaticamente.
- Account 3 (verde): questo account utilizza la politica di configurazione che gli è stata applicata.
- Account 4 (blu): questo account eredita il comportamento autogestito da OU:Dev.
- ou:Test (Blue) — Questo account eredita la politica di configurazione da ou:Root.
- Account 5 (blu): questo account eredita la politica di configurazione da OU:Root poiché il suo genitore immediato, ou:Test, non è associato a una politica di configurazione.

Test di una politica di configurazione

Per testare l'effetto di una politica di configurazione, è possibile associarla a un singolo account o unità organizzativa prima di associarla più ampiamente all'interno dell'organizzazione.

Per testare una politica di configurazione

1. Crea una politica di configurazione personalizzata, ma non applicarla a nessun account. Verificare che le impostazioni specificate per l'abilitazione, gli standard e i controlli del Security Hub siano corrette.
2. Applica la politica di configurazione a un account di prova o a un'unità organizzativa che non dispone di account secondari o unità organizzative.
3. Verifica che l'account di test o l'unità organizzativa utilizzi la politica di configurazione nel modo previsto nella tua regione di origine e in tutte le regioni collegate. Puoi anche verificare che tutti gli altri account e unità organizzative dell'organizzazione rimangano autogestiti e che sia possibile modificare le proprie impostazioni in ciascuna regione.

Dopo aver testato una politica di configurazione in un singolo account o unità organizzativa, è possibile associarla ad altri account e unità organizzative. Per istruzioni sulla creazione e l'associazione delle policy, consulta [Creazione e associazione dei criteri di configurazione del Security](#)

[Hub](#). I figli degli account applicati ereditano la politica, a meno che non siano gestiti autonomamente o non si applichi loro una politica di configurazione diversa. È inoltre possibile modificare le politiche di configurazione e creare politiche di configurazione aggiuntive, se necessario.

Creazione e associazione dei criteri di configurazione del Security Hub

L'account amministratore delegato può creare politiche di AWS Security Hub configurazione e associarle agli account dell'organizzazione, alle unità organizzative (OU) o alla radice. È inoltre possibile associare una configurazione autogestita agli account, alle unità organizzative o alla directory principale.

Se è la prima volta che crei una politica di configurazione, ti consigliamo di [Come funzionano le politiche di configurazione di Security Hub](#) esaminarla prima.

Scegliete il metodo di accesso preferito e seguite i passaggi per creare e associare una policy di configurazione o una configurazione autogestita. Quando si utilizza la console Security Hub, è possibile associare una configurazione a più account o unità organizzative contemporaneamente. Quando si utilizza l'API Security Hub oppure AWS CLI, è possibile associare una configurazione a un solo account o unità organizzativa in ogni richiesta.

Note

Se si utilizza la configurazione centrale, Security Hub disattiva automaticamente i controlli che coinvolgono risorse globali in tutte le regioni tranne la regione di origine. Gli altri controlli che scegli di abilitare tramite una politica di configurazione sono abilitati in tutte le regioni in cui sono disponibili. Per limitare i risultati di questi controlli a una sola regione, puoi aggiornare le impostazioni del AWS Config registratore e disattivare la registrazione globale delle risorse in tutte le regioni tranne la regione d'origine. Quando utilizzi la configurazione centrale, non hai la copertura necessaria per un controllo che non è disponibile nella regione d'origine e in nessuna delle regioni collegate. Per un elenco dei controlli che coinvolgono risorse globali, consulta [Controlli che riguardano le risorse globali](#).

Security Hub console

Per creare e associare politiche di configurazione

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).

Accedi utilizzando le credenziali dell'account amministratore delegato di Security Hub nella regione di residenza.

2. Nel riquadro di navigazione, scegli Configurazione e la scheda Politiche. Quindi, scegli Crea politica.

3. Nella pagina Configura organizzazione, se è la prima volta che crei una politica di configurazione, vedi tre opzioni in Tipo di configurazione. Se hai già creato almeno una politica di configurazione, vedi solo l'opzione Politica personalizzata.

- Scegli Usa la configurazione AWS consigliata di Security Hub in tutta la mia organizzazione per utilizzare la nostra politica consigliata. La politica consigliata abilita Security Hub in tutti gli account dell'organizzazione, abilita lo standard AWS Foundational Security Best Practices (FSBP) e abilita tutti i controlli FSBP nuovi ed esistenti. I controlli utilizzano i valori dei parametri predefiniti.
- Scegli Non sono ancora pronto a configurare per creare una politica di configurazione in un secondo momento.
- Scegli Politica personalizzata per creare una politica di configurazione personalizzata. Specificare se abilitare o disabilitare Security Hub, quali standard abilitare e quali controlli abilitare in base a tali standard. Facoltativamente, specifica [i valori dei parametri personalizzati](#) per uno o più controlli abilitati che supportano i parametri personalizzati.

4. Nella sezione Account, scegli gli account di destinazione, le unità organizzative o la radice a cui desideri applicare la politica di configurazione.

- Scegli Tutti gli account se desideri applicare la politica di configurazione alla radice. Ciò include tutti gli account e le unità organizzative dell'organizzazione a cui non è stata applicata o ereditata un'altra politica.
- Scegli Account specifici se desideri applicare la politica di configurazione a account o unità organizzative specifici. Inserisci gli ID degli account o seleziona gli account e le unità organizzative dalla struttura dell'organizzazione. È possibile applicare la politica a un massimo di 15 account o a un'unità organizzativa contenente un massimo di 15 account. Per specificare un numero maggiore, modifica la politica dopo la creazione e applicala ad altri account.

- Scegli Solo l'amministratore delegato per applicare la politica di configurazione all'account amministratore delegato corrente.
5. Seleziona Successivo.
 6. Nella pagina Rivedi e applica, esamina i dettagli della politica di configurazione. Quindi, scegli Crea politica e applica. Nella tua regione d'origine e nelle aree collegate, questa azione sostituisce le impostazioni di configurazione esistenti degli account associati a questa politica di configurazione. Gli account possono essere associati alla politica di configurazione tramite l'applicazione o l'ereditarietà da un nodo principale. Gli account secondari e le unità organizzative delle destinazioni applicate ereditano automaticamente questa politica di configurazione a meno che non vengano specificamente esclusi, gestiti automaticamente o utilizzino una politica di configurazione diversa.

Security Hub API

Per creare e associare politiche di configurazione

1. Richiama l'[CreateConfigurationPolicy](#) API dall'account amministratore delegato di Security Hub nella regione di origine.
2. Per `Name`, fornisci un nome univoco per la politica di configurazione. Facoltativamente `Description`, fornisci una descrizione della politica di configurazione.
3. Per il `ServiceEnabled` campo, specifica se desideri che Security Hub sia abilitato o disabilitato in questa politica di configurazione.
4. Per il `EnabledStandardIdentifiers` campo, specifica quali standard Security Hub desideri abilitare in questa politica di configurazione.
5. Per l'`SecurityControlsConfiguration` oggetto, specifica quali controlli vuoi abilitare o disabilitare in questa politica di configurazione. La scelta `EnabledSecurityControlIdentifiers` significa che i controlli specificati sono abilitati. Gli altri controlli che fanno parte degli standard abilitati (inclusi i controlli appena rilasciati) sono disabilitati. La scelta `DisabledSecurityControlIdentifiers` significa che i controlli specificati sono disabilitati. Gli altri controlli che fanno parte degli standard abilitati (inclusi i controlli appena rilasciati) sono abilitati.
6. Facoltativamente, per il `SecurityControlCustomParameters` campo, specificate i controlli abilitati per i quali desiderate personalizzare i parametri. `CUSTOM` specificate il `ValueType` campo e il valore del parametro personalizzato per il `Value` campo. Il valore deve essere il tipo di dati corretto e rientrare negli intervalli validi specificati da Security

Hub. Solo i controlli selezionati supportano valori di parametri personalizzati. Per ulteriori informazioni, consulta [Parametri di controllo personalizzati](#).

7. Per applicare i criteri di configurazione agli account o alle unità organizzative, richiama l'[StartConfigurationPolicyAssociation](#) API dall'account amministratore delegato di Security Hub nella regione di residenza.
8. Per il `ConfigurationPolicyIdentifier` campo, fornisci l'Amazon Resource Name (ARN) o l'identificatore univoco universale (UUID) della politica. L'ARN e l'UUID vengono restituiti dall'API. `CreateConfigurationPolicy` Per una configurazione autogestita, il `ConfigurationPolicyIdentifier` campo è uguale a `SELF_MANAGED_SECURITY_HUB`
9. Per il `Target` campo, fornisci l'unità organizzativa, l'account o l'ID root a cui desideri applicare questa politica di configurazione. È possibile fornire un solo obiettivo in ogni richiesta API. Gli account secondari e le unità organizzative della destinazione selezionata ereditano automaticamente questa politica di configurazione, a meno che non vengano gestiti automaticamente o utilizzino una politica di configurazione diversa.

Esempio di richiesta API per creare una politica di configurazione:

```
{
  "Name": "SampleConfigurationPolicy",
  "Description": "Configuration policy for production accounts",
  "ConfigurationPolicy": {
    "SecurityHub": {
      "ServiceEnabled": true,
      "EnabledStandardIdentifiers": [
        "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
        "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
      ],
      "SecurityControlsConfiguration": {
        "DisabledSecurityControlIdentifiers": [
          "CloudTrail.2"
        ],
        "SecurityControlCustomParameters": [
          {
            "SecurityControlId": "ACM.1",
            "Parameters": {
              "daysToExpiration": {
                "ValueType": "CUSTOM",
```

```

    "Value": {
      "Integer": 15
    }
  }
}

```

Esempio di richiesta API per associare una politica di configurazione:

```

{
  "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Target": {"OrganizationalUnitId": "ou-examplerootid111-exampleouid111"}
}

```

AWS CLI

Per creare e associare politiche di configurazione

1. Esegui il [create-configuration-policy](#) comando dall'account amministratore delegato di Security Hub nella regione di residenza.
2. Per `name`, fornisci un nome univoco per la politica di configurazione. Facoltativamente `description`, fornisci una descrizione della politica di configurazione.
3. Per il `ServiceEnabled` campo, specifica se desideri che Security Hub sia abilitato o disabilitato in questa politica di configurazione.
4. Per il `EnabledStandardIdentifiers` campo, specifica quali standard Security Hub desideri abilitare in questa politica di configurazione.
5. Per il `SecurityControlsConfiguration` campo, specifica quali controlli vuoi abilitare o disabilitare in questa politica di configurazione. La scelta `EnabledSecurityControlIdentifiers` significa che i controlli specificati sono abilitati. Gli altri controlli che fanno parte degli standard abilitati (inclusi i controlli appena rilasciati) sono disabilitati. La scelta `DisabledSecurityControlIdentifiers` significa che i

controlli specificati sono disabilitati. Gli altri controlli che si applicano agli standard abilitati (inclusi i controlli appena rilasciati) sono abilitati.

6. Facoltativamente, per il `SecurityControlCustomParameters` campo, specificate i controlli abilitati per i quali desiderate personalizzare i parametri. `CUSTOM` specificate il `ValueType` campo e il valore del parametro personalizzato per il `Value` campo. Il valore deve essere il tipo di dati corretto e rientrare negli intervalli validi specificati da Security Hub. Solo i controlli selezionati supportano valori di parametri personalizzati. Per ulteriori informazioni, consulta [Parametri di controllo personalizzati](#).
7. Per applicare i criteri di configurazione agli account o alle unità organizzative, esegui il [start-configuration-policy-association](#) comando dall'account amministratore delegato di Security Hub nella regione di origine.
8. Per il `configuration-policy-identifier` campo, fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione. L'ARN e l'ID vengono restituiti dal `create-configuration-policy` comando.
9. Per il `target` campo, fornisci l'unità organizzativa, l'account o l'ID root a cui desideri applicare questa politica di configurazione. È possibile fornire un solo obiettivo ogni volta che si esegue il comando. I figli della destinazione selezionata ereditano automaticamente questa politica di configurazione a meno che non si gestiscano autonomamente o utilizzino una politica di configurazione diversa.

Comando di esempio per creare una politica di configurazione:

```
aws securityhub --region us-east-1 create-configuration-policy \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-
foundational-security-best-practices/v/1.0.0", "arn:aws:securityhub:::ruleset/
cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}]}}}'
```

Comando di esempio per associare una politica di configurazione:

```
aws securityhub --region us-east-1 start-configuration-policy-association \
```

```
--configuration-policy-identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"OrganizationalUnitId": "ou-examplerootid111-exampleeuid111"}'
```

L'`StartConfigurationPolicyAssociationAPI` restituisce un campo chiamato `AssociationStatus`. Questo campo indica se un'associazione di politiche è in sospeso o in uno stato di successo o di fallimento. La modifica dello stato da a SUCCESS o FAILURE può richiedere fino a 24 ore. PENDING Per ulteriori informazioni sullo stato dell'associazione, vedere [Stato di associazione di una configurazione](#).

Visualizzazione dei criteri di configurazione del Security Hub

L'account amministratore delegato può visualizzare le politiche di AWS Security Hub configurazione di un'organizzazione e i relativi dettagli.

Scegli il tuo metodo preferito e segui i passaggi per visualizzare le tue politiche di configurazione.

Console

Per visualizzare le politiche di configurazione

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.

Accedi utilizzando le credenziali dell'account amministratore delegato di Security Hub nella regione di residenza.

2. Nel riquadro di navigazione, scegli Impostazioni e configurazione.
3. Scegli la scheda Politiche per visualizzare una panoramica delle tue politiche di configurazione.
4. Seleziona una politica di configurazione e scegli Visualizza dettagli per visualizzare ulteriori dettagli al riguardo.

API

Per visualizzare i criteri di configurazione

Per visualizzare un elenco riepilogativo di tutte le politiche di configurazione, richiama l'[ListConfigurationPolicies](#) API dall'account amministratore delegato di Security Hub nella tua area geografica. È possibile fornire parametri di impaginazione opzionali

Esempio di richiesta API:

```
{
  "MaxResults": 5,
  "NextToken": "U2FsdGVkX19nUI2zoh+Pou9Yyut1YJHwPn9xnG4hqS0hvw3o2JqjI23QDxdf"
}
```

Per visualizzare i dettagli su una politica di configurazione specifica, richiama l'[GetConfigurationPolicy](#) API dall'account amministratore delegato di Security Hub nella tua regione di residenza. Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione di cui desideri visualizzare i dettagli.

Esempio di richiesta API:

```
{
  "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

Per visualizzare un elenco riepilogativo di tutte le politiche di configurazione e delle relative associazioni, richiama l'[ListConfigurationPolicyAssociations](#) API dall'account amministratore delegato di Security Hub nella tua regione di residenza. Facoltativamente, puoi fornire parametri di impaginazione o filtrare i risultati in base a un ID di policy specifico, al tipo di associazione o allo stato dell'associazione.

Esempio di richiesta API:

```
{
  "AssociationType": "APPLIED"
}
```

Per visualizzare le associazioni per uno specifico account, unità organizzativa o root, richiama l'[BatchGetConfigurationPolicyAssociations](#) API

[GetConfigurationPolicyAssociation](#) dall'account amministratore delegato del Security Hub nella tua regione di residenza. Per Target, fornisci il numero di account, l'ID dell'unità organizzativa o l'ID root.

```
{
  "Target": {"AccountId": "123456789012"}
}
```

AWS CLI

Per visualizzare le politiche di configurazione

Per visualizzare un elenco riepilogativo di tutte le politiche di configurazione, esegui il [list-configuration-policies](#) comando dall'account amministratore delegato di Security Hub nella tua area geografica.

Comando di esempio:

```
aws securityhub --region us-east-1 list-configuration-policies \
--max-items 5 \
--starting-token U2FsdGVkX19nUI2zoh+Pou9YyutlYJHWpn9xnG4hqS0hvw3o2JqjI23QDxdf
```

Per visualizzare i dettagli su una politica di configurazione specifica, esegui il [get-configuration-policy](#) comando dall'account amministratore delegato di Security Hub nella tua area geografica. Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione di cui desideri visualizzare i dettagli.

```
aws securityhub --region us-east-1 get-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Per visualizzare un elenco riepilogativo di tutte le politiche di configurazione e le relative associazioni di account, esegui il [list-configuration-policy-associations](#) comando dall'account amministratore delegato di Security Hub nella tua regione di residenza.

Facoltativamente, è possibile fornire parametri di impaginazione o filtrare i risultati in base a un ID di policy specifico, al tipo di associazione o allo stato dell'associazione.

```
aws securityhub --region us-east-1 list-configuration-policy-associations \
--association-type "APPLIED"
```

Per visualizzare le associazioni per un account specifico, esegui il [batch-get-configuration-policy-associations](#) comando [get-configuration-policy-association](#) dall'account amministratore delegato di Security Hub nella tua regione di residenza. Per `target`, fornisci il numero di account, l'ID dell'unità organizzativa o l'ID root.

```
aws securityhub --region us-east-1 get-configuration-policy-association \
--target '{"AccountId": "123456789012"}
```

Stato di associazione di una configurazione

Le seguenti operazioni API di configurazione centrale restituiscono un campo chiamato `AssociationStatus`:

- `BatchGetConfigurationPolicyAssociations`
- `GetConfigurationPolicyAssociation`
- `ListConfigurationPolicyAssociations`
- `StartConfigurationPolicyAssociation`

Questo campo viene restituito sia quando la configurazione sottostante è una politica di configurazione sia quando si tratta di un comportamento autogestito.

Il valore di `AssociationStatus` indica se un'associazione di policy è in sospeso o in uno stato di successo o di fallimento. La modifica dello stato da a `SUCCESS` o `FAILURE` può richiedere fino a 24 ore. `PENDING` Lo stato di associazione di un'unità organizzativa principale o dell'unità principale dipende dallo stato dei relativi elementi secondari. Se lo status di associazione di tutti i figli è `SUCCESS`, lo stato dell'associazione del genitore è `SUCCESS`. Se lo status dell'associazione di uno o più figli è `FAILED`, lo stato dell'associazione del genitore è `FAILED`.

Il valore di `AssociationStatus` dipende anche da tutte le regioni. Se l'associazione ha successo nella regione d'origine e in tutte le regioni collegate, il valore di `AssociationStatus` è `SUCCESS`. Se l'associazione fallisce in una o più di queste regioni, il valore di `AssociationStatus` è `FAILED`.

Il seguente comportamento influisce anche sul valore di `AssociationStatus`:

- Se la destinazione è un'unità organizzativa principale o la radice, ha uno stato `AssociationStatus` di `SUCCESS` o `FAILED` solo quando tutti i figli hanno uno `FAILED` stato `SUCCESS` or. Se lo stato di associazione di un account figlio o di un'unità organizzativa cambia (ad esempio, quando viene aggiunta o rimossa una regione collegata) dopo aver associato per la prima volta l'account principale a una configurazione, la modifica non aggiorna lo stato di associazione dell'unità principale a meno che non si richiami nuovamente `StartConfigurationPolicyAssociationAPI`.
- Se la destinazione è un account, ha un `AssociationStatus` `SUCCESS` o `FAILED` solo se l'associazione ha un risultato nella regione d'`SUCCESS`origine e `FAILED` in tutte le regioni collegate. Se lo stato dell'associazione di un account di destinazione cambia (ad esempio, quando viene aggiunta o rimossa una regione collegata) dopo averlo associato per la prima volta a una configurazione, lo stato dell'associazione viene aggiornato. Tuttavia, la modifica non aggiorna lo stato dell'associazione del genitore a meno che non si richiami nuovamente `StartConfigurationPolicyAssociationAPI`.

Se aggiungi una nuova regione collegata, Security Hub replica le associazioni esistenti che si trovano in una `PENDING` o in `FAILED` uno stato della nuova regione. `SUCCESS`

Le cause più comuni del fallimento dell'associazione

Un'associazione ai criteri di configurazione potrebbe fallire per i seguenti motivi comuni:

- L'account di gestione Organizations non è un membro: se desideri associare una policy di configurazione all'account di gestione Organizations, su quell'account deve essere già abilitato Security Hub. Questo rende l'account di gestione un account membro dell'organizzazione.
- AWS Config non è abilitato o configurato correttamente: per abilitare gli standard in una politica di configurazione, AWS Config deve essere abilitato e configurato per registrare le risorse pertinenti.
- È necessario eseguire l'associazione da un account amministratore delegato: è possibile associare una politica agli account e alle unità organizzative di destinazione solo dopo aver effettuato l'accesso all'account amministratore delegato.
- È necessario l'associazione dalla regione di origine: puoi associare una politica agli account e alle unità organizzative di destinazione solo quando hai effettuato l'accesso alla regione d'origine.
- Regione di attivazione non abilitata: l'associazione delle politiche non riesce per un account membro o un'unità organizzativa in una regione collegata se si tratta di una regione opt-in che

l'amministratore delegato non ha abilitato. È possibile riprovare dopo aver abilitato la regione dall'account amministratore delegato.

- Account membro sospeso: l'associazione delle politiche fallisce se si tenta di associare una politica a un account membro sospeso.

Aggiornamento delle politiche di configurazione del Security Hub

L'account amministratore delegato può aggiornare le politiche di AWS Security Hub configurazione in base alle esigenze. L'amministratore delegato può aggiornare le impostazioni dei criteri, gli account o le unità organizzative a cui è associata una politica o entrambi. Quando le impostazioni dei criteri vengono aggiornate, gli account associati alla politica di configurazione iniziano automaticamente a utilizzare la politica aggiornata.

Analogamente a quando è stata creata la politica di configurazione, è possibile aggiornare le seguenti impostazioni dei criteri:

- Abilita o disabilita Security Hub.
- Abilita uno o più [standard di sicurezza](#).
- Indica quali [controlli di sicurezza](#) sono abilitati tra gli standard abilitati. Puoi farlo fornendo un elenco di controlli specifici che devono essere abilitati e Security Hub disabilita tutti gli altri controlli, inclusi i nuovi controlli quando vengono rilasciati. In alternativa, puoi fornire un elenco di controlli specifici che devono essere disabilitati e Security Hub abilita tutti gli altri controlli, inclusi i nuovi controlli quando vengono rilasciati.
- Facoltativamente, [personalizza i parametri](#) per selezionare i controlli abilitati tra gli standard abilitati.

Scegli il tuo metodo preferito e segui i passaggi per aggiornare una politica di configurazione.

Se si utilizza la configurazione centrale, Security Hub disattiva automaticamente i controlli che coinvolgono risorse globali in tutte le regioni tranne la regione di origine. Gli altri controlli che scegli di abilitare tramite una politica di configurazione sono abilitati in tutte le regioni in cui sono disponibili. Per limitare i risultati di questi controlli a una sola regione, puoi aggiornare le impostazioni del AWS Config registratore e disattivare la registrazione globale delle risorse in tutte le regioni tranne la regione d'origine. Quando utilizzi la configurazione centrale, non hai la copertura necessaria per un controllo che non è disponibile nella regione d'origine e in nessuna delle regioni collegate. Per un elenco dei controlli che coinvolgono risorse globali, consulta [Controlli che riguardano le risorse globali](#).

Console

Per aggiornare le politiche di configurazione

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).

Accedi utilizzando le credenziali dell'account amministratore delegato di Security Hub nella regione di residenza.

2. Nel riquadro di navigazione, scegli Impostazioni e configurazione.
3. Scegliere la scheda Policy.
4. Seleziona la politica di configurazione che desideri modificare e scegli Modifica. Se lo desideri, modifica le impostazioni dei criteri. Lasciate questa sezione così com'è se desiderate mantenere invariate le impostazioni dei criteri.
5. Scegliete Avanti. Se lo desiderate, modificate le associazioni di policy. Lasciate questa sezione così com'è se desiderate mantenere invariate le associazioni di politiche.
6. Seleziona Successivo.
7. Rivedi le modifiche e scegli Salva e applica. Nella tua regione d'origine e nelle regioni collegate, questa azione sostituisce le impostazioni di configurazione esistenti degli account associati a questa politica di configurazione. Gli account possono essere associati a una politica di configurazione tramite l'applicazione o ereditati da un nodo principale.

API

Per aggiornare le politiche di configurazione

1. Per aggiornare le impostazioni in una politica di configurazione, richiama l'[UpdateConfigurationPolicy](#) API dall'account amministratore delegato di Security Hub nella regione di residenza.
2. Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione che desideri aggiornare.
3. Fornisci valori aggiornati per i campi `ConfigurationPolicy` sottostanti. Facoltativamente, puoi anche fornire un motivo per l'aggiornamento.
4. Per aggiungere nuove associazioni per questa politica di configurazione, richiama l'[StartConfigurationPolicyAssociation](#) API dall'account amministratore delegato di Security Hub nella regione di residenza. Per rimuovere una o più associazioni correnti, richiama

l'[StartConfigurationPolicyDisassociation](#) API dall'account amministratore delegato di Security Hub nella regione di origine.

5. Per il `ConfigurationPolicyIdentifier` campo, fornisci l'ARN o l'ID della politica di configurazione di cui desideri aggiornare le associazioni.
6. Per il `Target` campo, fornite gli account, le unità organizzative o l'ID root che desiderate associare o dissociare. Questa azione sostituisce le precedenti associazioni di policy per le unità organizzative o gli account specificati.

Note

Quando richiami l'`UpdateConfigurationPolicy` API, Security Hub esegue una sostituzione completa dell'elenco per i `SecurityControlCustomParameters` campi `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers` e. Ogni volta che richiami questa API, fornisci l'elenco completo degli standard che desideri abilitare e l'elenco completo dei controlli per i quali desideri abilitare o disabilitare e personalizzare i parametri.

Esempio di richiesta API per aggiornare una politica di configurazione:

```
{
  "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Description": "Updated configuration policy",
  "UpdatedReason": "Disabling CloudWatch.1",
  "ConfigurationPolicy": {
    "SecurityHub": {
      "ServiceEnabled": true,
      "EnabledStandardIdentifiers": [
        "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0",
        "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0"
      ],
      "SecurityControlsConfiguration": {
        "DisabledSecurityControlIdentifiers": [
          "CloudTrail.2",
          "CloudWatch.1"
        ]
      }
    }
  }
}
```

```
"SecurityControlCustomParameters": [  
  {  
    "SecurityControlId": "ACM.1",  
    "Parameters": {  
      "daysToExpiration": {  
        "ValueType": "CUSTOM",  
        "Value": {  
          "Integer": 15  
        }  
      }  
    }  
  }  
]
```

AWS CLI

Per aggiornare le politiche di configurazione

1. Per aggiornare le impostazioni in una politica di configurazione, esegui il [update-configuration-policy](#) comando dall'account amministratore delegato di Security Hub nella regione di residenza.
2. Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione che desideri aggiornare.
3. Fornisci valori aggiornati per i campi `configuration-policy` sottostanti. Facoltativamente, puoi anche fornire un motivo per l'aggiornamento.
4. Per aggiungere nuove associazioni per questa politica di configurazione, esegui il [start-configuration-policy-association](#) comando dall'account amministratore delegato di Security Hub nella regione di residenza. Per rimuovere una o più associazioni correnti, esegui il [start-configuration-policy-disassociation](#) comando dall'account amministratore delegato di Security Hub nella regione di residenza.
5. Per il `configuration-policy-identifier` campo, fornisci l'ARN o l'ID della politica di configurazione di cui desideri aggiornare le associazioni.

- Per il target campo, fornite gli account, le unità organizzative o l'ID root che desiderate associare o dissociare. Questa azione sostituisce le precedenti associazioni di policy per le unità organizzative o gli account specificati.

Note

Quando si esegue il `update-configuration-policy` comando, Security Hub sostituisce l'elenco completo dei `SecurityControlCustomParameters` campi `EnabledStandardIdentifiers`, `EnabledSecurityControlIdentifiers`, `DisabledSecurityControlIdentifiers`, e. Ogni volta che esegui questo comando, fornisci l'elenco completo degli standard che desideri abilitare e l'elenco completo dei controlli per i quali desideri abilitare o disabilitare e personalizzare i parametri.

Comando di esempio per aggiornare una politica di configurazione:

```
aws securityhub update-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--description "Updated configuration policy" \
--updated-reason "Disabling CloudWatch.1" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0","arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2","CloudWatch.1"],
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}}]}'
```

L'`StartConfigurationPolicyAssociationAPI` restituisce un campo chiamato `AssociationStatus`. Questo campo indica se un'associazione di politiche è in sospeso o in uno stato di successo o di fallimento. La modifica dello stato da a SUCCESS o FAILURE può richiedere fino a 24 ore. PENDING Per ulteriori informazioni sullo stato dell'associazione, vedere [Stato di associazione di una configurazione](#).

Eliminazione e dissociazione delle politiche di configurazione del Security Hub

L'account amministratore delegato può eliminare una politica di AWS Security Hub configurazione. In alternativa, l'account amministratore delegato può mantenere la politica di configurazione, ma dissociarla da account o unità organizzative (OU) specifici.

La sezione seguente illustra entrambe queste opzioni.

Eliminazione delle politiche di configurazione

Quando elimini una politica di configurazione, questa non esiste più per la tua organizzazione. Gli account di destinazione, le unità organizzative e la radice dell'organizzazione non possono più utilizzare la politica di configurazione. Le destinazioni associate a una politica di configurazione eliminata ereditano la politica di configurazione del genitore più vicino o vengono gestite automaticamente se il genitore più vicino è autogestito. Se si desidera che una destinazione utilizzi una configurazione diversa, è possibile associare la destinazione a una nuova politica di configurazione. Per ulteriori informazioni, consulta [Creazione e associazione dei criteri di configurazione del Security Hub](#).

Ti consigliamo di creare e associare almeno una politica di configurazione alla tua organizzazione per fornire una copertura di sicurezza adeguata.

Prima di poter eliminare una politica di configurazione, è necessario [dissociarla](#) dagli account, dalle unità organizzative o dalla radice a cui si applica attualmente.

Scegliete il metodo preferito e seguite i passaggi per eliminare una politica di configurazione.

Console

Per eliminare una politica di configurazione

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.

Accedi utilizzando le credenziali dell'account amministratore delegato di Security Hub nella regione di residenza.

2. Nel riquadro di navigazione, scegli Impostazioni e configurazione.
3. Scegliere la scheda Policy. Seleziona la politica di configurazione che desideri eliminare e scegli Elimina. Se la politica di configurazione è ancora associata a qualsiasi account o unità

organizzativa, ti viene richiesto di dissociare la politica da tali destinazioni prima di poterla eliminare.

4. Controlla il messaggio di conferma. Inserisci **confirm** e scegli Elimina.

API

Per eliminare una politica di configurazione

Richiama l'[DeleteConfigurationPolicy](#) API dall'account amministratore delegato di Security Hub nella regione di origine.

Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione che desideri eliminare. Se ricevi un `ConflictException` errore, la politica di configurazione si applica ancora agli account o alle unità organizzative della tua organizzazione. Per risolvere l'errore, dissocia la politica di configurazione da questi account o unità organizzative prima di provare a eliminarla.

Esempio di richiesta API per eliminare una politica di configurazione:

```
{
  "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Per eliminare una politica di configurazione

Esegui il [delete-configuration-policy](#) comando dall'account amministratore delegato di Security Hub nella regione di residenza.

Fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione che desideri eliminare. Se ricevi un `ConflictException` errore, la politica di configurazione si applica ancora agli account o alle unità organizzative della tua organizzazione. Per risolvere l'errore, dissocia la politica di configurazione da questi account o unità organizzative prima di provare a eliminarla.

```
aws securityhub --region us-east-1 delete-configuration-policy \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Dissociazione di una configurazione dagli account e dalle unità organizzative

Dall'account amministratore delegato, è possibile dissociare un account di destinazione, un'unità organizzativa o la directory principale da una politica di configurazione attualmente applicabile o da una configurazione autogestita. È possibile dissociare una destinazione solo da una configurazione applicata, non da una configurazione ereditata. Per modificare una configurazione ereditata, è possibile applicare una politica di configurazione o un comportamento autogestito all'account o all'unità organizzativa interessati. È inoltre possibile applicare una nuova politica di configurazione, che include le modifiche desiderate, al genitore più vicino.

La disassociazione non elimina una politica di configurazione. La politica viene mantenuta nel tuo account, quindi puoi associarla ad altri obiettivi della tua organizzazione. Una volta completata la dissociazione, un obiettivo interessato eredita la politica di configurazione o il comportamento autogestito del genitore più vicino. Se non esiste una configurazione ereditabile, una destinazione mantiene le impostazioni che aveva prima della disassociazione ma viene gestita automaticamente.

Scegli il metodo preferito e segui i passaggi per dissociare un account, un'unità organizzativa o un utente root dalla configurazione corrente.

Console

Per dissociare un account o un'unità organizzativa dalla configurazione corrente

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.
Accedi utilizzando le credenziali dell'account amministratore delegato di Security Hub nella regione di residenza.
2. Nel riquadro di navigazione, scegli Impostazioni e configurazione.
3. Nella scheda Organizations, seleziona l'account, l'unità organizzativa o la radice che desideri dissociare dalla configurazione corrente. Scegli Modifica.
4. Nella pagina Definisci configurazione, per Gestione, scegli Politica applicata se desideri che l'amministratore delegato sia in grado di applicare le politiche direttamente alla destinazione. Scegli Inherited se desideri che la destinazione erediti la configurazione del suo elemento principale più vicino. In entrambi i casi, l'amministratore delegato controlla le impostazioni per

la destinazione. Scegli Autogestito se desideri che l'account o l'unità organizzativa controllino le proprie impostazioni.

5. Dopo aver esaminato le modifiche, scegli Avanti e Applica. Questa azione sostituisce le configurazioni esistenti di tutti gli account o le unità organizzative che rientrano nell'ambito, se tali configurazioni sono in conflitto con le selezioni correnti.

API

Per dissociare un account o un'unità organizzativa dalla configurazione corrente

1. Richiama l'[StartConfigurationPolicyDisassociation](#) API dall'account amministratore delegato di Security Hub nella regione di origine.
2. Per `ConfigurationPolicyIdentifier`, fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione da cui desideri dissociare. Inserisci questo campo `SELF_MANAGED_SECURITY_HUB` per dissociare il comportamento autogestito.
3. Per `Target`, fornisci gli account, le unità organizzative o la radice che desideri separare da questa politica di configurazione.

Esempio di richiesta API per dissociare una politica di configurazione:

```
{
  "ConfigurationPolicyIdentifier": "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Target": {"RootId": "r-f6g7h8i9j0example"}
}
```

AWS CLI

Per dissociare un account o un'unità organizzativa dalla configurazione corrente

1. Esegui il [start-configuration-policy-disassociation](#) comando dall'account amministratore delegato di Security Hub nella regione di residenza.
2. Per `configuration-policy-identifier`, fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione da cui desideri dissociare. Inserisci questo campo `SELF_MANAGED_SECURITY_HUB` per dissociare il comportamento autogestito.

3. Per target, fornisci gli account, le unità organizzative o la radice che desideri separare da questa politica di configurazione.

Esempio di comando per dissociare una politica di configurazione:

```
aws securityhub --region us-east-1 start-configuration-policy-disassociation \
--configuration-policy-identifier "arn:aws:securityhub:us-
east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" \
--target '{"RootId": "r-f6g7h8i9j0example"}'
```

Configurazione centrale nel contesto di uno standard o di un controllo

È possibile utilizzare la configurazione centrale dalla pagina Configurazione della AWS Security Hub console o nel contesto di uno standard di sicurezza o di un controllo di sicurezza specifici. L'utilizzo di questa funzionalità nel contesto consente di configurare standard e controlli all'interno dell'organizzazione in modo integrato con i flussi di lavoro esistenti. Inoltre, man mano che visualizzi i risultati, puoi scoprire quali standard e controlli sono più pertinenti per il tuo ambiente e configurarli allo stesso tempo.

La configurazione contestuale è disponibile solo sulla console Security Hub. A livello di codice, è necessario richiamare l'[UpdateConfigurationPolicy](#) API per modificare il modo in cui gli standard o i controlli specifici sono configurati nell'organizzazione.

Configurazione di uno standard di sicurezza nel contesto

Segui i passaggi per configurare uno standard di sicurezza contestualmente tramite la configurazione centrale.

Per configurare uno standard di sicurezza nel contesto (solo console)

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).

Accedi utilizzando le credenziali dell'account amministratore delegato di Security Hub nella regione di residenza.

2. Nel riquadro di navigazione, scegli Standard di sicurezza.

3. Per lo standard che desideri configurare, scegli Configura. Puoi anche scegliere uno standard specifico e quindi scegliere Configura dalla pagina dei dettagli dello standard. La console elenca le policy di configurazione esistenti del Security Hub (policy di configurazione) e lo stato di questo standard in ciascuna di esse.
4. Scegli le opzioni per abilitare o disabilitare lo standard in ogni politica di configurazione.
5. Dopo aver apportato le modifiche, scegli Avanti.
6. Controlla le modifiche e scegli Applica. Questa azione ha effetto su tutti gli account e le unità organizzative associati a una politica di configurazione. La configurazione ha effetto nella regione di origine e in tutte le regioni collegate.

Configurazione di un controllo di sicurezza nel contesto

Segui i passaggi per configurare un controllo di sicurezza contestualmente tramite la configurazione centrale.

Per configurare un controllo di sicurezza nel contesto (solo console)

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).

Accedi utilizzando le credenziali dell'account amministratore delegato di Security Hub nella regione di residenza.

2. Nel riquadro di navigazione, scegli Controlli.
3. Scegli un controllo specifico, quindi scegli Configura. La console elenca le politiche di configurazione correnti e lo stato di questo controllo in ciascuna di esse.
4. Scegli le opzioni per abilitare o disabilitare il controllo in ogni politica di configurazione. Puoi anche scegliere di personalizzare i parametri di controllo.
5. Dopo aver apportato le modifiche, scegli Avanti.
6. Controlla le modifiche e scegli Applica. Questa azione ha effetto su tutti gli account e le unità organizzative associati a una politica di configurazione. La configurazione ha effetto nella regione di origine e in tutte le regioni collegate.

Smetti di usare la configurazione centrale

Quando si smette di utilizzare la configurazione centrale in AWS Security Hub, l'amministratore delegato perde la possibilità di configurare Security Hub, gli standard di sicurezza e i controlli

di sicurezza su più Account AWS unità organizzative (OU) e Regioni AWS. Invece, gli account dell'organizzazione devono configurare la maggior parte delle proprie impostazioni separatamente in ciascuna regione.

⚠ Important

Prima di poter smettere di utilizzare la configurazione centrale, è necessario [dissociare gli account e](#) le unità organizzative dalla configurazione corrente, che si tratti di una politica di configurazione o di un comportamento autogestito.

Prima di poter smettere di usare la configurazione centrale, è necessario [eliminare anche le politiche di configurazione](#).

Quando si interrompe la configurazione centrale, si verificano le seguenti modifiche:

- L'amministratore delegato non può più creare politiche di configurazione per l'organizzazione.
- Gli account a cui era stata applicata o ereditata una politica di configurazione mantengono le impostazioni correnti, ma si gestiscono automaticamente.
- L'organizzazione passa alla configurazione locale. Nella configurazione locale, la maggior parte delle impostazioni di Security Hub deve essere configurata separatamente in ogni account e regione dell'organizzazione. L'amministratore delegato può scegliere di abilitare automaticamente Security Hub, [gli standard di sicurezza predefiniti](#) e tutti i controlli che fanno parte degli standard predefiniti nei nuovi account dell'organizzazione. Gli standard predefiniti sono AWS Foundational Security Best Practices (FSBP) e Center for Internet Security (CIS) Foundations Benchmark v1.2.0. AWS Queste impostazioni hanno effetto solo nella regione corrente e influiscono solo sui nuovi account dell'organizzazione. L'amministratore delegato non può modificare gli standard predefiniti. La configurazione locale non supporta l'uso di politiche di configurazione o la configurazione a livello di unità organizzativa.

L'identità dell'account amministratore delegato rimane la stessa quando si smette di utilizzare la configurazione centrale. Anche la regione d'origine e le regioni collegate rimangono invariate (la regione d'origine è ora denominata regione di aggregazione e può essere utilizzata per trovare aggregazioni).

Scegli il tuo metodo preferito e segui i passaggi per smettere di usare la configurazione centrale e passare alla configurazione locale.

Security Hub console

Per smettere di usare la configurazione centrale

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.

Accedi utilizzando le credenziali dell'account amministratore delegato di Security Hub nella regione di residenza.
2. Nel pannello di navigazione, scegli Impostazioni e configurazione.
3. Nella sezione Panoramica, scegli Modifica.
4. Nella casella Modifica configurazione dell'organizzazione, scegli Configurazione locale. Se non l'hai già fatto, ti viene richiesto di annullare l'associazione ed eliminare le politiche di configurazione correnti prima di poter interrompere la configurazione centrale. Gli account o le unità organizzative designati come autogestiti devono essere dissociati dalla relativa configurazione autogestita. È possibile eseguire questa operazione nella console [modificando il tipo di gestione](#) di ogni account o unità organizzativa autogestito in Gestito centralmente e eredita dalla mia organizzazione.
5. Facoltativamente, selezionare le impostazioni predefinite di configurazione locale per i nuovi account dell'organizzazione.
6. Scegli Conferma.

Security Hub API

Per smettere di usare la configurazione centrale

1. Invoca l'[UpdateOrganizationConfiguration](#) API.
2. Imposta il ConfigurationType campo nell'OrganizationConfiguration oggetto su. LOCAL L'API restituisce un errore se sono presenti politiche di configurazione o associazioni di politiche esistenti. Per dissociare una politica di configurazione, richiama l'StartConfigurationPolicyDisassociation API. Per eliminare una politica di configurazione, richiama l'API. DeleteConfigurationPolicy
3. Se desideri abilitare automaticamente Security Hub nei nuovi account dell'organizzazione, imposta il AutoEnable campo su true. Per impostazione predefinita, il valore di questo campo è false e Security Hub non viene abilitato automaticamente nei nuovi account dell'organizzazione. Facoltativamente, se desideri abilitare automaticamente gli standard di sicurezza predefiniti nei nuovi account dell'organizzazione, imposta il

AutoEnableStandards campo su. DEFAULT Questo è il valore predefinito. Se non desideri abilitare automaticamente gli standard di sicurezza predefiniti nei nuovi account dell'organizzazione, imposta il AutoEnableStandards campo suNONE.

Esempio di richiesta API:

```
{
  "AutoEnable": true,
  "OrganizationConfiguration": {
    "ConfigurationType" : "LOCAL"
  }
}
```

AWS CLI

Per smettere di usare la configurazione centrale

1. Esegui il comando [update-organization-configuration](#).
2. Imposta il ConfigurationType campo nell'organization-configurationoggetto suLOCAL. Il comando restituisce un errore se sono presenti criteri di configurazione o associazioni di criteri esistenti. Per dissociare una politica di configurazione, esegui il start-configuration-policy-disassociation comando. Per eliminare una politica di configurazione, esegui il delete-configuration-policy comando.
3. Se desideri abilitare automaticamente Security Hub nei nuovi account dell'organizzazione, includi il auto-enable parametro. Per impostazione predefinita, il valore di questo parametro è no-auto-enable e Security Hub non viene abilitato automaticamente nei nuovi account dell'organizzazione. Facoltativamente, se desideri abilitare automaticamente gli standard di sicurezza predefiniti nei nuovi account dell'organizzazione, imposta il auto-enable-standards campo su. DEFAULT Questo è il valore predefinito. Se non desideri abilitare automaticamente gli standard di sicurezza predefiniti nei nuovi account dell'organizzazione, imposta il auto-enable-standards campo suNONE.

```
aws securityhub --region us-east-1 update-organization-configuration \
--auto-enable \
--organization-configuration '{"ConfigurationType": "LOCAL"}'
```

Gestione degli account degli amministratori e dei membri

Se il tuo AWS ambiente ha più account, puoi trattare gli account che utilizzano AWS Security Hub come account membro e associarli a un singolo account amministratore. L'amministratore può monitorare il livello di sicurezza generale dell'utente e intraprendere [le azioni consentite](#) sugli account dei membri. L'amministratore può anche eseguire varie attività di gestione e amministrazione degli account su larga scala, come il monitoraggio dei costi di utilizzo stimati e la valutazione delle quote degli account.

È possibile associare gli account dei membri a un amministratore in due modi: integrando Security Hub con AWS Organizations o inviando e accettando manualmente gli inviti di iscrizione in Security Hub.

Gestione degli account con AWS Organizations

AWS Organizations è un servizio globale di gestione degli account che consente AWS agli amministratori di consolidare e gestire più account. Account AWS Fornisce funzionalità di gestione degli account e fatturazione consolidata progettate per supportare le esigenze di budget, sicurezza e conformità. È offerto senza costi aggiuntivi e si integra con più piattaforme Servizi AWS, tra cui AWS Security Hub, Amazon Macie e Amazon GuardDuty. Per ulteriori informazioni, consulta la [AWS Organizations Guida per l'utente](#).

Quando si integra Security Hub e AWS Organizations, l'account di gestione Organizations designa un amministratore delegato di Security Hub. Security Hub viene abilitato automaticamente nell'account amministratore delegato Regione AWS in cui è stato designato.

Dopo aver designato un amministratore delegato, consigliamo di gestire gli account in Security Hub con configurazione [centralizzata](#). Questo è il modo più efficiente per personalizzare Security Hub e garantire un'adeguata copertura di sicurezza per l'organizzazione.

La configurazione centrale consente all'amministratore delegato di personalizzare Security Hub su più account e regioni dell'organizzazione anziché configurare regione per regione. È possibile creare una politica di configurazione per l'intera organizzazione o creare politiche di configurazione diverse per account e unità organizzative diversi. Le policy specificano se Security Hub è abilitato o disabilitato negli account associati e quali standard e controlli di sicurezza sono abilitati.

L'amministratore delegato può designare gli account come gestiti centralmente o autogestiti. Gli account gestiti centralmente sono configurabili solo dall'amministratore delegato. Gli account autogestiti possono specificare le proprie impostazioni.

Se non si attiva la configurazione centralizzata, l'amministratore delegato ha una capacità più limitata di configurare Security Hub, chiamata configurazione locale. Nella configurazione locale, l'amministratore delegato può abilitare automaticamente Security Hub e [gli standard di sicurezza predefiniti](#) nei nuovi account dell'organizzazione nella regione corrente. Tuttavia, gli account esistenti non utilizzano queste impostazioni, quindi è possibile che si verifichi una variazione della configurazione dopo che un account si unisce all'organizzazione.

Oltre a queste nuove impostazioni dell'account, la configurazione locale è specifica dell'account e della regione. Ogni account dell'organizzazione deve configurare il servizio, gli standard e i controlli Security Hub separatamente in ciascuna regione. Inoltre, la configurazione locale non supporta l'uso di politiche di configurazione.

Gestione manuale degli account tramite invito

È necessario gestire manualmente gli account dei membri su invito in Security Hub se si dispone di un account autonomo o se non si esegue l'integrazione con Organizations. Un account autonomo non può integrarsi con Organizations, quindi è necessario gestirlo manualmente. Ti consigliamo di integrare AWS Organizations e utilizzare la configurazione centrale se aggiungi altri account in futuro.

Quando si utilizza la gestione manuale degli account, si designa un account come amministratore del Security Hub. L'account amministratore può visualizzare i dati negli account dei membri e intraprendere determinate azioni in base ai risultati degli account dei membri. L'amministratore del Security Hub invita altri account a diventare account membro e la relazione amministratore-membro viene stabilita quando un potenziale account membro accetta l'invito.

La gestione manuale degli account non supporta l'uso di politiche di configurazione. Senza criteri di configurazione, l'amministratore non può personalizzare centralmente Security Hub configurando impostazioni variabili per account diversi. Invece, ogni account dell'organizzazione deve abilitare e configurare Security Hub separatamente in ogni regione. Ciò può rendere più difficile e dispendioso in termini di tempo garantire un'adeguata copertura di sicurezza in tutti gli account e le regioni in cui si utilizza Security Hub. Ciò può anche causare variazioni nella configurazione, in quanto gli account membri possono specificare le proprie impostazioni senza alcun intervento da parte dell'amministratore.

Per gestire gli account su invito, consulta [Gestione degli account tramite invito](#).

Gestione degli account con AWS Organizations

Puoi eseguire l'integrazione AWS Security Hub e AWS Organizations quindi gestire Security Hub per gli account della tua organizzazione.

Per integrare Security Hub con AWS Organizations, crei un'organizzazione in AWS Organizations. L'account di gestione Organizations designa un account come amministratore delegato di Security Hub per l'organizzazione. L'amministratore delegato può quindi abilitare Security Hub per altri account dell'organizzazione, aggiungere tali account come account membro di Security Hub e intraprendere le azioni consentite sugli account dei membri. L'amministratore delegato di Security Hub può abilitare e gestire Security Hub per un massimo di 10.000 account membri.

L'estensione delle capacità di configurazione dell'amministratore delegato dipende dall'utilizzo o meno della configurazione [centrale](#). Con la configurazione centralizzata abilitata, non è necessario configurare Security Hub separatamente in ogni account membro e Regione AWS. L'amministratore delegato può applicare impostazioni specifiche del Security Hub in account membri e unità organizzative (OU) specifici in tutte le regioni.

L'account amministratore delegato di Security Hub può eseguire le seguenti azioni sugli account dei membri:

- Se utilizzi la configurazione centrale, configura centralmente Security Hub per gli account dei membri e le unità organizzative creando politiche di configurazione di Security Hub. Le policy di configurazione possono essere utilizzate per abilitare e disabilitare Security Hub, abilitare e disabilitare gli standard e abilitare e disabilitare i controlli.
- Tratta automaticamente i nuovi account come account membri del Security Hub quando entrano a far parte dell'organizzazione. Se si utilizza la configurazione centrale, una politica di configurazione associata a un'unità organizzativa include account nuovi e esistenti che fanno parte dell'unità organizzativa.
- Tratta gli account aziendali esistenti come account membri del Security Hub. Ciò avviene automaticamente se si utilizza la configurazione centrale.
- Dissocia gli account dei membri che appartengono all'organizzazione. Se si utilizza la configurazione centrale, è possibile dissociare un account membro solo dopo averlo designato come autogestito. In alternativa, è possibile associare una politica di configurazione che disabiliti Security Hub a specifici account membro gestiti centralmente.

Per un elenco completo delle azioni che l'amministratore delegato può eseguire sugli account dei membri, vedere. [Azioni consentite per gli account](#)

Gli argomenti di questa sezione spiegano come integrare Security Hub con AWS Organizations e come gestire Security Hub per gli account di un'organizzazione. Ove pertinente, ogni sezione identifica i vantaggi e le differenze di gestione per gli utenti della configurazione centrale.

Argomenti

- [Integrazione del Security Hub con AWS Organizations](#)
- [Attivazione automatica di Security Hub nei nuovi account dell'organizzazione](#)
- [Abilitazione manuale di Security Hub nei nuovi account dell'organizzazione](#)
- [Dissociazione degli account dei membri dall'organizzazione](#)
- [Disattivazione dell'integrazione del Security Hub con AWS Organizations](#)

Integrazione del Security Hub con AWS Organizations

Per integrare AWS Security Hub e AWS Organizations, è necessario creare un'organizzazione in Organizations e utilizzare l'account di gestione dell'organizzazione per designare un account amministratore delegato di Security Hub. L'amministratore delegato può quindi abilitare Security Hub per gli account dei membri, visualizzare i dati negli account dei membri ed eseguire altre [azioni consentite](#) sugli account dei membri.

Se si utilizza la [configurazione centrale](#), l'amministratore delegato può anche creare politiche di configurazione del Security Hub che specificano come configurare il servizio, gli standard e i controlli di Security Hub negli account dell'organizzazione.

Creazione di un'organizzazione

Un'organizzazione è un'entità creata per consolidare la propria Account AWS in modo da poterla amministrare come una singola unità.

Puoi creare un'organizzazione utilizzando la AWS Organizations console o utilizzando un comando proveniente da AWS CLI o da una delle API SDK. Per istruzioni dettagliate, consulta [Creare un'organizzazione nella Guida](#) per l'AWS Organizations utente.

Puoi utilizzarlo AWS Organizations per visualizzare e gestire centralmente tutti gli account all'interno della tua organizzazione. Un'organizzazione ha un account di gestione insieme a zero o più account

membri. È possibile organizzare gli account in una struttura gerarchica ad albero con una radice nella parte superiore e unità organizzative (OU) annidate sotto la radice. Ogni account può trovarsi direttamente sotto la radice o collocato in una delle unità organizzative della gerarchia. Un'unità organizzativa è un contenitore per account specifici. Ad esempio, è possibile creare un'unità organizzativa finanziaria che includa tutti i conti relativi alle operazioni finanziarie.

Consigli per la scelta dell'amministratore delegato del Security Hub

Se disponi di un account amministratore dopo la procedura di invito manuale e stai passando alla gestione degli account con AWS Organizations, Security Hub consiglia di designare quell'account come amministratore delegato del Security Hub.

Non è necessario designare l'account di gestione dell'organizzazione come amministratore delegato del Security Hub. Questo perché è probabile che gli utenti che hanno accesso all'account di gestione dell'organizzazione per gestire la fatturazione siano diversi dagli utenti che devono accedere a Security Hub per la gestione della sicurezza.

Si consiglia di utilizzare lo stesso amministratore delegato in tutte le regioni. Se opti per la configurazione centralizzata, Security Hub designa automaticamente lo stesso amministratore delegato nella tua regione d'origine e in tutte le regioni collegate.

Verifica le autorizzazioni per configurare l'amministratore delegato del Security Hub

Per designare e rimuovere un account amministratore delegato di Security Hub, l'account di gestione dell'organizzazione deve disporre delle `DisableOrganizationAdminAccount` autorizzazioni `EnableOrganizationAdminAccount` e delle azioni in Security Hub. L'account di gestione Organizations deve inoltre disporre delle autorizzazioni amministrative per Organizations.

Per concedere tutte le autorizzazioni richieste, collega le seguenti politiche gestite da Security Hub al principale IAM per l'account di gestione dell'organizzazione:

- [AWSSecurityHubFullAccess](#)
- [AWSSecurityHubOrganizationsAccess](#)

Designazione dell'amministratore delegato del Security Hub

Per designare l'account amministratore delegato di Security Hub, è possibile utilizzare la console Security Hub, l'API Security Hub oppure. AWS CLISecurity Hub imposta l'amministratore delegato

Regione AWS solo nell'area corrente ed è necessario ripetere l'azione in altre regioni. Se inizi a utilizzare la configurazione centrale, Security Hub imposta automaticamente lo stesso amministratore delegato nella regione di origine e nelle regioni collegate.

L'account di gestione dell'organizzazione non deve abilitare Security Hub per designare l'account amministratore delegato di Security Hub.

È consigliabile che l'account di gestione dell'organizzazione non sia l'account amministratore delegato di Security Hub. Tuttavia, se si sceglie l'account di gestione dell'organizzazione come amministratore delegato di Security Hub, l'account di gestione deve avere Security Hub abilitato. Se l'account di gestione non ha Security Hub abilitato, è necessario abilitare Security Hub manualmente. Security Hub non può essere abilitato automaticamente per l'account di gestione dell'organizzazione.

Note

È necessario designare l'amministratore delegato del Security Hub utilizzando uno dei seguenti metodi. La designazione dell'amministratore delegato di Security Hub con le API Organizations non si riflette in Security Hub.

Scegli il tuo metodo preferito e segui i passaggi per designare l'account amministratore delegato di Security Hub.

Security Hub console

Per designare l'amministratore delegato del Security Hub durante l'onboarding

1. [Aprire la console all'indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/) **AWS Security Hub**.
2. Scegli **Vai a Security Hub**. Ti viene richiesto di accedere all'account di gestione dell'organizzazione.
3. Nella pagina **Designa amministratore delegato**, nella sezione **Account amministratore delegato**, specifica l'account amministratore delegato. Ti consigliamo di scegliere lo stesso amministratore delegato che hai impostato per altri AWS servizi di sicurezza e conformità.
4. Scegli **Imposta amministratore delegato**. Ti viene richiesto di accedere all'account amministratore delegato (se non lo sei già) per continuare l'onboarding con la configurazione centrale. Se non desideri avviare la configurazione centralizzata, scegli **Annulla**. L'amministratore delegato è impostato, ma non stai ancora utilizzando la configurazione centrale.

Per designare l'amministratore delegato del Security Hub dalla pagina Impostazioni

1. [Aprire la AWS Security Hub console all'indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione Security Hub, scegli Impostazioni. Quindi scegli Generale.
3. Se al momento è assegnato un account amministratore di Security Hub, prima di poter designare un nuovo account, è necessario rimuovere l'account corrente.

In Amministratore delegato, per rimuovere l'account corrente, scegli Rimuovi.

4. Inserisci l'ID dell'account che desideri designare come account amministratore del Security Hub.

È necessario designare lo stesso account amministratore del Security Hub in tutte le regioni. Se si designa un account diverso da quello designato in altre regioni, la console restituisce un errore.

5. Scegli Delega.

Security Hub API

Richiama l'[EnableOrganizationAdminAccount](#) API dall'account di gestione dell'organizzazione. Fornisci l' Account AWS ID dell'account amministratore delegato di Security Hub.

AWS CLI

Esegui il [enable-organization-admin-account](#) comando dall'account di gestione dell'organizzazione. Fornisci l' Account AWS ID dell'account amministratore delegato di Security Hub.

Comando di esempio:

```
aws securityhub enable-organization-admin-account --admin-account-id 777788889999
```

Rimozione dell'amministratore delegato del Security Hub

Warning

Quando si utilizza la configurazione centrale, non è possibile utilizzare la console di Security Hub o le API di Security Hub per modificare o rimuovere l'account amministratore delegato. Se l'account di gestione dell'organizzazione utilizza la AWS Organizations console o le

AWS Organizations API per modificare o rimuovere l'amministratore delegato di Security Hub, Security Hub interrompe automaticamente la configurazione centrale ed elimina i criteri di configurazione e le associazioni di policy. Gli account dei membri mantengono le configurazioni che avevano prima della modifica o della rimozione dell'amministratore delegato.

Solo l'account di gestione dell'organizzazione può rimuovere l'account amministratore delegato di Security Hub.

Per cambiare l'amministratore delegato di Security Hub, è necessario prima rimuovere l'account amministratore delegato corrente e quindi designarne uno nuovo.

Se si utilizza la console Security Hub per rimuovere l'amministratore delegato in una regione, l'amministratore delegato viene rimosso automaticamente in tutte le regioni.

L'API Security Hub rimuove solo l'account amministratore delegato di Security Hub dalla regione in cui viene emessa la chiamata o il comando API. È necessario ripetere l'azione in altre regioni.

Se si utilizza l'API Organizations per rimuovere l'account amministratore delegato di Security Hub, questo viene rimosso automaticamente in tutte le regioni.

Rimozione dell'amministratore delegato del Security Hub (Organizations API, AWS CLI)

È possibile utilizzare Organizations per rimuovere l'amministratore delegato del Security Hub in tutte le regioni.

Se si utilizza la configurazione centrale per gestire gli account, la rimozione dell'account amministratore delegato comporta l'eliminazione delle politiche di configurazione e delle associazioni di policy. Gli account membro mantengono le configurazioni che avevano prima della modifica o della rimozione dell'amministratore delegato. Tuttavia, questi account non possono più essere gestiti dall'account amministratore delegato rimosso. Diventano account autogestiti che devono essere configurati separatamente in ciascuna regione.

Scegli il tuo metodo preferito e segui le istruzioni per rimuovere l'account amministratore delegato di Security Hub con AWS Organizations.

AWS Organizations API

Per rimuovere l'amministratore delegato del Security Hub

Invoca l'API. [DeregisterDelegatedAdministrator](#) Fornisci l'ID account dell'account amministratore delegato e il responsabile del servizio per Security Hub, che è `securityhub.amazonaws.com`.

AWS CLI

Per rimuovere l'amministratore delegato del Security Hub

Esegui il comando [deregister-delegated-administrator](#). Fornisci l'ID account dell'account amministratore delegato e il responsabile del servizio per Security Hub, che è `securityhub.amazonaws.com`.

```
aws organizations deregister-delegated-administrator --account-id <admin account ID>
--service-principal <Security Hub service principal>
```

Esempio

```
aws organizations deregister-delegated-administrator --account-id 123456789012 --
service-principal securityhub.amazonaws.com
```

Rimozione dell'amministratore delegato di Security Hub (console Security Hub)

È possibile utilizzare la console Security Hub per rimuovere l'amministratore delegato del Security Hub in tutte le regioni.

Quando l'account amministratore delegato di Security Hub viene rimosso, gli account dei membri vengono dissociati dall'account amministratore delegato di Security Hub rimosso.

Security Hub è ancora abilitato negli account dei membri. Diventano account autonomi fino a quando un nuovo amministratore del Security Hub non li abilita come account membro.

Se l'account di gestione dell'organizzazione non è un account abilitato in Security Hub, utilizza l'opzione nella pagina Benvenuto in Security Hub.

Per rimuovere l'account amministratore delegato di Security Hub dalla pagina di benvenuto in Security Hub

1. Aprire la AWS Security Hub console all'indirizzo <https://console.aws.amazon.com/securityhub/>.
2. Scegli Vai a Security Hub.
3. In Amministratore delegato, scegli Rimuovi.

Se l'account di gestione dell'organizzazione è un account abilitato in Security Hub, utilizza l'opzione nella scheda Generale della pagina Impostazioni.

Per rimuovere l'account amministratore delegato di Security Hub dalla pagina Impostazioni

1. Aprire la AWS Security Hub console all'indirizzo <https://console.aws.amazon.com/securityhub/>.
2. Nel riquadro di navigazione Security Hub, scegli Impostazioni. Quindi scegli Generale.
3. In Amministratore delegato, scegli Rimuovi.

Rimozione dell'amministratore delegato di Security Hub (Security Hub API, AWS CLI)

È possibile utilizzare l'API Security Hub o le operazioni Security Hub per AWS CLI rimuovere l'amministratore delegato del Security Hub. Quando si rimuove l'amministratore delegato con uno di questi metodi, questo viene rimosso solo nella regione in cui è stata emessa la chiamata o il comando API. Security Hub non aggiorna le altre regioni e non rimuove l'account amministratore delegato in AWS Organizations.

Scegli il tuo metodo preferito e segui questi passaggi per rimuovere l'account amministratore delegato di Security Hub con Security Hub.

Security Hub API

Per rimuovere l'amministratore delegato del Security Hub

Utilizzando le credenziali dell'account di gestione dell'organizzazione, richiama l'API.

[DisableOrganizationAdminAccount](#) Fornisci l'ID account dell'account amministratore delegato di Security Hub.

AWS CLI

Per rimuovere l'amministratore delegato del Security Hub

Utilizzando le credenziali dell'account di gestione dell'organizzazione, esegui il [disable-organization-admin-account](#) comando. Fornisci l'ID account dell'account amministratore delegato di Security Hub.

```
aws securityhub disable-organization-admin-account --admin-account-id <admin account ID>
```

Esempio

```
aws securityhub disable-organization-admin-account --admin-account-id 123456789012
```

Attivazione automatica di Security Hub nei nuovi account dell'organizzazione

Quando nuovi account si aggiungono alla tua organizzazione, vengono aggiunti all'elenco nella pagina Account della AWS Security Hub console. Per gli account dell'organizzazione, Tipo è Per organizzazione. Per impostazione predefinita, i nuovi account non diventano membri del Security Hub quando entrano a far parte dell'organizzazione. Il loro stato è Non membro. L'account amministratore delegato può aggiungere automaticamente nuovi account come membri e abilitare Security Hub in questi account quando entrano a far parte dell'organizzazione.

Note

Sebbene molti Regioni AWS siano attivi per impostazione predefinita per le tue Account AWS, alcune regioni devono essere attivate manualmente. In questo documento, queste regioni sono chiamate regioni opt-in. Per abilitare automaticamente Security Hub in un nuovo account in una regione opt-in, l'account deve prima avere quella regione attivata. Solo il proprietario dell'account può attivare la regione di attivazione. Per ulteriori informazioni sulle regioni che richiedono l'iscrizione, vedi [Specificare quali possono essere utilizzate dal Regioni AWS tuo account](#).

Questo processo è diverso a seconda che si utilizzi la configurazione centrale (consigliata) o la configurazione locale.

Abilitazione automatica di nuovi account aziendali (configurazione centrale)

Se si utilizza la [configurazione centrale](#), è possibile abilitare automaticamente Security Hub negli account dell'organizzazione nuovi ed esistenti creando una politica di configurazione in cui sia abilitato Security Hub. È quindi possibile associare la politica alla radice dell'organizzazione o alle unità organizzative (OU) specifiche.

Se si associa una politica di configurazione in cui Security Hub è abilitato a un'unità organizzativa specifica, Security Hub viene automaticamente abilitato in tutti gli account (esistenti e nuovi) che appartengono a quell'unità organizzativa. I nuovi account che non appartengono all'unità

organizzativa vengono gestiti automaticamente e non hanno Security Hub abilitato automaticamente. Se si associa una politica di configurazione in cui Security Hub è abilitato alla root, Security Hub viene automaticamente abilitato in tutti gli account (esistenti e nuovi) che entrano a far parte dell'organizzazione. Le eccezioni si verificano se un account utilizza una politica diversa tramite l'applicazione o l'ereditarietà o è autogestito.

Nella politica di configurazione, è inoltre possibile definire quali standard e controlli di sicurezza devono essere abilitati nell'unità organizzativa. Per generare risultati di controllo per gli standard abilitati, gli account nell'unità organizzativa devono essere AWS Config abilitati e configurati per registrare le risorse richieste. Per ulteriori informazioni sulla AWS Config registrazione, vedere [Attivazione e configurazione AWS Config](#).

Per istruzioni sulla creazione di una politica di configurazione, vedere [Creazione e associazione dei criteri di configurazione del Security Hub](#).

Abilitazione automatica di nuovi account aziendali (configurazione locale)

Quando si utilizza la configurazione locale e si attiva l'abilitazione automatica, Security Hub aggiunge nuovi account dell'organizzazione come membri e abilita Security Hub in essi nella regione corrente. Le altre regioni non sono interessate. Inoltre, l'attivazione dell'abilitazione automatica non abilita Security Hub negli account aziendali esistenti, a meno che non siano già stati aggiunti come account membro.

Dopo aver attivato l'abilitazione automatica, [gli standard di sicurezza predefiniti](#) vengono abilitati automaticamente anche per i nuovi account nella regione corrente quando entrano a far parte dell'organizzazione. Gli standard predefiniti sono AWS Foundational Security Best Practices (FSBP) e Center for Internet Security (CIS) Foundations Benchmark v1.2.0. AWS Non è possibile modificare gli standard predefiniti. Se desideri abilitare altri standard in tutta l'organizzazione o abilitare gli standard per determinati account e unità organizzative, ti consigliamo di utilizzare la configurazione centrale.

Per generare risultati di controllo per gli standard predefiniti (e altri standard abilitati), gli account dell'organizzazione devono essere AWS Config abilitati e configurati per registrare le risorse richieste. Per ulteriori informazioni sulla AWS Config registrazione, vedere [Attivazione e configurazione AWS Config](#).

Scegli il tuo metodo preferito e segui i passaggi per abilitare automaticamente Security Hub nei nuovi account dell'organizzazione. Queste istruzioni si applicano solo se utilizzi la configurazione locale.

Security Hub console

Per abilitare automaticamente i nuovi account dell'organizzazione come membri del Security Hub

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).

Sign utilizza le credenziali dell'account amministratore delegato.

2. Nel pannello di navigazione di Security Hub, in Impostazioni, scegli Configurazione.
3. Nella sezione Account, attiva l'attivazione automatica degli account.

Security Hub API

Per abilitare automaticamente i nuovi account dell'organizzazione come membri del Security Hub

Richiama l'[UpdateOrganizationConfiguration](#) API dall'account amministratore delegato. Imposta il `AutoEnable` campo su `true` per abilitare automaticamente Security Hub nei nuovi account dell'organizzazione.

AWS CLI

Per abilitare automaticamente i nuovi account dell'organizzazione come membri del Security Hub

Esegui il [update-organization-configuration](#) comando dall'account amministratore delegato. Includi il `auto-enable` parametro per abilitare automaticamente Security Hub nei nuovi account dell'organizzazione.

```
aws securityhub update-organization-configuration --auto-enable
```

Abilitazione manuale di Security Hub nei nuovi account dell'organizzazione

Se non abiliti automaticamente Security Hub nei nuovi account dell'organizzazione quando entrano a far parte dell'organizzazione, puoi aggiungere tali account come membri e abilitare Security Hub manualmente dopo che si sono uniti all'organizzazione. È inoltre necessario abilitare manualmente Security Hub in quanto in precedenza Account AWS si è dissociati da un'organizzazione.

Note

Questa sezione non si applica a te se utilizzi la [configurazione centrale](#). Se si utilizza la configurazione centrale, è possibile creare policy di configurazione che abilitino Security Hub

in account membri e unità organizzative (OU) specifici. È inoltre possibile abilitare standard e controlli specifici in tali account e unità organizzative.

Non puoi abilitare Security Hub in un account se è già un account membro di un'altra organizzazione.

Inoltre, non puoi abilitare Security Hub in un account attualmente sospeso. Se tenti di abilitare il servizio in un account sospeso, lo stato dell'account cambia in Account sospeso.

- Se l'account non ha Security Hub abilitato, Security Hub è abilitato in quell'account. Nell'account sono abilitati anche lo standard AWS Foundational Security Best Practices (FSBP) e CIS AWS Foundations Benchmark v1.2.0, a meno che non vengano disattivati gli standard di sicurezza predefiniti.

L'eccezione è rappresentata dall'account di gestione Organizations. Security Hub non può essere abilitato automaticamente nell'account di gestione Organizations. È necessario abilitare manualmente Security Hub nell'account di gestione Organizations prima di poterlo aggiungere come account membro.

- Se l'account ha già abilitato Security Hub, Security Hub non apporta altre modifiche all'account. Abilita solo l'iscrizione.

Affinché Security Hub generi i risultati del controllo, gli account dei membri devono essere AWS Config abilitati e configurati per registrare le risorse richieste. Per ulteriori informazioni, consulta [Abilitazione e configurazione di AWS Config](#).

Scegli il tuo metodo preferito e segui i passaggi per abilitare un account dell'organizzazione come account membro di Security Hub.

Security Hub console

Per abilitare manualmente gli account dell'organizzazione come membri del Security Hub

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).

Accedi utilizzando le credenziali dell'account amministratore delegato.

2. Nel pannello di navigazione di Security Hub, in Impostazioni, scegli Configurazione.
3. Nell'elenco Account, seleziona ogni account dell'organizzazione che desideri abilitare.
4. Scegli Azioni, quindi scegli Aggiungi membro.

Security Hub API

Per abilitare manualmente gli account dell'organizzazione come membri del Security Hub

Richiama l'[CreateMembers](#) API dall'account amministratore delegato. Per ogni account da abilitare, fornisci l'ID dell'account.

A differenza della procedura di invito manuale, quando `CreateMembers` richiami per abilitare un account dell'organizzazione, non devi inviare un invito.

AWS CLI

Per abilitare manualmente gli account dell'organizzazione come membri del Security Hub

Esegui il `create-members` comando dall'account amministratore delegato. Per ogni account da abilitare, fornisci l'ID dell'account.

A differenza della procedura di invito manuale, quando `create-members` esegui l'attivazione di un account aziendale, non devi inviare un invito.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountId>"}]'
```

Esempio

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"}, {"AccountId": "123456789222"}]'
```

Dissociazione degli account dei membri dall'organizzazione

Per interrompere la ricezione e la visualizzazione dei risultati di un account AWS Security Hub membro, puoi dissociare l'account membro dalla tua organizzazione.

Note

Se si utilizza la [configurazione centrale](#), la dissociazione funziona in modo diverso. È possibile creare una politica di configurazione che disabiliti Security Hub in uno o più account membro gestiti centralmente. Dopodiché, questi account fanno ancora parte dell'organizzazione, ma non genereranno i risultati del Security Hub. Se utilizzi la configurazione centrale ma disponi anche di account membri invitati manualmente, puoi dissociare uno o più account invitati manualmente.

Gli account membro gestiti utilizzando non AWS Organizations possono dissociare i propri account dall'account amministratore. Solo l'account amministratore può dissociare un account membro.

La dissociazione di un account membro non comporta la chiusura dell'account. Rimuove invece l'account membro dall'organizzazione. L'account membro dissociato diventa autonomo e non Account AWS è più gestito dall'integrazione del Security Hub con AWS Organizations

Scegli il tuo metodo preferito e segui i passaggi per dissociare un account membro dall'organizzazione.

Security Hub console

Per dissociare un account membro dall'organizzazione

1. Apri la AWS Security Hub console all'indirizzo <https://console.aws.amazon.com/securityhub/>.

Accedi utilizzando le credenziali dell'account amministratore delegato.

2. Nel riquadro di navigazione, in Impostazioni, scegli Configurazione.
3. Nella sezione Account, seleziona gli account da cui desideri dissociare. Se utilizzi la configurazione centrale, puoi selezionare un account invitato manualmente da dissociare dalla scheda `Invitation accounts`. Questa scheda è visibile solo se si utilizza la configurazione centrale.
4. Scegli Azioni, quindi scegli Dissocia account.

Security Hub API

Per dissociare un account membro dall'organizzazione

Richiama l'[DisassociateMembers](#) API dall'account amministratore delegato. È necessario fornire Account AWS gli ID per la dissociazione degli account dei membri. Per visualizzare un elenco di account membri, richiama l'[ListMembers](#) API.

AWS CLI

Per dissociare un account membro dall'organizzazione

Esegui il `disassociate-members` comando `>` dall'account amministratore delegato. È necessario fornire Account AWS gli ID per la dissociazione degli account dei membri. Per visualizzare un elenco di account membri, esegui il `list-members` comando `>`.

```
aws securityhub disassociate-members --account-ids "<accountIds>"
```

Esempio

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Puoi anche utilizzare la AWS Organizations console o gli AWS CLI AWS SDK per dissociare un account membro dalla tua organizzazione. Per ulteriori informazioni, consulta [Rimuovere un account membro dall'organizzazione nella Guida](#) per l'AWS Organizations utente.

Disattivazione dell'integrazione del Security Hub con AWS Organizations

Dopo l'integrazione di un' AWS Organizations organizzazione con AWS Security Hub, l'account di gestione Organizations può successivamente disabilitare l'integrazione. Come utente dell'account di gestione Organizations, puoi farlo disabilitando l'accesso affidabile per Security Hub in AWS Organizations.

Quando si disabilita l'accesso affidabile per Security Hub, si verifica quanto segue:

- Security Hub perde lo status di servizio affidabile in AWS Organizations.
- L'account amministratore delegato di Security Hub perde l'accesso alle impostazioni, ai dati e alle risorse di Security Hub per tutti gli account membri del Security Hub. Regioni AWS
- Se stavi utilizzando la [configurazione centrale](#), Security Hub smette automaticamente di utilizzarla per la tua organizzazione. Le policy di configurazione e le associazioni di policy vengono eliminate. Gli account mantengono le configurazioni che avevano prima della disattivazione dell'accesso affidabile.
- Tutti gli account dei membri di Security Hub diventano account autonomi e mantengono le impostazioni correnti. Se Security Hub è stato abilitato per un account membro in una o più regioni, Security Hub continua a essere abilitato per l'account in tali regioni. Anche gli standard e i controlli abilitati rimangono invariati. Puoi modificare queste impostazioni separatamente in ogni account e regione. Tuttavia, l'account non è più associato a un amministratore delegato in nessuna regione.

Per ulteriori informazioni sui risultati della disabilitazione dell'accesso affidabile ai servizi, vedere [Using AWS Organizations with other Servizi AWS nella Guida](#) per l'AWS Organizations utente.

Per disabilitare l'accesso affidabile, puoi utilizzare la AWS Organizations console, l'API Organizations o AWS CLI. Solo un utente dell'account di gestione Organizations può disabilitare l'accesso affidabile

ai servizi per Security Hub. Per i dettagli sulle autorizzazioni necessarie, consulta [Autorizzazioni necessarie per disabilitare l'accesso affidabile nella Guida](#) per l'AWS Organizations utente.

Prima di disabilitare l'accesso affidabile, consigliamo di collaborare con l'amministratore delegato dell'organizzazione per disabilitare Security Hub negli account dei membri e per ripulire le risorse del Security Hub in tali account.

Scegli il tuo metodo preferito e segui i passaggi per disabilitare l'accesso affidabile per Security Hub.

Organizations console

Per disabilitare l'accesso affidabile per Security Hub

1. Accedi AWS Management Console utilizzando le credenziali dell'account di AWS Organizations gestione.
2. Apri la console Organizations all'[indirizzo https://console.aws.amazon.com/organizations/](https://console.aws.amazon.com/organizations/).
3. Nel riquadro di navigazione, scegli Servizi.
4. In Servizi integrati, scegli AWS Security Hub.
5. Scegli Disable trusted access (Disabilita accesso attendibile).
6. Conferma di voler disabilitare l'accesso affidabile.

Organizations API

Per disabilitare l'accesso affidabile per Security Hub

Invoca l'AWSServiceAccessoperazione [Disable](#) dell' AWS Organizations API. Per il `ServicePrincipal` parametro, specificare il principale del servizio Security Hub (`securityhub.amazonaws.com`).

AWS CLI

Per disabilitare l'accesso affidabile per Security Hub

Esegui il [disable-aws-service-access](#) comando dell' AWS Organizations API. Per il `service-principal` parametro, specificare il principale del servizio Security Hub (`securityhub.amazonaws.com`).

Esempio:

```
aws organizations disable-aws-service-access --service-principal
securityhub.amazonaws.com
```

Gestione degli account tramite invito

È possibile gestire centralmente più AWS Security Hub account in due modi: integrando Security Hub con AWS Organizations o inviando e accettando manualmente gli inviti di iscrizione. È necessario utilizzare la procedura manuale se si dispone di un account autonomo o se non si effettua l'integrazione con Organizations. Nella gestione manuale degli account, l'amministratore del Security Hub invita gli account a diventare membri. La relazione amministratore-membro viene stabilita quando un potenziale membro accetta l'invito. Un account amministratore di Security Hub può gestire Security Hub per un massimo di 1.000 account membro basati su invito.

Tip

Se crei un'organizzazione basata su inviti in Security Hub, puoi successivamente [passare a usare AWS Organizations](#) invece. Se hai più di un account membro, ti consigliamo di gestire gli account tramite AWS Organizations

L'aggregazione interregionale dei risultati e di altri dati è disponibile per gli account che inviti tramite la procedura di invito manuale. Tuttavia, l'amministratore deve invitare l'account membro della regione di aggregazione e di tutte le regioni collegate affinché l'aggregazione tra regioni funzioni. Inoltre, l'account membro deve avere il Security Hub abilitato nella regione di aggregazione e in tutte le regioni collegate per consentire all'amministratore di visualizzare i risultati dell'account membro.

Le politiche di configurazione non sono supportate per gli account membro invitati manualmente. È invece necessario configurare le impostazioni di Security Hub separatamente in ogni account membro e Regione AWS quando si utilizza la procedura di invito manuale.

È inoltre necessario utilizzare la procedura manuale basata sugli inviti per gli account che non appartengono alla propria organizzazione. Ad esempio, potresti non includere un account di prova nella tua organizzazione. In alternativa, potresti voler consolidare gli account di più organizzazioni in un unico account amministratore di Security Hub. L'account amministratore di Security Hub deve inviare inviti ad account che appartengono ad altre organizzazioni.

Nella pagina Configurazione della console Security Hub, gli account aggiunti su invito sono elencati nella scheda Account di invito. Se utilizzi [Come funziona la configurazione centrale](#), ma anche inviti,

account esterni alla tua organizzazione, puoi visualizzare i risultati degli account basati su invito in questa scheda. Tuttavia, l'amministratore del Security Hub non può configurare account basati su inviti in tutte le regioni tramite l'uso di policy di configurazione.

Gli argomenti di questa sezione spiegano come gestire gli account dei membri tramite gli inviti.

Argomenti

- [Aggiungere e invitare account membri](#)
- [Rispondere a un invito a diventare un account membro](#)
- [Dissociazione degli account dei membri](#)
- [Eliminazione degli account dei membri](#)
- [Dissociarsi dal proprio account amministratore](#)
- [Passaggio alla gestione AWS Organizations degli account](#)

Aggiungere e invitare account membri

Il tuo account diventa l' AWS Security Hub amministratore degli account che accettano il tuo invito.

Quando accetti un invito da un altro account, il tuo account diventa un account membro e quell'account diventa il tuo amministratore.

Se il tuo account è un account amministratore, non puoi accettare un invito a diventare un account membro.

L'aggiunta di un account membro prevede i seguenti passaggi:

1. L'account amministratore aggiunge l'account membro al relativo elenco di account membri.
2. L'account amministratore invia un invito all'account membro.
3. L'account membro accetta l'invito.

Aggiungi account membri

Dalla console Security Hub, puoi aggiungere account all'elenco degli account membri. Nella console Security Hub, è possibile selezionare gli account singolarmente o caricare un .csv file contenente le informazioni sull'account.

Per ogni account, è necessario fornire l'ID dell'account e un indirizzo e-mail. L'indirizzo e-mail deve essere l'indirizzo e-mail da contattare in merito ai problemi di sicurezza dell'account. Non viene utilizzato per verificare l'account.

Scegli il tuo metodo preferito e segui i passaggi per aggiungere account membri.

Security Hub console

Per aggiungere account al tuo elenco di account membri

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).

Accedi utilizzando le credenziali dell'account amministratore.

2. Nel riquadro a sinistra, scegliere Settings (Impostazioni).
3. Nella pagina Impostazioni, scegli Account, quindi scegli Aggiungi account. Puoi quindi aggiungere account singolarmente o caricare un .csv file contenente l'elenco degli account.
4. Per selezionare gli account, esegui una delle seguenti operazioni:

- Per aggiungere gli account singolarmente, in Inserisci account, inserisci l'ID account e l'indirizzo e-mail dell'account da aggiungere, quindi scegli Aggiungi.

Ripeti questa procedura per ogni account.

- Per utilizzare un file con valori separati da virgole (.csv) per aggiungere più account, devi prima creare il file. Il file deve contenere l'ID dell'account e l'indirizzo e-mail di ogni account da aggiungere.

Nell'.csv file, gli account devono apparire uno per riga. La prima riga del .csv file deve contenere l'intestazione. Nell'intestazione, la prima colonna è **Account ID** e la seconda colonna è **Email**.

Ogni riga successiva deve contenere un ID account e un indirizzo e-mail validi per l'account da aggiungere.

Ecco un esempio di .csv file visualizzato in un editor di testo.

```
Account ID,Email
111111111111,user@example.com
```

In un programma per fogli di calcolo, i campi vengono visualizzati in colonne separate. Il formato sottostante è ancora separato da virgole. È necessario formattare gli ID degli account come numeri non decimali. Ad esempio, l'ID account 444455556666 non può essere formattato come 444455556666.0. Assicurati inoltre che la formattazione del numero non rimuova gli zeri iniziali dall'ID dell'account.

Per selezionare il file, sulla console, scegli Carica lista (.csv). Quindi scegli Sfoglia.

Dopo aver selezionato il file, scegli Aggiungi account.

5. Dopo aver aggiunto gli account, in Account da aggiungere, scegli Avanti.

Security Hub API

Per aggiungere account al tuo elenco di account membri

Richiama l'[CreateMembers](#) API dall'account amministratore. Per ogni account membro da aggiungere, devi fornire l' Account AWS ID.

AWS CLI

Per aggiungere account al tuo elenco di account membri

Esegui il [create-members](#) comando dall'account amministratore. Per ogni account membro da aggiungere, devi fornire l' Account AWS ID.

```
aws securityhub create-members --account-details '[{"AccountId": "<accountID1>"}]'
```

Esempio

```
aws securityhub create-members --account-details '[{"AccountId": "123456789111"}, {"AccountId": "123456789222"}]'
```

Invita gli account dei membri

Dopo aver aggiunto gli account membro, invii un invito all'account membro. Puoi anche inviare nuovamente un invito a un account che hai dissociato dall'amministratore.

Security Hub console

Per invitare account di potenziali membri

1. Apri la AWS Security Hub console all'indirizzo <https://console.aws.amazon.com/securityhub/>.

Accedi utilizzando le credenziali dell'account amministratore.

2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli Account.
3. Per l'account da invitare, scegliere Invite (Invita) nella colonna Status (Stato).
4. Quando ti viene richiesto di confermare, scegli Invita.

Note

Per inviare nuovamente gli inviti ad account dissociati, seleziona ciascun account dissociato nella pagina Account. Per Azioni, scegli Reinvia l'invito.

Security Hub API

Per invitare account di potenziali membri

Richiama l'[InviteMembers](#) API dall'account amministratore. Per ogni account da invitare, devi fornire l' Account AWS ID.

AWS CLI

Per invitare account di potenziali membri

Esegui il [invite-members](#) comando dall'account amministratore. Per ogni account da invitare, devi fornire l' Account AWS ID.

```
aws securityhub invite-members --account-ids <accountIDs>
```

Esempio

```
aws securityhub invite-members --account-ids "123456789111" "123456789222"
```

Rispondere a un invito a diventare un account membro

Puoi accettare o rifiutare un invito a diventare un account membro.

Dopo aver accettato un invito, il tuo account diventa un account AWS Security Hub membro. L'account che ha inviato l'invito diventa il tuo account amministratore di Security Hub. L'utente dell'account amministratore può visualizzare i risultati relativi al proprio account membro in Security Hub.

Se rifiuti l'invito, il tuo account viene contrassegnato come Rinunciato nell'elenco degli account membri dell'account amministratore.

Puoi accettare solo un invito a diventare un account membro.

Prima di poter accettare o rifiutare un invito, devi abilitare Security Hub.

Ricorda che tutti gli account Security Hub devono essere AWS Config abilitati e configurati per registrare tutte le risorse. Per i dettagli sui requisiti per AWS Config, vedere [Attivazione e configurazione AWS Config](#).

Accetta un invito

Scegli il tuo metodo preferito e segui i passaggi per accettare un invito a diventare un account membro.

Security Hub console

Per accettare un invito all'iscrizione

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli Account.
3. Nella sezione Account amministratore, attiva Accetta, quindi scegli Accetta invito.

Security Hub API

Per accettare un invito all'iscrizione

Richiama l'[AcceptAdministratorInvitation](#) API. È necessario fornire l'identificatore dell'invito e l' Account AWS ID dell'account amministratore. Per recuperare i dettagli sull'invito, usa l'[ListInvitations](#) operazione.

AWS CLI

Per accettare un invito all'iscrizione

Esegui il comando [accept-administrator-invitation](#). È necessario fornire l'identificatore dell'invito e l' Account AWS ID dell'account amministratore. Per recuperare i dettagli sull'invito, esegui il [list-invitations](#) comando.

```
aws securityhub accept-administrator-invitation --administrator-id <administratorAccountID> --invitation-id <invitationID>
```

Esempio

```
aws securityhub accept-administrator-invitation --administrator-id 123456789012 --invitation-id 7ab938c5d52d7904ad09f9e7c20cc4eb
```

Note

La console Security Hub continua a funzionare `AcceptInvitation`. Alla fine verrà modificata per essere utilizzata `AcceptAdministratorInvitation`. Tutte le policy IAM che controllano specificamente l'accesso a questa funzione devono continuare a essere utilizzate `AcceptInvitation`. È inoltre necessario `AcceptAdministratorInvitation` completare le policy per garantire che siano disponibili le autorizzazioni corrette dopo l'inizio dell'utilizzo `AcceptAdministratorInvitation` della console.

Rifiutare un invito

Puoi rifiutare un invito a diventare un account membro. Quando rifiuti un invito nella console Security Hub, il tuo account viene contrassegnato come Rinunciato nell'elenco degli account membri dell'account amministratore.

Quando rifiuti un invito, devi accedere all'account membro che ha ricevuto l'invito.

Scegli il tuo metodo preferito e segui i passaggi per rifiutare un invito a diventare un account membro.

Security Hub console

Per rifiutare un invito all'iscrizione

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli Account.
3. Nella sezione Account amministratore, scegli Rifiuta invito.

Security Hub API

Per rifiutare un invito all'iscrizione

Richiama l'[DeclineInvitations](#) API. È necessario fornire l' Account AWS ID dell'account amministratore che ha emesso l'invito. Per visualizzare le informazioni sugli inviti, utilizza l'[ListInvitations](#) operazione.

AWS CLI

Per rifiutare un invito all'iscrizione

Esegui il comando [decline-invitations](#). È necessario fornire l' Account AWS ID dell'account amministratore che ha emesso l'invito. Per visualizzare le informazioni sugli inviti, esegui il [list-invitations](#) comando.

```
aws securityhub decline-invitations --account-ids "<administratorAccountId>"
```

Esempio

```
aws securityhub decline-invitations --account-ids "123456789012"
```

Dissociazione degli account dei membri

Un account AWS Security Hub amministratore può annullare l'associazione di un account membro per interrompere la ricezione e la visualizzazione dei risultati di quell'account. È necessario dissociare un account membro prima di poterlo eliminare.

Quando dissociate un account membro, questo rimane nell'elenco degli account membri con lo stato Rimosso (Non associato). L'account viene rimosso dalle informazioni relative all'account amministratore dell'account membro.

Per riprendere a ricevere i risultati relativi all'account, puoi inviare nuovamente l'invito. Per rimuovere completamente l'account membro, puoi eliminare l'account membro.

Scegli il tuo metodo preferito e segui i passaggi per dissociare un account membro invitato manualmente dall'account amministratore.

Security Hub console

Per dissociare un account membro invitato manualmente

1. [Apri la console all'indirizzo https://console.aws.amazon.com/securityhub/ AWS Security Hub](https://console.aws.amazon.com/securityhub/) .

Accedi utilizzando le credenziali dell'account amministratore.

2. Nel riquadro di navigazione, in Impostazioni, scegli Configurazione.
3. Nella sezione Account, seleziona gli account da cui desideri dissociare.
4. Scegli Azioni, quindi scegli Dissocia account.

Security Hub API

Per dissociare un account membro invitato manualmente

Richiama l'[DisassociateMembers](#) API dall'account amministratore. È necessario fornire gli Account AWS ID degli account dei membri da cui si desidera dissociare. Per visualizzare un elenco di account membri, utilizza l'[ListMembers](#) operazione.

AWS CLI

Per dissociare un account membro invitato manualmente

Esegui il [disassociate-members](#) comando dall'account amministratore. È necessario fornire gli Account AWS ID degli account dei membri da cui si desidera dissociare. Per visualizzare un elenco di account membri, esegui il [list-members](#) comando.

```
aws securityhub disassociate-members --account-ids <accountIds>
```

Esempio

```
aws securityhub disassociate-members --account-ids "123456789111" "123456789222"
```

Eliminazione degli account dei membri

In qualità di account AWS Security Hub amministratore, puoi eliminare gli account dei membri aggiunti su invito. Prima di poter eliminare un account abilitato, è necessario dissociarlo.

Quando si elimina un account membro, questo viene completamente rimosso dall'elenco. Per ripristinare l'iscrizione dell'account, devi aggiungerlo e invitarlo nuovamente come se fosse un account membro completamente nuovo.

Non puoi eliminare gli account che appartengono a un'organizzazione e che vengono gestiti utilizzando l'integrazione con AWS Organizations.

Scegli il tuo metodo preferito e segui i passaggi per eliminare gli account dei membri invitati manualmente.

Security Hub console

Per eliminare un account membro invitato manualmente

1. [Apri la AWS Security Hub console all'indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).

Accedi utilizzando l'account amministratore.

2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli Configurazione.
3. Scegli la scheda Account di invito. Quindi, seleziona gli account da eliminare.
4. Scegli Azioni, quindi Elimina. Questa opzione è disponibile solo se hai dissociato l'account. È necessario dissociare un account membro prima che possa essere eliminato.

Security Hub API

Per eliminare un account membro invitato manualmente

Richiama l'[DeleteMembers](#) API dall'account amministratore. È necessario fornire gli Account AWS ID degli account dei membri che si desidera eliminare. Per recuperare l'elenco degli account membri, richiama l'[ListMembers](#) API.

AWS CLI

Per eliminare un account membro invitato manualmente

Esegui il [delete-members](#) comando dall'account amministratore. È necessario fornire gli Account AWS ID degli account membro che si desidera eliminare. Per recuperare l'elenco degli account membri, esegui il [list-members](#) comando.

```
aws securityhub delete-members --account-ids <memberAccountIDs>
```

Esempio

```
aws securityhub delete-members --account-ids "123456789111" "123456789222"
```

Dissociarsi dal proprio account amministratore

Se il tuo account è stato aggiunto come account AWS Security Hub membro su invito, puoi dissociare l'account membro dall'account amministratore. Una volta dissociato un account membro, Security Hub non invia i risultati dall'account all'account amministratore.

Gli account membro gestiti utilizzando l'integrazione con non AWS Organizations possono dissociare i propri account dall'account amministratore. Solo l'amministratore delegato di Security Hub può dissociare gli account dei membri gestiti con Organizations.

Quando ci si dissocia dall'account amministratore, l'account rimane nell'elenco dei membri dell'account amministratore con lo stato di Dimesso. Tuttavia, l'account amministratore non riceve alcun risultato relativo al tuo account.

Dopo la dissociazione dall'account amministratore, l'invito a diventare membro rimane valido. Potrai accettare nuovamente l'invito in futuro.

Security Hub console

Per dissociarsi dal proprio account amministratore

1. Apri la AWS Security Hub console all'indirizzo <https://console.aws.amazon.com/securityhub/>.
2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli Account.
3. Nella sezione Account amministratore, disattiva Accetta, quindi scegli Aggiorna.

Security Hub API

Per dissociarti dal tuo account amministratore

Richiama l'API. [DisassociateFromAdministratorAccount](#)

AWS CLI

Per dissociarsi dal proprio account amministratore

Esegui il comando [disassociate-from-administrator-account](#).

```
aws securityhub disassociate-from-administrator-account
```

Note

La console Security Hub continua a funzionare `DisassociateFromMasterAccount`. Alla fine verrà modificata per essere utilizzata `DisassociateFromAdministratorAccount`. Tutte le policy IAM che controllano specificamente l'accesso a questa funzione devono continuare a essere utilizzate `DisassociateFromMasterAccount`. È inoltre necessario `DisassociateFromAdministratorAccount` completare le policy per garantire che siano disponibili le autorizzazioni corrette dopo l'inizio dell'utilizzo `DisassociateFromAdministratorAccount` della console.

Passaggio alla gestione AWS Organizations degli account

Quando gestisci gli account manualmente AWS Security Hub, devi invitare gli account dei potenziali membri e configurare ogni account membro separatamente in ciascuno Regione AWS di essi.

Integrando Security Hub e AWS Organizations, puoi eliminare la necessità di inviare inviti e ottenere un maggiore controllo sul modo in cui Security Hub è configurato e personalizzato nella tua organizzazione.

È possibile utilizzare un approccio combinato in cui si utilizza l'AWS Organizations integrazione, ma anche invitare manualmente account esterni all'organizzazione. Tuttavia, consigliamo di utilizzare esclusivamente l'integrazione Organizations. La [configurazione centrale](#), una funzionalità che consente di gestire Security Hub su più account e regioni, è disponibile solo in caso di integrazione con Organizations.

Questa sezione spiega come passare dalla gestione manuale degli account basata su inviti alla gestione degli account con. AWS Organizations

Integrazione del Security Hub con AWS Organizations

Innanzitutto, è necessario integrare Security Hub e AWS Organizations.

Puoi integrare questi servizi completando i seguenti passaggi:

- Crea un'organizzazione in AWS Organizations. Per istruzioni, consulta [Creare un'organizzazione](#) nella Guida AWS Organizations per l'utente.
- Dall'account di gestione Organizations, designare un account amministratore delegato di Security Hub.

Note

L'account di gestione dell'organizzazione non può essere impostato come account DA.

Per istruzioni dettagliate, vedi [Integrazione del Security Hub con AWS Organizations](#).

Completando i passaggi precedenti, concedi [l'accesso affidabile](#) per Security Hub in AWS Organizations. Ciò abilita anche Security Hub nella versione corrente Regione AWS per l'account amministratore delegato.

L'amministratore delegato può gestire l'organizzazione in Security Hub, principalmente aggiungendo gli account dell'organizzazione come account membri del Security Hub. L'amministratore può anche accedere a determinate impostazioni, dati e risorse del Security Hub per tali account.

Quando si passa alla gestione degli account utilizzando Organizations, gli account basati su invito non diventano automaticamente membri del Security Hub. Solo gli account che aggiungi alla nuova organizzazione possono diventare membri del Security Hub.

Configurazione centrale e configurazione locale

Dopo aver attivato l'integrazione, puoi gestire gli account con Organizations. Per informazioni, consulta [Gestione degli account con AWS Organizations](#). La gestione degli account varia in base al tipo di configurazione dell'organizzazione.

Esistono due tipi di configurazione possibili per l'organizzazione, locale e centrale. Il tipo di configurazione predefinito è la configurazione locale. Per visualizzare il tipo di configurazione corrente, scegli Impostazioni nel pannello di navigazione della console Security Hub, quindi

Configurazione. Puoi anche richiamare l'[DescribeOrganizationConfiguration](#) API per visualizzare il tipo di configurazione.

Nella configurazione locale, l'account amministratore delegato può scegliere di abilitare automaticamente Security Hub e gli standard di sicurezza predefiniti nei nuovi account quando entrano a far parte dell'organizzazione. Queste nuove impostazioni dell'account hanno effetto nella regione corrente. Le altre impostazioni del Security Hub devono essere configurate separatamente da ciascun account membro in ciascuna regione.

Si consiglia di utilizzare la configurazione centrale anziché la configurazione locale. In configurazione centrale, l'account amministratore delegato può creare politiche di configurazione del Security Hub che hanno effetto su più regioni e specificare le funzionalità del Security Hub nei vari account e unità organizzative (OU) dell'organizzazione. È possibile applicare un'unica politica di configurazione all'intera organizzazione o politiche di configurazione diverse a diversi account e unità organizzative. Ad esempio, è possibile abilitare un set di standard e controlli negli account di produzione e un set diverso di standard e controlli negli account di test. Il DA può modificare le politiche di configurazione in base alle esigenze.

Per ulteriori informazioni su come funziona la configurazione centrale, vedere [Come funziona la configurazione centrale](#).

Per istruzioni sul passaggio dalla configurazione locale a quella centrale, vedere [Inizia a usare la configurazione centrale](#).

Azioni consentite per gli account

Gli account amministratore e membro hanno accesso alle AWS Security Hub azioni riportate nelle tabelle seguenti. Nelle tabelle, i valori hanno i seguenti significati:

- **Qualsiasi:** l'account può eseguire l'azione per qualsiasi account membro sotto lo stesso amministratore.
- **Corrente:** l'account può eseguire l'azione solo per se stesso (l'account a cui hai attualmente effettuato l'accesso).
- **Dash:** indica che l'account non è in grado di eseguire l'azione.

Come indicato nelle tabelle, le azioni consentite variano in base all'integrazione AWS Organizations e al tipo di configurazione utilizzato dall'organizzazione. Per informazioni sulla differenza tra configurazione centrale e locale, vedere [Gestione degli account con AWS Organizations](#).

Security Hub non copia i risultati degli account dei membri nell'account amministratore. In Security Hub, tutti i risultati vengono inseriti in una regione specifica per un account specifico. In ogni regione, l'account amministratore può visualizzare e gestire i risultati per i propri account membro in quella regione.

Se si imposta una regione di aggregazione, l'account amministratore può visualizzare e gestire i risultati degli account membro provenienti dalle regioni collegate che vengono replicati nella regione di aggregazione. [Per ulteriori informazioni sull'aggregazione tra regioni, vedere Aggregazione tra regioni.](#)

Questa tabella riporta le autorizzazioni predefinite per gli account amministratore e membro. Puoi utilizzare policy IAM personalizzate per limitare ulteriormente l'accesso alle caratteristiche e alle funzioni di Security Hub. Per indicazioni ed esempi, consulta il post sul blog [Aligning IAM policies to user personas](#) for. AWS Security Hub

Azioni consentite se si effettua l'integrazione con Organizations e si utilizza la configurazione centrale

Gli account amministratore e membro possono accedere alle azioni di Security Hub come segue se si effettua l'integrazione con Organizations e si utilizza la configurazione centrale.

Azione	Account amministratore delegato Security Hub	Account membro gestito centralmente	Account membro autogestito
Creare e gestire le politiche di configurazione del Security Hub	Per account gestiti autonomamente e centralmente	–	–
Visualizza gli account dell'organizzazione	Qualsiasi	–	–
Account socio dissociato	Qualsiasi	–	–
Eliminare l'account del membro	Qualsiasi account non aziendale	–	–

Azione	Account amministratore delegato Security Hub	Account membro gestito centralmente	Account membro autogestito
Disattiva Security Hub	Per conti correnti e conti gestiti centralmente	–	Attuali
Visualizza i risultati e la cronologia dei risultati	Qualsiasi	Attuali	Attuali
Aggiorna i risultati	Qualsiasi	Attuali	Attuali
Visualizza i risultati delle analisi	Qualsiasi	Attuali	Attuali
Visualizza i dettagli del controllo	Qualsiasi	Attuali	Attuali
Attiva o disattiva i risultati del controllo consolidato	Qualsiasi	–	–
Abilita e disabilita gli standard	Per conti correnti e conti gestiti centralmente	–	Attuali
Abilita e disabilita i controlli	Per conti correnti e conti gestiti centralmente	–	Attuali
Abilita e disabilita le integrazioni	Attuali	Attuali	Attuali
Configura l'aggregazione tra regioni	Qualsiasi	–	–

Azione	Account amministratore delegato Security Hub	Account membro gestito centralmente	Account membro autogestito
Seleziona la regione d'origine e le regioni collegate	Qualsiasi (è necessario interrompere e riavviare la configurazione centrale per modificare la regione di origine)	–	–
Configura azioni personalizzate	Attuali	Attuali	Attuali
Configura le regole di automazione	Qualsiasi	–	–
Configura approfondimenti personalizzati	Attuali	Attuali	Attuali

Azioni consentite se si esegue l'integrazione con Organizations e si utilizza la configurazione locale

Gli account amministratore e membro possono accedere alle azioni di Security Hub come segue se si effettua l'integrazione con Organizations e si utilizza la configurazione locale.

Azione	Account amministratore delegato Security Hub	Account membro
Creare e gestire le politiche di configurazione del Security Hub	–	–
Visualizza gli account dell'organizzazione	Qualsiasi	–
Account socio dissociato	Qualsiasi	–

Azione	Account amministratore delegato Security Hub	Account membro
Eliminare l'account del membro	–	–
Disattiva Security Hub	–	Corrente (se l'account non è associato all'amministratore delegato)
Visualizza i risultati e la cronologia delle scoperte	Qualsiasi	Attuali
Aggiorna i risultati	Qualsiasi	Attuali
Visualizza i risultati delle analisi	Qualsiasi	Attuali
Visualizza i dettagli del controllo	Qualsiasi	Attuali
Attiva o disattiva i risultati del controllo consolidato	Qualsiasi	–
Abilita e disabilita gli standard	Attuali	Attuali
Abilita automaticamente Security Hub e gli standard predefiniti nei nuovi account dell'organizzazione	Per account correnti e nuovi account aziendali	–
Abilita e disabilita i controlli	Attuali	Attuali
Abilita e disabilita le integrazioni	Attuali	Attuali
Configura l'aggregazione tra regioni	Qualsiasi	–

Azione	Account amministratore delegato Security Hub	Account membro
Configura azioni personalizzate	Attuali	Attuali
Configura le regole di automazione	Qualsiasi	–
Configura approfondimenti personalizzati	Attuali	Attuali

Azioni consentite per gli account basati su invito

Gli account amministratore e membro possono accedere alle azioni del Security Hub come segue se si utilizza il metodo basato su invito per gestire manualmente gli account anziché integrarsi con AWS Organizations

Azione	Account amministratore Security Hub	Account membro
Creare e gestire le politiche di configurazione del Security Hub	–	–
Visualizza gli account dell'organizzazione	Qualsiasi	–
Account socio dissociato	Qualsiasi	Attuali
Eliminare l'account del membro	Qualsiasi	–
Disattiva Security Hub	Attuale (se non ci sono account membri abilitati)	Corrente (se l'account è dissociato dall'account amministratore)

Azione	Account amministratore Security Hub	Account membro
Visualizza i risultati e la cronologia delle scoperte	Qualsiasi	Attuali
Aggiorna i risultati	Qualsiasi	Attuali
Visualizza i risultati delle analisi	Qualsiasi	Attuali
Visualizza i dettagli del controllo	Qualsiasi	Attuali
Attiva o disattiva i risultati del controllo consolidato	Qualsiasi	–
Abilita e disabilita gli standard	Attuali	Attuali
Abilita automaticamente Security Hub e gli standard predefiniti nei nuovi account dell'organizzazione	–	–
Abilita e disabilita i controlli	Attuali	Attuali
Abilita e disabilita le integrazioni	Attuali	Attuali
Configura l'aggregazione tra regioni	Qualsiasi	–
Configura azioni personalizzate	Attuali	Attuali
Configura le regole di automazione	Qualsiasi	–
Configura approfondimenti personalizzati	Attuali	Attuali

Restrizioni e raccomandazioni sulla gestione degli account

La sezione seguente riassume alcune restrizioni e raccomandazioni da tenere a mente quando si gestiscono gli account dei membri in AWS Security Hub.

Numero massimo di account membri

Se utilizzi l'integrazione con AWS Organizations, Security Hub supporta fino a 10.000 account membro per account amministratore delegato in ciascuna Regione AWS. Se abiliti e gestisci Security Hub manualmente, Security Hub supporta fino a 1.000 inviti di account membro per account amministratore in ciascuna regione.

Account e Regioni

Iscrizione per organizzazione

Se si integra Security Hub con AWS Organizations, l'account di gestione Organizations può designare un account amministratore delegato (DA) per Security Hub. L'account di gestione dell'organizzazione non può essere impostato come DA in Organizations. Sebbene ciò sia consentito in Security Hub, consigliamo che l'account di gestione di Organizations non sia il DA.

Ti consigliamo di scegliere lo stesso account DA in tutte le regioni. Se utilizzi la [configurazione centrale](#), Security Hub imposta lo stesso account DA in tutte le regioni in cui configuri Security Hub per la tua organizzazione.

Ti consigliamo inoltre di scegliere lo stesso account DA per tutti i servizi AWS di sicurezza e conformità per aiutarti a gestire i problemi relativi alla sicurezza in un unico pannello di controllo.

Iscrizione su invito

Per gli account membro creati su invito, l'associazione tra account amministratore e membro viene creata solo nella regione da cui viene inviato l'invito. L'account amministratore deve abilitare Security Hub in ogni regione in cui si desidera utilizzarlo. L'account amministratore invita quindi ogni account a diventare un account membro in quella regione.

Restrizioni alle relazioni amministratore-membro

Note

Se utilizzi l'integrazione di Security Hub con AWS Organization e non hai invitato manualmente alcun account membro, questa sezione non ti riguarda.

Un account non può essere contemporaneamente un account amministratore e un account membro.

Un account membro può essere associato a un solo account amministratore. Se un account dell'organizzazione è abilitato dall'account amministratore di Security Hub, l'account non può accettare un invito da un altro account. Se un account ha già accettato un invito, l'account non può essere abilitato dall'account amministratore di Security Hub dell'organizzazione. Inoltre, non può ricevere inviti da altri account.

Per la procedura di invito manuale, l'accettazione di un invito all'iscrizione è facoltativa.

Coordinamento degli account degli amministratori tra i vari servizi

Security Hub aggrega i risultati di vari AWS servizi, come Amazon GuardDuty, Amazon Inspector e Amazon Macie. Security Hub consente inoltre agli utenti di passare da un GuardDuty risultato all'avvio di un'indagine in Amazon Detective.

Tuttavia, le relazioni amministratore-membro impostate in questi altri servizi non si applicano automaticamente a Security Hub. Security Hub consiglia di utilizzare lo stesso account dell'account amministratore per tutti questi servizi. Questo account amministratore deve essere un account responsabile degli strumenti di sicurezza. Lo stesso account deve essere utilizzato anche come account aggregatore per AWS Config.

Ad esempio, un utente dell'account GuardDuty amministratore A può visualizzare i risultati GuardDuty degli account membro B e C sulla GuardDuty console. Se l'account A abilita quindi Security Hub, gli utenti dell'account A non visualizzano automaticamente GuardDuty i risultati per gli account B e C in Security Hub. Per questi account è richiesta anche una relazione amministratore-membro di Security Hub.

A tale scopo, imposta l'account A come account amministratore del Security Hub e abilita gli account B e C a diventare account membri del Security Hub.

Effetto delle azioni dell'account sui dati del Security Hub

Queste azioni dell'account hanno i seguenti effetti sui AWS Security Hub dati.

Security Hub disattivato

Se si utilizza la [configurazione centrale](#), l'amministratore delegato (DA) può creare politiche di configurazione del Security Hub che si disabilitano AWS Security Hub in account e unità organizzative (OU) specifici. In questo caso, Security Hub è disabilitato negli account e nelle unità organizzative specificati nella regione di residenza e in tutte le regioni collegate.

Se non utilizzi la configurazione centrale, devi disabilitare Security Hub separatamente in ogni account e regione in cui l'hai abilitato.

Non vengono generati nuovi risultati per l'account amministratore se Security Hub è disabilitato nell'account amministratore. Inoltre, non è possibile utilizzare la configurazione centrale se Security Hub è disabilitato nell'account DA. I risultati esistenti vengono eliminati dopo 90 giorni.

Le integrazioni con altri Servizi AWS vengono rimosse.

Gli standard e i controlli di sicurezza abilitati sono disabilitati.

Vengono conservati altri dati e impostazioni del Security Hub, tra cui azioni personalizzate, approfondimenti e abbonamenti a prodotti di terze parti.

Account membro dissociato dall'account amministratore

Quando un account membro viene dissociato dall'account amministratore, l'account amministratore perde l'autorizzazione a visualizzare i risultati nell'account membro. Tuttavia, Security Hub è ancora abilitato in entrambi gli account.

Se utilizzi la configurazione centrale, il DA non può configurare Security Hub per un account membro dissociato dall'account DA.

Le impostazioni o le integrazioni personalizzate definite per l'account amministratore non vengono applicate ai risultati dell'account del precedente membro. Ad esempio, dopo la dissociazione degli account, potresti avere un'azione personalizzata nell'account amministratore utilizzato come modello di evento in una EventBridge regola Amazon. Tuttavia, questa azione personalizzata non può essere utilizzata nell'account del membro.

Nell'elenco Account per l'account amministratore di Security Hub, un account rimosso ha lo stato Disassociato.

L'account membro viene rimosso da un'organizzazione

Quando un account membro viene rimosso da un'organizzazione, l'account amministratore di Security Hub perde l'autorizzazione a visualizzare i risultati nell'account membro. Tuttavia, Security Hub è ancora abilitato in entrambi gli account con le stesse impostazioni che avevano prima della rimozione.

Se utilizzi la configurazione centrale, non puoi configurare Security Hub per un account membro dopo che è stato rimosso dall'organizzazione a cui appartiene l'amministratore delegato. Tuttavia, l'account mantiene le impostazioni che aveva prima della rimozione, a meno che non le modifichi manualmente.

Nell'elenco Account per l'account amministratore di Security Hub, un account rimosso ha lo stato Eliminato.

L'account è sospeso

Quando un account viene sospeso AWS, l'account perde l'autorizzazione a visualizzare i risultati in Security Hub. Non vengono generati nuovi risultati per quell'account. L'account amministratore di un account sospeso può visualizzare i risultati dell'account esistente.

Per un account dell'organizzazione, lo stato dell'account membro può anche cambiare in Account sospeso. Ciò accade se l'account viene sospeso nello stesso momento in cui l'account amministratore tenta di abilitarlo. L'account amministratore di un account sospeso non può visualizzare i risultati relativi a quell'account. In caso contrario, lo stato di sospensione non influisce sullo stato dell'account membro.

Se si utilizza la configurazione centrale, l'associazione delle politiche fallisce se l'amministratore delegato tenta di associare una politica di configurazione a un account sospeso.


Dopo 90 giorni, l'account viene chiuso o riattivato. Quando l'account viene riattivato, le autorizzazioni del Security Hub vengono ripristinate. Se lo stato dell'account membro è Account sospeso, l'account amministratore deve abilitare l'account manualmente.

L'account è chiuso

Quando un Account AWS è chiuso, Security Hub risponde alla chiusura come segue.

Security Hub conserva i risultati dell'account per 90 giorni dalla data effettiva della chiusura dell'account. Al termine del periodo di 90 giorni, Security Hub elimina definitivamente tutti i risultati relativi all'account.

- Per conservare i risultati per più di 90 giorni, puoi utilizzare un'azione personalizzata con una EventBridge regola per archiviare i risultati in un bucket Amazon S3. Finché Security Hub conserva i risultati, quando riapri l'account chiuso, Security Hub ripristina i risultati per l'account.
- Se l'account è un account amministratore di Security Hub, viene rimosso come amministratore e tutti gli account dei membri vengono rimossi. Se l'account è un account membro, viene dissociato e rimosso come membro dall'account amministratore di Security Hub.
- Per ulteriori informazioni, consulta [Chiusura di un account](#) nella Guida per l'utente di AWS Billing and Cost Management.

 Important

Per i clienti nelle regioni AWS GovCloud (US):

- Prima di chiudere il tuo account, effettua il backup ed elimina i dati delle policy e le altre risorse dell'account. Dopo aver chiuso l'account, non avrai più accesso ad essi.

Aggregazione tra regioni

Con l'aggregazione tra regioni, puoi aggregare i risultati, trovare aggiornamenti e approfondimenti, controllare gli stati di conformità e i punteggi di sicurezza di più regioni in un'unica regione di aggregazione. È quindi possibile gestire tutti questi dati dalla regione di aggregazione.

Note

In AWS GovCloud (US), l'aggregazione tra regioni è supportata solo per i risultati, la ricerca di aggiornamenti e le informazioni approfondite in tutta la regione. AWS GovCloud (US) In particolare, puoi aggregare i risultati, trovare aggiornamenti e approfondimenti solo tra AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali). Nelle regioni cinesi, l'aggregazione interregionale è supportata solo per i risultati, gli aggiornamenti dei risultati e gli approfondimenti nelle regioni cinesi. In particolare, puoi aggregare risultati, trovare aggiornamenti e approfondimenti solo tra Cina (Pechino) e Cina (Ningxia).

Supponiamo di impostare Stati Uniti orientali (Virginia settentrionale) come regione di aggregazione e Stati Uniti occidentali (Oregon) e Stati Uniti occidentali (California settentrionale) come regioni collegate. Quando si visualizza la pagina Risultati negli Stati Uniti orientali (Virginia settentrionale), vengono visualizzati i risultati di tutte e tre le regioni. Gli aggiornamenti a tali risultati si riflettono anche in tutte e tre le regioni.

Lo stato di attivazione di un controllo deve essere modificato in ciascuna regione. Se un controllo è abilitato in una regione collegata ma disabilitato nella regione di aggregazione, è possibile visualizzare lo stato di conformità del controllo dalla regione di aggregazione, ma non è possibile abilitare o disabilitare tale controllo dalla regione di aggregazione.

Per visualizzare i punteggi di sicurezza e gli stati di conformità tra le regioni, aggiungi le seguenti autorizzazioni al tuo ruolo IAM che utilizza Security Hub:

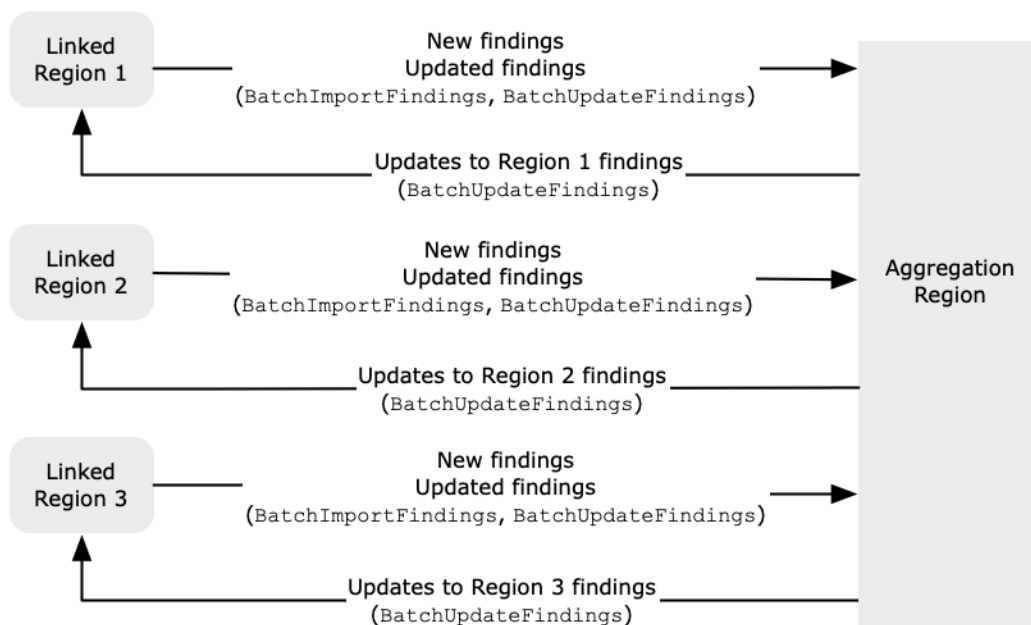
- [ListSecurityControlDefinitions](#)
- [BatchGetStandardsControlAssociations](#)
- [BatchUpdateStandardsControlAssociations](#)

Come funziona l'aggregazione tra regioni

Quando l'aggregazione tra regioni è abilitata, Security Hub replica i seguenti dati dalle regioni collegate alla regione di aggregazione. Ciò si verifica in tutti gli account in cui è abilitata l'aggregazione tra regioni.

- Risultati
- Informazioni dettagliate
- Controlla gli stati di conformità
- Punteggi di sicurezza

Oltre ai nuovi dati nell'elenco precedente, Security Hub replica anche gli aggiornamenti di questi dati tra le regioni collegate e la regione di aggregazione. Gli aggiornamenti che si verificano in una regione collegata vengono replicati nella regione di aggregazione. Gli aggiornamenti che si verificano nella regione di aggregazione vengono replicati nella regione collegata.



Se sono presenti aggiornamenti in conflitto nella regione di aggregazione e nella regione collegata, viene utilizzato l'aggiornamento più recente.

L'aggregazione tra regioni non aumenta il costo di Security Hub. Non ti viene addebitato alcun costo quando Security Hub replica nuovi dati o aggiornamenti.

Nella regione di aggregazione, la pagina di riepilogo fornisce una visualizzazione dei risultati attivi nelle regioni collegate. Per informazioni, consulta [Visualizzazione di un riepilogo interregionale dei risultati per gravità](#). In altri pannelli della pagina di riepilogo che analizzano i risultati vengono visualizzate anche informazioni provenienti da tutte le regioni collegate.

I punteggi di sicurezza nella regione di aggregazione vengono calcolati confrontando il numero di controlli approvati con il numero di controlli abilitati in tutte le aree collegate. Inoltre, se un controllo è abilitato in almeno una regione collegata, è visibile nelle pagine dei dettagli degli standard di sicurezza della regione di aggregazione. Lo stato di conformità dei controlli nelle pagine dei dettagli degli standard riflette i risultati delle regioni collegate. Se un controllo di sicurezza associato a un controllo ha esito negativo in una o più aree collegate, lo stato di conformità di tale controllo viene visualizzato come Non riuscito nelle pagine dei dettagli degli standard della regione di aggregazione. Il numero di controlli di sicurezza include i risultati di tutte le regioni collegate.

Security Hub aggrega solo i dati delle regioni in cui un account ha Security Hub abilitato. Security Hub non è abilitato automaticamente per un account in base alla configurazione di aggregazione tra regioni.

Aggregazione per account amministrativi e membri

Gli account autonomi, gli account membro e gli account amministratore possono configurare l'aggregazione tra regioni. Se configurata da un amministratore, la presenza dell'account amministratore è essenziale affinché l'aggregazione tra regioni funzioni negli account amministrati. Se l'account amministratore viene rimosso o dissociato da un account membro, l'aggregazione tra aree geografiche per l'account membro si interrompe. Ciò è vero anche se l'aggregazione tra aree geografiche era abilitata per l'account prima dell'inizio della relazione amministratore-membro.

Quando un account amministratore abilita l'aggregazione tra regioni, Security Hub replica i dati generati dall'account amministratore in tutte le regioni collegate alla regione di aggregazione. Inoltre, Security Hub identifica gli account membro associati a quell'amministratore e ogni account membro eredita le impostazioni di aggregazione interregionale dell'amministratore. Security Hub replica i dati generati da un account membro in tutte le regioni collegate alla regione di aggregazione.

L'amministratore può accedere e gestire i risultati di sicurezza di tutti gli account membri all'interno delle regioni amministrare. Tuttavia, in qualità di amministratore di Security Hub, è necessario accedere alla regione di aggregazione per visualizzare i dati aggregati di tutti gli account membri e le regioni collegate.

In qualità di account membro di Security Hub, devi accedere alla regione di aggregazione per visualizzare i dati aggregati del tuo account da tutte le regioni collegate. Gli account dei membri non dispongono delle autorizzazioni per visualizzare i dati degli altri account membri.

Un account amministratore può invitare manualmente gli account dei membri o fungere da amministratore delegato di un'organizzazione integrata con AWS Organizations. Per un [account membro invitato manualmente, l'amministratore deve invitare l'account](#) dalla regione di aggregazione e da tutte le regioni collegate affinché l'aggregazione tra regioni funzioni. Inoltre, l'account membro deve avere il Security Hub abilitato nella regione di aggregazione e in tutte le regioni collegate per consentire all'amministratore di visualizzare i risultati dell'account membro. Se non utilizzi la regione di aggregazione per altri scopi, puoi disabilitare gli standard e le integrazioni di Security Hub in quella regione per evitare addebiti.

Se prevedi di utilizzare l'aggregazione tra regioni e disponi di più account amministratore, ti consigliamo di seguire queste best practice:

- Ogni account amministratore ha account membri diversi.
- Ogni account amministratore ha gli stessi account membro in tutte le regioni.
- Ogni account amministratore utilizza una regione di aggregazione diversa.

Note

Per comprendere in che modo l'aggregazione tra aree geografiche influisce sulla configurazione centrale, consulta [Configurazione centrale e aggregazione tra regioni](#)

Configurazione centrale e aggregazione tra regioni

La configurazione centrale è una funzionalità opzionale di Security Hub che puoi utilizzare se esegui l'integrazione con AWS Organizations. Se si utilizza la configurazione centrale, l'account amministratore delegato può configurare il servizio Security Hub, gli standard e i controlli per gli account e le unità organizzative (OU) dell'organizzazione. Per configurare account e unità organizzative, l'amministratore delegato crea le politiche di configurazione del Security Hub. Le policy di configurazione possono essere utilizzate per definire se Security Hub è abilitato o disabilitato e quali standard e controlli sono abilitati. L'amministratore delegato associa le politiche di configurazione a account specifici, unità organizzative o alla radice (l'intera organizzazione).

L'amministratore delegato può creare e gestire le politiche di configurazione per l'organizzazione solo dalla regione di aggregazione. Inoltre, le politiche di configurazione hanno effetto nella regione di aggregazione e in tutte le regioni collegate. Non è possibile creare una politica di configurazione che si applichi solo in alcune regioni collegate e non in altre. Nella configurazione centrale, la regione di aggregazione è denominata regione principale. La stessa regione deve fungere da regione di origine per la configurazione centrale e da regione di aggregazione per l'aggregazione tra regioni. [Per informazioni sull'aggregazione tra regioni, vedere *Aggregazione tra regioni*](#).

Per utilizzare la configurazione centrale, è necessario designare una regione di origine e almeno una regione collegata.

La modifica delle impostazioni di aggregazione tra regioni può influire sulle politiche di configurazione. Quando aggiungi una regione collegata, le tue politiche di configurazione hanno effetto in quella regione. Se la Regione è una [regione opzionale](#), deve essere abilitata affinché le politiche di configurazione abbiano effetto in quella regione. Al contrario, quando rimuovi una regione collegata, le politiche di configurazione non hanno più effetto in quella regione. In quella regione, gli account mantengono le impostazioni che avevano quando la regione collegata è stata rimossa. È possibile modificare tali impostazioni, ma è necessario farlo separatamente in ogni account e regione.

Se si rimuove o si modifica la regione di origine, i criteri di configurazione e le associazioni di criteri vengono eliminati. Non è più possibile utilizzare la configurazione centrale o creare politiche di configurazione in nessuna regione. Gli account mantengono le impostazioni che avevano prima che la regione di origine venisse modificata o rimossa. È possibile modificare tali impostazioni in qualsiasi momento, ma poiché non si utilizza più la configurazione centrale, le impostazioni devono essere modificate separatamente in ogni account e regione. È possibile utilizzare la configurazione centrale e creare nuovamente politiche di configurazione se si designa una nuova regione di residenza.

Per ulteriori informazioni sulla configurazione centrale, vedere [Come funziona la configurazione centrale](#).

Abilitazione dell'aggregazione tra regioni

È necessario abilitare l'aggregazione tra regioni dalla regione Regione AWS che si desidera designare come area di aggregazione.

Non è possibile utilizzare una regione disattivata per impostazione predefinita come regione di aggregazione. Per un elenco delle regioni disabilitate per impostazione predefinita, vedi [Abilitazione di una regione](#) in *Riferimenti generali di AWS*

Abilitazione dell'aggregazione tra regioni (console)

Quando abiliti l'aggregazione tra regioni, scegli le regioni collegate. Puoi anche scegliere se collegare automaticamente le nuove regioni quando Security Hub inizia a supportarle e le hai accettate.

Per abilitare l'aggregazione tra regioni

1. [Apri la AWS Security Hub console all'indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Utilizzando il Regione AWS selettore, accedi alla regione che desideri utilizzare come regione di aggregazione.
3. Nel menu di navigazione di Security Hub, scegli Impostazioni e poi Regioni.
4. Per Trovare l'aggregazione, scegli Configura l'aggregazione dei risultati.

Per impostazione predefinita, la regione di aggregazione è impostata su Nessuna regione di aggregazione.

5. In Regione di aggregazione, selezionate l'opzione per designare la regione corrente come regione di aggregazione.
6. Facoltativamente, per le regioni collegate, selezionare le regioni da cui aggregare i dati.
7. Per aggregare automaticamente i dati provenienti da nuove regioni nella partizione supportate da Security Hub e attivarle, seleziona Collega regioni future.
8. Selezionare Salva.

Abilitazione dell'aggregazione tra regioni (API Security Hub,) AWS CLI

Puoi utilizzare l'API Security Hub per abilitare l'aggregazione tra regioni.

Per abilitare l'aggregazione tra regioni dall'API Security Hub, crei un aggregatore di ricerca. È necessario creare l'aggregatore di ricerca dalla regione che si desidera utilizzare come regione di aggregazione.

Per creare l'aggregatore di risultati (Security Hub API, AWS CLI)

- API Security Hub: dalla regione che desideri utilizzare come regione di aggregazione, usa l'[CreateFindingAggregator](#) operazione. Infatti `RegionLinkingMode`, puoi scegliere tra le seguenti opzioni:
 - ALL_REGIONS— Security Hub aggrega i dati di tutte le regioni. Security Hub aggrega anche i dati provenienti da nuove regioni man mano che sono supportate e l'utente le accetta.

- **ALL_REGIONS_EXCEPT_SPECIFIED**— Security Hub aggrega i dati di tutte le regioni ad eccezione delle regioni che si desidera escludere. Security Hub aggrega anche i dati provenienti da nuove regioni man mano che sono supportate e l'utente le accetta. `RegionsDa` utilizzare per fornire l'elenco delle regioni da escludere dall'aggregazione.
- **SPECIFIED_REGIONS**— Security Hub aggrega i dati da un elenco selezionato di regioni. Security Hub non aggrega automaticamente i dati provenienti da nuove regioni. `RegionsDa` utilizzare per fornire l'elenco delle regioni da cui eseguire l'aggregazione.
- **AWS CLI**: alla riga di comando, esegui il comando [create-finding-aggregator](#). Separa ogni regione con uno spazio.

```
aws securityhub create-finding-aggregator --region <aggregation Region> --region-linking-mode ALL_REGIONS | ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --regions <Region List>
```

Nell'esempio seguente, l'aggregazione tra regioni è configurata per regioni selezionate. La regione di aggregazione è Stati Uniti orientali (Virginia settentrionale). Le regioni collegate sono Stati Uniti occidentali (California settentrionale) e Stati Uniti occidentali (Oregon).

```
aws securityhub create-finding-aggregator --region us-east-1 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Visualizzazione delle impostazioni di aggregazione tra regioni

È possibile visualizzare l'attuale configurazione di aggregazione interregionale da qualsiasi regione. La configurazione include la regione di aggregazione, le regioni collegate e se collegare automaticamente nuove regioni.

Visualizzazione della configurazione di aggregazione tra regioni (console)

La scheda Regioni della pagina Impostazioni mostra la configurazione corrente di aggregazione tra regioni. È possibile visualizzare la configurazione da qualsiasi regione. Gli account membro possono anche visualizzare la configurazione interregionale configurata dall'account amministratore.

Se l'aggregazione tra regioni non è abilitata, nella scheda Regioni viene visualizzata l'opzione per abilitare l'aggregazione tra regioni. Per informazioni, consulta [the section called “Abilitazione dell'aggregazione tra regioni”](#). Solo gli account amministratore e gli account autonomi possono abilitare l'aggregazione tra regioni.

Se l'aggregazione tra regioni è abilitata, la scheda Regioni visualizza le seguenti informazioni:

- La regione di aggregazione
- Se aggregare automaticamente risultati, approfondimenti, stati di controllo e punteggi di sicurezza provenienti da nuove aree supportate da Security Hub e a cui l'utente ha aderito
- L'elenco delle regioni collegate

Visualizzazione dell'attuale configurazione di aggregazione tra regioni (API Security Hub,) AWS CLI

È possibile utilizzare l'API Security Hub o AWS CLI visualizzare l'attuale configurazione di aggregazione tra regioni. È possibile visualizzare la configurazione di aggregazione tra regioni da qualsiasi regione.

Per visualizzare l'attuale configurazione di aggregazione tra regioni (API Security Hub,) AWS CLI

- API Security Hub: utilizza l'[GetFindingAggregator](#) API. Quando si effettua la richiesta, è necessario fornire l'ARN dell'aggregatore di ricerca. Per ottenere l'aggregatore di ricerca ARN, utilizzare. [ListFindingAggregators](#)
- AWS CLI: alla riga di comando, esegui il comando [get-finding-aggregator](#). Per ottenere l'aggregatore di ricerca ARN, utilizzare. [list-finding-aggregators](#)

```
aws securityhub get-finding-aggregator --finding-aggregator-arn <finding aggregator ARN>
```

Aggiornamento della configurazione di aggregazione tra regioni

Puoi aggiornare la configurazione di aggregazione tra regioni per modificare il collegamento Regioni AWS per la regione di aggregazione corrente. Puoi anche decidere se aggregare automaticamente risultati, approfondimenti, stati di controllo e punteggi di sicurezza provenienti da nuove regioni.

Le modifiche all'aggregazione tra aree geografiche non vengono implementate per una regione che richiede l'attivazione fino a quando la regione non viene abilitata in una. Account AWS Le regioni AWS introdotte a partire dal 20 marzo 2019 o in data successiva sono regioni opt-in.

Quando si interrompe l'aggregazione dei dati da una regione collegata, Security Hub non rimuove alcun dato aggregato esistente dalla regione di aggregazione.

Non è possibile utilizzare il processo di aggiornamento per modificare la regione di aggregazione. Per modificare la regione di aggregazione, devi fare quanto segue:

1. Interrompi l'aggregazione tra regioni. Per informazioni, consulta [the section called “Interruzione dell'aggregazione tra regioni”](#).
2. Passa alla regione che desideri utilizzare come nuova regione di aggregazione.
3. Abilita l'aggregazione tra regioni. Per informazioni, consulta [the section called “Abilitazione dell'aggregazione tra regioni”](#).

Aggiornamento della configurazione di aggregazione tra regioni (console)

È necessario aggiornare la configurazione di aggregazione tra regioni dalla regione di aggregazione corrente.

Regioni AWS Oltre alla regione di aggregazione, il pannello Finding aggregation visualizza un messaggio che indica che è necessario modificare la configurazione nella regione di aggregazione. Scegliete questo messaggio per visualizzare un collegamento per accedere alla regione di aggregazione.

Per modificare le regioni collegate per la regione di aggregazione corrente

1. Apri la AWS Security Hub console all'indirizzo <https://console.aws.amazon.com/securityhub/>.
2. Passa alla regione di aggregazione corrente.
3. Nel menu di navigazione di Security Hub, scegli Impostazioni, quindi scegli Regioni.
4. In Ricerca di aggregazione, scegli Modifica.
5. In Regioni collegate, aggiorna le aree collegate selezionate.
6. Se necessario, cambia se è selezionata l'opzione Collega regioni future. Questa impostazione determina se Security Hub collega automaticamente le nuove regioni man mano che ne aggiunge il supporto e l'utente le accetta.
7. Selezionare Salva.

Aggiornamento della configurazione di aggregazione tra regioni (API Security Hub,) AWS CLI

Puoi utilizzare l'API Security Hub o AWS CLI aggiornare la configurazione di aggregazione tra regioni. È necessario aggiornare l'aggregazione tra regioni dalla regione di aggregazione corrente.

È possibile modificare la modalità di collegamento della regione. Se la modalità di collegamento è `ALL_REGIONS_EXCEPT_SPECIFIED` o `SPECIFIED_REGIONS`, è possibile modificare l'elenco delle regioni escluse o incluse.

Quando si modifica l'elenco delle regioni escluse o incluse, è necessario fornire l'elenco completo con gli aggiornamenti. Ad esempio, supponiamo che attualmente tu voglia aggregare i risultati degli Stati Uniti orientali (Ohio) e di voler aggregare anche i risultati degli Stati Uniti occidentali (Oregon). Quando chiami [UpdateFindingAggregator](#), fornisci un Regions elenco che contiene sia Stati Uniti orientali (Ohio) che Stati Uniti occidentali (Oregon).

Per aggiornare l'aggregazione tra regioni (API Security Hub,) AWS CLI

- API Security Hub: utilizza l'operazione [UpdateFindingAggregator](#) API. Per identificare l'aggregatore di risultati, è necessario fornire l'ARN dell'aggregatore di risultati. Per ottenere l'aggregatore di ricerca ARN, utilizzare. [ListFindingAggregators](#)

Fornisci la modalità di collegamento della regione e l'elenco aggiornato delle regioni escluse o incluse.

- AWS CLI: alla riga di comando, esegui il comando [update-finding-aggregator](#). Separa ogni regione con uno spazio.

```
aws securityhub update-finding-aggregator --region <aggregation Region> --finding-aggregator-arn <finding aggregator ARN> --region-linking-mode ALL_REGIONS | ALL_REGIONS_EXCEPT_SPECIFIED | SPECIFIED_REGIONS --regions <Region list>
```

Nell'esempio seguente, la configurazione di aggregazione tra regioni viene modificata in aggregazione per regioni selezionate. Il comando viene eseguito dalla regione di aggregazione corrente, che è Stati Uniti orientali (Virginia settentrionale). Le regioni collegate sono Stati Uniti occidentali (California settentrionale) e Stati Uniti occidentali (Oregon).

```
aws securityhub update-finding-aggregator --region us-east-1 --finding-aggregator-arn arn:aws:securityhub:us-east-1:222222222222:finding-aggregator/123e4567-e89b-12d3-a456-426652340000 --region-linking-mode SPECIFIED_REGIONS --regions us-west-1 us-west-2
```

Interruzione dell'aggregazione tra regioni

Interrompi l'aggregazione tra regioni se non desideri più aggregare i dati o se desideri modificare la regione di aggregazione.

Quando interrompi l'aggregazione tra regioni, Security Hub interrompe l'aggregazione dei dati. Non rimuove alcun dato aggregato esistente dalla regione di aggregazione.

Interruzione dell'aggregazione tra regioni (console)

È necessario interrompere l'aggregazione tra regioni dalla regione di aggregazione corrente.

Nelle regioni diverse dalla regione di aggregazione, il pannello Alla ricerca dell'aggregazione visualizza un messaggio che indica che è necessario modificare la configurazione nella regione di aggregazione. Scegliete questo messaggio per visualizzare un collegamento per passare alla regione di aggregazione.

Per interrompere l'aggregazione tra regioni

1. [Apri la AWS Security Hub console all'indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Passa alla regione di aggregazione corrente.
3. Nel menu di navigazione di Security Hub, scegli Impostazioni, quindi scegli Regioni.
4. In Ricerca di aggregazione, scegli Modifica.
5. In Regione di aggregazione, scegli Nessuna regione di aggregazione.
6. Selezionare Salva.
7. Nella finestra di dialogo di conferma, nel campo di conferma, digita. **Confirm**
8. Scegli Conferma.

Interruzione dell'aggregazione tra regioni (API Security Hub,) AWS CLI

Puoi utilizzare l'API Security Hub per interrompere l'aggregazione tra regioni. È necessario interrompere l'aggregazione tra regioni dalla regione di aggregazione.

Per interrompere l'aggregazione tra regioni (API Security Hub,) AWS CLI

- API Security Hub: utilizza l'[DeleteFindingAggregator](#) operazione. Per identificare l'aggregatore di risultati da eliminare, fornisci l'ARN dell'aggregatore di risultati. Per ottenere l'aggregatore di ricerca ARN, utilizzare. [ListFindingAggregators](#)

- AWS CLI: alla riga di comando, esegui il comando [delete-finding-aggregator](#).

```
aws securityhub delete-finding-aggregator <finding aggregator ARN> --  
region <aggregation Region>
```

Risultati in AWS Security Hub

AWS Security Hub elimina la complessità di gestire grandi volumi di risultati provenienti da più provider. Riduce lo sforzo richiesto per gestire e migliorare la sicurezza di tutte le risorse e i carichi di lavoro. Account AWS

Security Hub riceve i risultati dalle seguenti fonti.

- Security Hub verifica i controlli abilitati. Per informazioni, consulta [the section called “Generazione e aggiornamento dei risultati del controllo”](#).
- Integrazioni con Servizi AWS cui abiliti. Per informazioni, consulta [the section called “Servizio AWS integrazioni”](#).
- Integrazioni con prodotti di terze parti abilitati. Per informazioni, consulta [the section called “Integrazioni di prodotti di terze parti”](#).
- Integrazioni personalizzate configurate. Per informazioni, consulta [the section called “Utilizzo di integrazioni di prodotti personalizzate”](#).

Security Hub utilizza i risultati utilizzando un formato di risultati standard chiamato AWS Security Finding Format. Per ulteriori informazioni sul formato dei risultati, consulta [the section called “Formato dei risultati”](#).

Security Hub mette in correlazione i risultati tra i prodotti integrati per dare priorità a quelli più importanti.

I provider di risultati possono aggiornare i risultati per riflettere ulteriori istanze del risultato. Puoi aggiornare i risultati per fornire dettagli sulla tua indagine e sui risultati.

Security Hub consente inoltre di aggregare i risultati tra le regioni, in modo da poter visualizzare tutti i risultati da un'unica posizione. Per informazioni, consulta [Aggregazione tra regioni](#).

Argomenti

- [Creazione e aggiornamento dei risultati in AWS Security Hub](#)
- [Gestione e revisione dei dettagli e della cronologia dei risultati](#)
- [Intervenire in base ai risultati in AWS Security Hub](#)
- [AWS Formato ASFF \(Security Finding Format\)](#)

Creazione e aggiornamento dei risultati in AWS Security Hub

Nel AWS Security Hub, un risultato può provenire da uno dei seguenti tipi di fornitori di ricerca.

- Un controllo di sicurezza abilitato in Security Hub
- Un'integrazione abilitata con un altro Servizio AWS
- Un'integrazione abilitata con un prodotto di terze parti

Una volta creato un risultato, può essere aggiornato dal provider di risultati o dal cliente.

- Il provider di risultati utilizza l'operazione API [BatchImportFindings](#) per aggiornare le informazioni generali su un risultato. I provider di risultati possono aggiornare solo i risultati che hanno creato.
- Il cliente utilizza il funzionamento dell'[BatchUpdateFindings](#) API per aggiornare lo stato dell'indagine su un risultato. [BatchUpdateFindings](#) può essere utilizzato anche da uno strumento di ticketing, gestione degli incidenti, orchestrazione, riparazione o SIEM per conto del cliente.

Dalla console Security Hub, i clienti possono gestire lo stato dei risultati del flusso di lavoro e inviare i risultati ad azioni personalizzate. Per informazioni, consulta [the section called “Intervenire in base ai risultati”](#).

Security Hub inoltre aggiorna ed elimina automaticamente i risultati. Tutti i risultati vengono eliminati automaticamente se non sono stati aggiornati negli ultimi 90 giorni.

Se abiliti l'aggregazione tra regioni, Security Hub aggrega automaticamente i nuovi risultati dalle regioni collegate alla regione di aggregazione. Security Hub replica anche gli aggiornamenti dei risultati. Gli aggiornamenti che si verificano nelle regioni collegate vengono replicati nella regione di aggregazione. Gli aggiornamenti che si verificano nella regione di aggregazione vengono replicati nella regione collegata. Per ulteriori informazioni sull'aggregazione tra regioni, vedere. [Aggregazione tra regioni](#)

Argomenti

- [Utilizzo di BatchImportFindings per creare e aggiornare i risultati](#)
- [Utilizzo di BatchUpdateFindings per aggiornare un risultato](#)

Utilizzo di BatchImportFindings per creare e aggiornare i risultati

I provider di risultati utilizzano l'operazione API [BatchImportFindings](#) per creare nuovi risultati e aggiornare le informazioni sui risultati creati. Non possono aggiornare i risultati che non hanno creato.

I clienti, i SIEM, gli strumenti di ticketing e gli strumenti SOAR li utilizzano [BatchUpdateFindings](#) per apportare aggiornamenti relativi all'analisi dei risultati ottenuti dalla ricerca dei fornitori. Per informazioni, consulta [the section called "Uso di BatchUpdateFindings"](#).

Ogni volta che AWS Security Hub riceve una BatchImportFindings richiesta per creare o aggiornare un risultato, genera automaticamente un Security Hub Findings - Importedevento in Amazon EventBridge. Per informazioni, consulta [the section called "Risposta e correzione automatizzate"](#).

Requisiti per gli account e le dimensioni dei lotti

BatchImportFindings deve essere chiamato da uno dei seguenti:

- L'account associato ai risultati. L'identificatore dell'account associato è il valore dell'AwsAccountId attribuito per il risultato.
- Un account che è nella lista consentita per l'integrazione ufficiale dei partner di Security Hub.

Security Hub può accettare la ricerca di aggiornamenti solo per gli account con Security Hub abilitato. Anche il provider di risultati deve essere abilitato. Se Security Hub è disabilitato o l'integrazione del provider di ricerca non è abilitata, i risultati vengono restituiti nell'FailedFindingselenco, con un InvalidAccess errore.

BatchImportFindings accetta fino a 100 risultati per batch, fino a 240 KB per risultato e fino a 6 MB per batch. Il limite di velocità di accelerazione è di 10 TPS per account per regione, con un picco di 30 TPS.

Determinazione per creare o aggiornare un risultato

Per determinare se creare o aggiornare un risultato, Security Hub controlla il ID campo. Se il valore di ID non corrisponde a un risultato esistente, viene creato un nuovo risultato.

Se ID corrisponde a un risultato esistente, Security Hub controlla il UpdatedAt campo per l'aggiornamento.

- Se UpdatedAt l'aggiornamento corrisponde o si verifica UpdatedAt in precedenza sul risultato esistente, l'aggiornamento viene ignorato.
- Se il campo UpdatedAt nell'aggiornamento è successivo al campo UpdatedAt del risultato esistente, il risultato esistente viene aggiornato.

Attributi limitati per BatchImportFindings

Per un risultato esistente, i provider di ricerca non possono utilizzare BatchImportFindings per aggiornare i seguenti attributi e oggetti. Questi attributi possono essere aggiornati solo utilizzando BatchUpdateFindings.

- Note
- UserDefinedFields
- VerificationState
- Workflow

Security Hub ignora qualsiasi contenuto fornito in una BatchImportFindings richiesta per tali attributi e oggetti. I clienti, o altri fornitori che agiscono per loro conto, BatchUpdateFindings li aggiornano.

Uso di FindingProviderFields

Inoltre, Finding Provider non dovrebbe BatchImportFindings utilizzare la funzione di aggiornamento dei seguenti attributi.

- Confidence
- Criticality
- RelatedFindings
- Severity
- Types

Invece, i provider di ricerca utilizzano l'[FindingProviderFields](#) oggetto per fornire valori per questi attributi.

Esempio

```

"FindingProviderFields": {
  "Confidence": 42,
  "Criticality": 99,
  "RelatedFindings": [
    {
      "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000"
    }
  ],
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}

```

Per `BatchImportFindings` le richieste, Security Hub gestisce i valori negli attributi di primo livello e nel modo [FindingProviderFields](#) seguente.

(Preferito) **BatchImportFindings** fornisce un valore per un attributo in [FindingProviderFields](#), ma non fornisce un valore per l'attributo di primo livello corrispondente.

Ad esempio `FindingProviderFields.Confidence`, `BatchImportFindings` fornisce ma non fornisce `Confidence`. Questa è l'opzione preferita per `BatchImportFindings` le richieste.

Security Hub aggiorna il valore dell'attributo in `FindingProviderFields`.

Replica il valore nell'attributo di primo livello solo se l'attributo non è già stato aggiornato da `BatchUpdateFindings`

BatchImportFindings fornisce un valore per un attributo di primo livello, ma non fornisce un valore per l'attributo corrispondente in **FindingProviderFields**

Ad esempio `Confidence`, `BatchImportFindings` fornisce ma non fornisce `FindingProviderFields.Confidence`.

Security Hub utilizza il valore per aggiornare l'attributo in `FindingProviderFields`. Sovrascrive qualsiasi valore esistente.

Security Hub aggiorna l'attributo di primo livello solo se l'attributo non è già stato aggiornato da `BatchUpdateFindings`.

BatchImportFindings fornisce un valore sia per un attributo di primo livello che per l'attributo corrispondente in **FindingProviderFields**

Ad esempio, **BatchImportFindings** fornisce entrambi **Confidence** e **FindingProviderFields.Confidence**.

Per una nuova scoperta, Security Hub utilizza il valore in **FindingProviderFields** per compilare sia l'attributo di primo livello che l'attributo corrispondente in.

FindingProviderFields Non utilizza il valore dell'attributo di primo livello fornito.

Per un risultato esistente, Security Hub utilizza entrambi i valori. Tuttavia, aggiorna il valore dell'attributo di primo livello solo se l'attributo non è già stato aggiornato da **BatchUpdateFindings**.

Utilizzando il `batch-import-findings` comando di AWS CLI

In AWS Command Line Interface, si utilizza il [batch-import-findings](#) comando per creare o aggiornare i risultati.

Fornisci ogni risultato come oggetto JSON.

Esempio

```
aws securityhub batch-import-findings --findings
  [{
    "AwsAccountId": "123456789012",
    "CreatedAt": "2019-08-07T17:05:54.832Z",
    "Description": "Vulnerability in a CloudTrail trail",
    "GeneratorId": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/
v/1.2.0/rule/2.2",
    "Id": "Id1",
    "ProductArn": "arn:aws:securityhub:us-west-1:123456789012:product/123456789012/
default",
    "Resources": [
      {
        "Id": "arn:aws:cloudtrail:us-west-1:123456789012:trail/TrailName",
        "Partition": "aws",
        "Region": "us-west-1",
        "Type": "AwsCloudTrailTrail"
      }
    ]
  },
```

```

    "SchemaVersion": "2018-10-08",
    "Title": "CloudTrail trail vulnerability",
    "UpdatedAt": "2020-06-02T16:05:54.832Z",
    "Types": [
      "Software and Configuration Checks/Vulnerabilities/CVE"
    ],
    "Severity": {
      "Label": "INFORMATIONAL",
      "Original": "0"
    }
  }
}]'

```

Utilizzo di BatchUpdateFindings per aggiornare un risultato

L'[BatchUpdateFindings](#) azione viene utilizzata per aggiornare le informazioni relative all'elaborazione da parte di un cliente dei risultati della ricerca dei fornitori. Può essere utilizzata da un cliente o da uno strumento SIEM, di ticketing, di gestione degli incidenti o SOAR che opera per conto di un cliente. È possibile utilizzare BatchUpdateFindings per aggiornare campi specifici nel AWS Security Finding Format (ASFF).

Non è possibile BatchUpdateFindings utilizzarlo per creare nuovi risultati. Puoi usarlo per aggiornare fino a 100 risultati alla volta.

Ogni volta che Security Hub riceve una BatchUpdateFindings richiesta di aggiornamento di un risultato, genera automaticamente un Security Hub Findings - Importedevento in Amazon EventBridge. Per informazioni, consulta [the section called "Risposta e correzione automatizzate"](#).

BatchUpdateFindings non modifica il UpdatedAt campo per la ricerca. UpdatedAt riflette solo l'aggiornamento più recente del fornitore dei risultati.

Campi disponibili per BatchUpdateFindings

Gli account amministratore possono utilizzare > BatchUpdateFindings per aggiornare i risultati relativi al proprio account o agli account dei membri. Gli account dei membri possono utilizzare > BatchUpdateFindings per aggiornare i risultati relativi al proprio account.

I clienti possono utilizzare > solo BatchUpdateFindings per aggiornare i seguenti campi e oggetti.

- Confidence
- Criticality

- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

Per impostazione predefinita, gli account amministratore e membro hanno accesso a tutti i campi e i valori dei campi sopra indicati. Security Hub fornisce anche chiavi contestuali per consentire di limitare l'accesso ai campi e ai valori dei campi.

Ad esempio, è possibile consentire solo l'impostazione degli account dei membri `Workflow.Status` su `RESOLVED`. Oppure potresti non voler consentire la modifica degli account dei membri `Severity.Label`.

Configurazione dell'accesso a `BatchUpdateFindings`

Puoi configurare le policy IAM per limitare l'accesso all'utilizzo `BatchUpdateFindings` per aggiornare campi e valori dei campi.

In un'istruzione a cui limitare l'accesso `BatchUpdateFindings`, utilizza i seguenti valori:

- Action è `securityhub:BatchUpdateFindings`
- Effect è `Deny`
- InfattiCondition, puoi rifiutare una `BatchUpdateFindings` richiesta in base a quanto segue:
 - La scoperta include un campo specifico.
 - Il risultato include un valore di campo specifico.

Chiavi di condizione

Queste sono le chiavi condizionali per limitare l'accesso a `BatchUpdateFindings`.

Campo ASFF

La chiave di condizione per un campo ASFF è la seguente:

```
securityhub:ASFFSyntaxPath/<fieldName>
```

Sostituisci *<fieldName>* con il campo ASFF. Quando configuri l'accesso a `BatchUpdateFindings`, includi uno o più campi ASFF specifici nella tua policy IAM anziché un campo a livello principale. Ad esempio, per limitare l'accesso al `Workflow.Status` campo, devi includere `securityhub:ASFFSyntaxPath/Workflow.Status` nella tua policy anziché il campo a livello principale. `Workflow`

Impedire tutti gli aggiornamenti a un campo

Per impedire a un utente di apportare aggiornamenti a un campo specifico, utilizza una condizione come questa:

```
"Condition": {
    "Null": {
        "securityhub:ASFFSyntaxPath/<fieldName>": "false"
    }
}
```

Ad esempio, la seguente dichiarazione indica che `BatchUpdateFindings` può essere utilizzata per aggiornare lo stato del flusso di lavoro.

```
{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "Null": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": "false"
    }
  }
}
```

Non consentire valori di campo specifici

Per impedire a un utente di impostare un campo su un valore specifico, usa una condizione come questa:

```
"Condition": {
```

```

        "StringEquals": {
            "securityhub:ASFFSyntaxPath/<fieldName>": "<fieldValue>"
        }
    }

```

Ad esempio, la seguente istruzione indica che non `BatchUpdateFindings` può essere utilizzata per `Workflow.Status` impostare su `SUPPRESSED`.

```

{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": "SUPPRESSED"
    }
  }
}

```

Puoi anche fornire un elenco di valori non consentiti.

```

"Condition": {
  "StringEquals": {
    "securityhub:ASFFSyntaxPath/<fieldName>": [ "<fieldValue1>",
    "<fieldValue2>", "<fieldValue3>" ]
  }
}

```

Ad esempio, la seguente dichiarazione indica che non `BatchUpdateFindings` può essere utilizzata per `Workflow.Status` impostare uno dei due `RESOLVED` valori `SUPPRESSED`.

```

{
  "Sid": "VisualEditor0",
  "Effect": "Deny",
  "Action": "securityhub:BatchUpdateFindings",
  "Resource": "*",
  "Condition": {
    "StringEquals": {
      "securityhub:ASFFSyntaxPath/Workflow.Status": [
        "RESOLVED",
        "NOTIFIED"
      ]
    }
  }
}

```

```
}
}
```

Utilizzando il batch-update-findings comando di AWS CLI

In AWS Command Line Interface, si utilizza il [batch-update-findings](#) comando per aggiornare i risultati.

Per ogni risultato da aggiornare, fornisci sia l'ID del risultato che l'ARN del prodotto che ha generato il risultato.

```
--finding-identifiers ID="<findingID1>",ProductArn="<productARN>"
ID="<findingID2>",ProductArn="<productARN2>"
```

Quando fornisci gli attributi da aggiornare, puoi utilizzare un formato JSON o un formato di scelta rapida.

Ecco un esempio di aggiornamento dell'Note oggetto che utilizza il formato JSON:

```
--note '{"Text": "Known issue that is not a risk.", "UpdatedBy": "user1"}'
```

Ecco lo stesso aggiornamento che utilizza il formato di scelta rapida:

```
--note Text="Known issue that is not a risk.",UpdatedBy="user1"
```

Il AWS CLI Command Reference fornisce la sintassi JSON e la scorciatoia per ogni campo.

L'batch-update-findings esempio seguente > aggiorna due risultati per aggiungere una nota, modificare l'etichetta di gravità e risolverli.

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-2::product/aws/securityhub" Id="arn:aws:securityhub:us-west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --note '{"Text": "Known issue that is not a risk.", "UpdatedBy": "user1"}' --severity '{"Label": "LOW"}' --workflow '{"Status": "RESOLVED"}'
```

Questo è lo stesso esempio, ma utilizza le scorciatoie anziché JSON.

```
aws securityhub batch-update-findings --finding-identifiers Id="arn:aws:securityhub:us-west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" Id="arn:aws:securityhub:us-west-1:123456789012:subscription/pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --note Text="Known issue that is not a risk.",UpdatedBy="user1" --severity Label="LOW" --workflow Status="RESOLVED"
```

Gestione e revisione dei dettagli e della cronologia dei risultati

Esistono diversi modi per visualizzare gli elenchi dei risultati sulla AWS Security Hub console:

- **Pagina dei risultati:** mostra un elenco completo dei risultati di tutti i controlli abilitati e le integrazioni di prodotti. Per impostazione predefinita, vengono visualizzati i risultati attivi con uno stato NOTIFIED del flusso di lavoro NEW o uno.
- **Pagina dei dettagli del controllo:** visualizza un elenco di risultati generati nelle ultime 24 ore per un controllo specifico.
- **Pagina Insights:** visualizza un elenco di risultati per un'analisi corrispondente. Un'analisi è un risultato specifico di una raccolta. Per ulteriori informazioni, consulta [the section called “Visualizzazione dei risultati e dei risultati di informazione dettagliata”](#).
- **Pagina delle integrazioni:** mostra un elenco di risultati generati da un prodotto integrato Servizio AWS o di terze parti.

Puoi filtrare e raggruppare i risultati in questi elenchi per concentrarti su tipi specifici di risultati. Puoi anche selezionare un risultato specifico nelle pagine precedenti per visualizzarne i dettagli.

Per visualizzare un elenco di risultati a livello di codice, utilizza il [GetFindings](#) funzionamento dell'API Security Hub. È possibile includere filtri per recuperare tipi specifici di risultati.

Se abiliti l'aggregazione tra regioni, puoi recuperare stati di controllo, punteggi di sicurezza, approfondimenti e risultati da tutte le regioni. Nella regione di aggregazione, i dati di ricerca includono i dati della regione di aggregazione e delle regioni collegate. In altre regioni, i dati di ricerca sono specifici solo per quella regione. Per informazioni sulla configurazione dell'aggregazione tra regioni, vedere. [Aggregazione tra regioni](#)

Filtraggio e raggruppamento dei risultati (console)

Quando si visualizza un elenco di risultati nella pagina Risultati, nella pagina Integrazioni o nella pagina Insights della console Security Hub, l'elenco viene prefiltrato in base allo stato del record e allo stato del flusso di lavoro. Questo si aggiunge ai filtri per un'analisi o un'integrazione.

Lo stato del record indica se un risultato è attivo o archiviato. Per impostazione predefinita, un elenco di risultati mostra solo i risultati attivi. Un risultato può essere archiviato dal fornitore dei risultati. AWS Security Hub inoltre, archivia automaticamente i risultati del controllo se la risorsa associata viene eliminata.

Lo stato del flusso di lavoro indica lo stato di un'indagine su un risultato. Per impostazione predefinita, un elenco di risultati mostra solo risultati con uno stato del flusso di lavoro NEW o NOTIFIED. È possibile aggiornare lo stato del flusso di lavoro di un risultato.

Se hai abilitato l'aggregazione dei risultati e hai effettuato l'accesso alla regione di aggregazione, puoi filtrare i risultati per regione nelle pagine Findings e Insights.

Per informazioni sull'utilizzo dei risultati del controllo, consulta [the section called “Filtraggio e ordinamento dei risultati”](#) Le informazioni contenute in questa pagina si riferiscono alla ricerca di elenchi nelle pagine Findings, Insights e Integrations.

Aggiunta di filtri

Per modificare l'ambito dell'elenco, è possibile aggiungere i filtri.

Puoi filtrare in base a un massimo di 10 attributi. Per ogni attributo, puoi fornire fino a 20 valori di filtro.

Quando filtra l'elenco dei risultati, Security Hub applica la logica AND al set di filtri. In altre parole, un risultato corrisponde solo se corrisponde a tutti i filtri forniti. Ad esempio, se si aggiunge GuardDuty come filtro per il nome del prodotto e AwsS3Bucket come filtro per il tipo di risorsa, i risultati corrispondenti devono soddisfare entrambi questi criteri.

Tuttavia, Security Hub applica la logica OR ai filtri che utilizzano lo stesso attributo ma valori diversi. Ad esempio, aggiungi entrambi GuardDuty e Amazon Inspector come valori di filtro per il nome del prodotto. In tal caso, un risultato corrisponde se è stato generato da uno dei due GuardDuty o da Amazon Inspector.

Per aggiungere un filtro all'elenco di risultati

1. Apri la AWS Security Hub console all'indirizzo <https://console.aws.amazon.com/securityhub/>.
2. Per visualizzare un elenco dei risultati, effettuate una delle seguenti operazioni:
 - Nel riquadro di navigazione di Security Hub, scegli Findings.
 - Nel riquadro di navigazione Security Hub, scegli Insights. Scegli un approfondimento. Quindi, nell'elenco dei risultati, scegli un risultato approfondito.
 - Nel riquadro di navigazione Security Hub, scegli Integrazioni. Scegli Vedi i risultati per un'integrazione.
3. Nella casella Aggiungi filtri, per Filtri, scegli un filtro.

Quando filtri in base al nome dell'azienda o al nome del prodotto, la console utilizza il livello `CompanyName` e `ProductName` i campi principali. L'API utilizza i valori presenti in `ProductFields`.

4. Scegliere il tipo di corrispondenza del filtro.

Per un filtro a stringa, puoi scegliere tra le seguenti opzioni di confronto:

- è: trova un valore che corrisponda esattamente al valore del filtro.
- inizia con: trova un valore che inizi con il valore del filtro.
- non è: trova un valore che non corrisponde al valore del filtro.
- non inizia con: trova un valore che non inizia con il valore del filtro.

Per un filtro numerico, puoi scegliere se fornire un numero singolo (Semplice) o un intervallo di numeri (Intervallo).

Per un filtro di data o ora, puoi scegliere se fornire un intervallo di tempo compreso tra la data e l'ora correnti (finestra scorrevole) o un intervallo di date specifico (intervallo fisso).

L'aggiunta di più filtri comporta le seguenti interazioni:

- is e inizia con i filtri sono uniti da OR. Un valore corrisponde se contiene uno qualsiasi dei valori del filtro. Ad esempio, se si specifica che l'etichetta di gravità è CRITICA e l'etichetta di gravità è ALTA, i risultati includono sia i risultati critici che quelli ad alta gravità.
- non è e non inizia con i filtri vengono uniti da AND. Un valore corrisponde solo se non contiene **nessuno di questi valori di filtro**. Ad esempio, se si specifica che l'etichetta di gravità non è

LOW e l'etichetta di severità non è MEDIUM, i risultati non includono i risultati di gravità bassa o media.

Se hai un filtro is su un campo, non puoi avere un filtro is no o un non inizia con un filtro sullo stesso campo.

5. Specificare il valore del filtro.

Per i filtri a stringa, il valore del filtro fa distinzione tra maiuscole e minuscole.

Ad esempio, per i risultati di Security Hub, il nome del prodotto è Security Hub. Se si utilizza l'operatore EQUALS per visualizzare i risultati di Security Hub, è necessario immettere **Security Hub** come valore del filtro. Se si immette **security hub**, non vengono visualizzati risultati.

Allo stesso modo, se si utilizza l'operatore PREFIX e si immette **Sec**, vengono visualizzati i risultati del Security Hub. Se si inserisce **sec**, non viene visualizzato alcun risultato del Security Hub.

6. Scegli Applica.

Raggruppamento dei risultati

Oltre a modificare i filtri, è possibile raggruppare i risultati in base ai valori di un attributo selezionato.

Quando si raggruppano i risultati, l'elenco dei risultati viene sostituito con un elenco di valori per l'attributo selezionato nei risultati corrispondenti. Per ogni valore, l'elenco mostra il numero di risultati che corrispondono agli altri criteri di filtro.

Ad esempio, se si raggruppano i risultati per Account AWS ID, viene visualizzato un elenco di identificatori di account, con il numero di risultati corrispondenti per ogni account.

Tieni presente che Security Hub può visualizzare solo 100 valori. Se sono presenti più di 100 valori di raggruppamento, vengono visualizzati solo i primi 100.

Quando si sceglie un valore di attributo, viene visualizzato l'elenco dei risultati corrispondenti per quel valore.

Per raggruppare i risultati in un elenco di risultati

1. Nell'elenco dei risultati, seleziona la casella Aggiungi filtri.

2. Per Raggruppamento, scegli Raggruppa per.
3. Nell'elenco, scegli l'attributo da utilizzare per il raggruppamento.
4. Scegli Applica.

Modifica del valore di un filtro o di un attributo di raggruppamento

Puoi modificare il valore di filtro per un filtro esistente. È inoltre possibile modificare l'attributo di raggruppamento.

Ad esempio, puoi modificare il filtro Record state (Stato record) per cercare i risultati ARCHIVED anziché i risultati ACTIVE.

Per modificare un filtro o un attributo di raggruppamento

1. In un elenco di risultati filtrato, scegli l'attributo di filtro o di raggruppamento.
2. Per Raggruppa per, scegli il nuovo attributo, quindi scegli Applica.
3. Per un filtro, scegli il nuovo valore, quindi scegli Applica.

Eliminazione di un filtro o di un attributo di raggruppamento

Per eliminare un attributo di filtro o di raggruppamento, scegliete l'icona x.

L'elenco viene aggiornato automaticamente in base alla modifica. Quando rimuovi l'attributo di raggruppamento, l'elenco passa dall'elenco dei valori dei campi a un elenco di risultati.

Informazioni di ricerca disponibili

È possibile ottenere una serie di dettagli sui risultati sulla console di Security Hub o chiamando l'[GetFindings](#) operazione dell'API Security Hub. Di seguito è riportato un elenco parziale dei tipi di dettagli di ricerca che è possibile ottenere.

- **Metadati dell'applicazione:** fornisce il nome e l'Amazon Resource Name (ARN) dell'applicazione coinvolta in una ricerca se hai creato un'applicazione e vi hai aggiunto AWS il tag dell'applicazione. Ti consigliamo di creare applicazioni in [AWS Service Catalog AppRegistry](#)
- **Cronologia dei risultati:** fornisce la cronologia dei risultati negli ultimi 90 giorni.
- **Finding Investigation in Detective (solo console):** fornisce un collegamento per approfondire una scoperta in Detective utilizzando strumenti di raccolta automatica dei log, analisi della sicurezza

ed esplorazione Servizio AWS delle risorse. Queste informazioni sono incluse solo per i risultati di Security Hub ricevuti da altri Servizi AWS se abiliti Detective.

- Campi relativi alla ricerca del fornitore: visualizza i valori del provider di ricerca relativi a confidenza, criticità, risultati correlati, gravità e tipo di risultato.
- Parametri: mostra i valori correnti dei parametri per un controllo di sicurezza. Security Hub utilizza questi valori dei parametri per eseguire i controlli di sicurezza del controllo.
- Correzione: fornisce un collegamento alle istruzioni per correggere i risultati dei controlli non riusciti.
- Risorsa: fornisce informazioni sulla AWS risorsa coinvolta in un risultato.
- Tag delle risorse: forniscono informazioni sulla chiave e sul valore dei tag per le risorse coinvolte in una ricerca. È possibile etichettare [le risorse supportate](#) dal GetResources funzionamento dell'API AWS Resource Groups Tagging. Per ulteriori informazioni sull'inclusione dei tag delle risorse nei risultati, consulta [Tag](#).
- Tipi e risultati correlati: contiene informazioni sul tipo di risultato.
- Dettagli sulla vulnerabilità: informazioni su una vulnerabilità rilevata in un risultato e sui pacchetti interessati. Questi dettagli sono disponibili se abiliti Amazon Inspector per [i risultati che Amazon Inspector invia a Security Hub](#).

Consulta le seguenti sezioni per capire come accedere a questi dettagli per una scoperta.

Revisione della cronologia dei risultati

La cronologia delle ricerche è una funzionalità del Security Hub che consente di tenere traccia delle modifiche apportate a un risultato negli ultimi 90 giorni. È disponibile per i risultati attivi e archiviati. La cronologia delle ricerche fornisce una traccia immutabile delle modifiche apportate a un risultato nel tempo, tra cui la modifica, quando è stata apportata e da quale utente.

In particolare, è possibile tenere traccia delle modifiche apportate ai campi di [AWS Formato ASFF \(Security Finding Format\)](#). Security Hub tiene traccia delle modifiche apportate manualmente e con [regole di automazione](#).

La cronologia delle ricerche è disponibile nella console Security Hub, nell'API e AWS CLI.

Se hai effettuato l'accesso a un account amministratore di Security Hub, puoi accedere alla cronologia delle ricerche per l'account amministratore e per tutti gli account dei membri.

Scegli il tuo metodo preferito e segui i passaggi per rivedere la cronologia dei risultati.

Security Hub console

Revisione della cronologia dei risultati

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione a sinistra, scegli Findings.
3. Seleziona un risultato. Nel pannello che appare, scegli la scheda Cronologia.

Security Hub API

Revisione della cronologia dei risultati

1. Esegui o [GetFindings](#), se stai usando AWS CLI, esegui il [get-findingscomando](#) utilizzando i filtri appropriati, se necessario, per identificare il risultato di cui si desidera visualizzare la cronologia. La risposta dell'API ti fornirà l'ProductArn ausilio Id per il risultato. I valori per questi campi sono necessari nel terzo passaggio.
2. Esegui o [GetFindingHistory](#), se stai usando AWS CLI, esegui il [get-finding-historycomando](#).
3. Identifica il risultato di cui vuoi ottenere la cronologia con i Id campi ProductArn and. Per ulteriori informazioni sui campi, consulta [AwsSecurityFindingIdentifier](#). Puoi ottenere la cronologia di un solo risultato per richiesta.
4. Fornisci valori per StartTime. e EndTime limita la cronologia dei risultati a un periodo di tempo specifico.
5. Fornisci un valore MaxResults per limitare la cronologia delle ricerche a un numero specifico di risultati. Se non viene fornita, la risposta dell'API restituisce i primi 100 risultati della cronologia delle ricerche.
6. Fornisci un valore NextToken per visualizzare i 100 risultati successivi (se applicabile) di un risultato. Nella richiesta API iniziale, il valore di NextToken dovrebbe essere NULL.

Il seguente comando CLI recupera la cronologia del risultato specificato. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (\) per migliorare la leggibilità.

```
$ aws securityhub get-finding-history \  
--region us-west-2 \  
--finding-identifier Id="a1b2c3d4-5678-90ab-cdef-  
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-  
west-2:123456789012:product/123456789012/default" \  

```

```
--max-results 2 \  
--start-time "2021-09-30T15:53:35.573Z" \  
--end-time "2021-09-31T15:53:35.573Z"
```

Esame dei dettagli del ritrovamento

Scegli il metodo che preferisci e segui i passaggi per visualizzare i dettagli della ricerca in Security Hub.

Security Hub console

Revisione dei dettagli dei risultati

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Per visualizzare un elenco dei risultati, esegui una delle seguenti azioni:
 - Nel riquadro di navigazione di Security Hub, scegli Findings. Aggiungi i filtri di ricerca necessari per restringere l'elenco dei risultati.
 - Nel riquadro di navigazione Security Hub, scegli Insights. Scegli un approfondimento. Quindi, nell'elenco dei risultati, scegli un risultato approfondito.
 - Nel riquadro di navigazione Security Hub, scegli Integrazioni. Scegli Vedi i risultati per un'integrazione.
3. Seleziona un titolo per la ricerca.
4. Dal pannello dei dettagli della ricerca, puoi intraprendere azioni aggiuntive come segue:
 - Per visualizzare il codice JSON completo del risultato, scegli l'ID del risultato. Da Finding JSON, scarica il file JSON di ricerca.
 - Per risultati basati su AWS Config regole, per visualizzare un elenco delle regole applicabili, scegli Regole.
 - Scegli Investiga con Macie per indagare sui dati sensibili scoperti nel ritrovamento nella console Macie. Questa opzione è disponibile solo se abiliti Amazon Macie e la sua funzione di rilevamento automatico dei dati sensibili.
 - Scegli Risorse per visualizzare le informazioni sulla risorsa coinvolta in un risultato.
 - Scegli Investigate in Amazon Detective per indagare sulla scoperta nella console Detective. Questa opzione è disponibile solo se abiliti Amazon Detective.
 - Scegli la scheda Cronologia per visualizzare fino a 90 giorni di cronologia delle ricerche.

Note

La parte superiore del pannello dei dettagli della ricerca contiene informazioni generali sulla scoperta, tra cui l'account, la gravità, le date e lo stato. Se esegui l'integrazione AWS Organizations e l'account a cui hai effettuato l'accesso è un account membro dell'organizzazione, il pannello dei dettagli include il nome dell'account. Per gli account membro che vengono invitati manualmente anziché tramite l'integrazione Organizations, il pannello dei dettagli include solo l'ID dell'account.

Security Hub API

Revisione dei dettagli dei risultati

Utilizza il [GetFindings](#) funzionamento dell'API Security Hub o, se stai utilizzando AWS CLI, esegui il comando [get-finding](#).

Puoi fornire uno o più valori per il `Filters` parametro per restringere i risultati che desideri recuperare.

Se il volume dei risultati è troppo grande, è possibile utilizzare il `MaxResults` parametro per limitare i risultati a un numero specifico e il `NextToken` parametro per impaginare i risultati. Utilizzate il `SortCriteria` parametro per ordinare i risultati in base a un campo specifico.

Se hai abilitato l'[aggregazione tra regioni](#) e richiami questa operazione dalla regione di aggregazione, i risultati includono i risultati dell'aggregazione e delle regioni collegate.

Il seguente comando CLI recupera i risultati che corrispondono ai filtri forniti e li ordina in ordine decrescente del campo. `LastObservedAt` Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di barra rovesciata (`\`) per migliorare la leggibilità.

```
$ aws securityhub get-findings \  
--filters '{"GeneratorId":[{"Value": "aws-  
foundational"}, {"Comparison": "PREFIX"}], "WorkflowStatus": [{"Value":  
"NEW"}, {"Comparison": "EQUALS"}], "Confidence": [{"Gte": 85}]}' --sort-criteria  
'{"Field": "LastObservedAt", "SortOrder": "desc"}' --page-size 5 --max-items 100
```

PowerShell

Revisione dei dettagli dei risultati

1. Utilizzare il `Get-SHUBFinding` cmdlet.
2. Facoltativamente, compila il `Filter` parametro per restringere i risultati che desideri recuperare.

Esempio

```
Get-SHUBFinding -Filter @{AwsAccountId =  
  [Amazon.SecurityHub.Model.StringFilter]@{Comparison = "EQUALS"; Value =  
  "XXX"};ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]@{Comparison =  
  "EQUALS"; Value = 'FAILED'}}
```

Note

Quando si filtrano i risultati per `CompanyName` o `ProductName`, Security Hub utilizza i valori che fanno parte dell'oggetto `ProductFields ASFF`. Security Hub non utilizza il livello `CompanyName` e `ProductName` i campi principali.

Intervenire in base ai risultati in AWS Security Hub

AWS Security Hub ti consente di tenere traccia dello stato attuale delle tue indagini su un risultato.

Puoi anche inviare i risultati ad azioni personalizzate per l'elaborazione.

Argomenti

- [Impostazione dello stato dei risultati del flusso di lavoro](#)
- [Invio dei risultati a un'operazione personalizzata](#)

Impostazione dello stato dei risultati del flusso di lavoro

Lo stato del flusso di lavoro tiene traccia dell'avanzamento dell'indagine su un risultato. Lo stato del flusso di lavoro è specifico per un singolo risultato. Non influisce sulla generazione di nuove scoperte.

Ad esempio, impostare lo stato del flusso di lavoro di un risultato su SUPPRESSED o RESOLVED non AWS Security Hub impedisce di generare un nuovo risultato per lo stesso problema.

Lo stato del flusso di lavoro può avere i seguenti valori:

NEW

Lo stato iniziale di un risultato prima della sua revisione.

I risultati che vengono acquisiti da sistemi integrati Servizi AWS, ad esempio AWS Config, hanno NEW come stato iniziale.

Security Hub reimposta inoltre lo stato del flusso di lavoro da uno NOTIFIED o RESOLVED a NEW nei seguenti casi:

- RecordState cambia da ARCHIVED a ACTIVE
- Compliance.Status modifiche da PASSED a FAILEDWARNING, o NOT_AVAILABLE.

Queste modifiche implicano la necessità di ulteriori indagini.

NOTIFIED

Indica che il problema di sicurezza è stato notificato al proprietario della risorsa. Puoi utilizzare questo stato quando non sei il proprietario della risorsa ed è necessario l'intervento del proprietario della risorsa per risolvere un problema di sicurezza.

Se si verifica una delle seguenti condizioni, lo stato del flusso di lavoro viene modificato automaticamente da NOTIFIED a NEW:

- RecordState cambia da ARCHIVED a ACTIVE.
- Compliance.Status modifiche da PASSED a FAILEDWARNING, o NOT_AVAILABLE.

SUPPRESSED

Indica che hai esaminato la scoperta e che non ritieni necessaria alcuna azione.

Lo stato del flusso di lavoro di un SUPPRESSED risultato non cambia se RecordState cambia da ARCHIVED a ACTIVE.

RESOLVED

Il risultato è stato esaminato e corretto ed è ora considerato risolto.

Il risultato rimane valido RESOLVED a meno che non si verifichi una delle seguenti condizioni:

- `RecordState` cambia da `ARCHIVED` a `ACTIVE`.
- `Compliance.Status` modifiche da `PASSED` a `FAILEDWARNING`, o `NOT_AVAILABLE`.

In questi casi, lo stato del flusso di lavoro viene reimpostato automaticamente su `NEW`.

Per i risultati dei controlli, in caso `Compliance.Status` `PASSED` affermativo, Security Hub imposta automaticamente lo stato del flusso di lavoro su `RESOLVED`.

Impostazione dello stato dei risultati del flusso di lavoro

Scegli il metodo preferito e segui i passaggi per impostare lo stato del flusso di lavoro di uno o più risultati.

Per aggiornare automaticamente lo stato del flusso di lavoro di risultati specifici, consulta [Regole di automazione](#).

Security Hub console

Per impostare lo stato dei risultati del flusso di lavoro

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Per visualizzare un elenco dei risultati, effettuate una delle seguenti operazioni:
 - Nel riquadro di navigazione di Security Hub, scegli Findings.
 - Nel riquadro di navigazione Security Hub, scegli Insights. Scegli un approfondimento. Quindi, nell'elenco dei risultati, scegli un risultato approfondito.
 - Nel riquadro di navigazione Security Hub, scegli Integrazioni. Scegli Vedi i risultati per un'integrazione.
 - Nel pannello di navigazione Security Hub, scegli Standard di sicurezza. Scegli Visualizza risultati per visualizzare un elenco di controlli. Quindi, seleziona un controllo per visualizzare un elenco di risultati relativi a quel controllo.
3. Nell'elenco dei risultati, seleziona la casella di controllo per ogni risultato che desideri aggiornare.
4. Nella parte superiore dell'elenco, per Stato del flusso di lavoro, scegli lo stato.
5. Nella finestra di dialogo Imposta lo stato del flusso di lavoro, inserisci una nota facoltativa che descriva in dettaglio il motivo dell'aggiornamento dello stato del flusso di lavoro. Scegliete Imposta stato.

Security Hub API

Invoca l'[BatchUpdateFindings](#) API. Fornisci sia l'ID del risultato che l'ARN del prodotto che ha generato il risultato. Puoi ottenere questi dettagli richiamando l'[GetFindings](#) API.

AWS CLI

Esegui il comando [batch-update-findings](#). Fornisci sia l'ID del risultato che l'ARN del prodotto che ha generato il risultato. È possibile ottenere questi dettagli eseguendo il [get-findings](#) comando.

```
batch-update-findings --finding-identifiers
  Id="<findingID>",ProductArn="<productARN>" --workflow Status="<workflowStatus>"
```

Esempio

```
aws securityhub batch-update-findings --finding-identifiers
  Id="arn:aws:securityhub:us-west-1:123456789012:subscription/
pci-dss/v/3.2.1/PCI.Lambda.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",ProductArn="arn:aws:securityhub:us-west-1::product/aws/securityhub" --
workflow Status="RESOLVED"
```

Invio dei risultati a un'operazione personalizzata

Puoi creare azioni AWS Security Hub personalizzate per automatizzare Security Hub con Amazon EventBridge. Per le operazioni personalizzate, il tipo di evento è Security Hub Findings - Custom Action.

Per ulteriori informazioni e fasi dettagliate sulla creazione di operazioni personalizzate, consulta [the section called "Risposta e correzione automatizzate"](#).

Dopo aver impostato un'operazione personalizzata, puoi inviare risultati.

Per inviare i risultati a un'azione personalizzata (console)

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Per visualizzare un elenco dei risultati, effettuate una delle seguenti operazioni:
 - Nel riquadro di navigazione di Security Hub, scegli Findings.

- Nel riquadro di navigazione Security Hub, scegli Insights. Scegli un approfondimento. Quindi, nell'elenco dei risultati, scegli un risultato approfondito.
 - Nel riquadro di navigazione Security Hub, scegli Integrazioni. Scegli Vedi i risultati per un'integrazione.
 - Nel pannello di navigazione Security Hub, scegli Standard di sicurezza. Scegli Visualizza risultati per visualizzare un elenco di controlli. Quindi scegli il nome del controllo.
3. Nell'elenco dei risultati, seleziona la casella di controllo per ogni risultato da inviare all'azione personalizzata.

È possibile inviare fino a 20 risultati alla volta.

4. Per Azioni, scegli l'azione personalizzata.

AWS Formato ASFF (Security Finding Format)

AWS Security Hub utilizza, aggrega, organizza e dà priorità ai risultati dei servizi di AWS sicurezza e delle integrazioni di prodotti di terze parti. Security Hub elabora questi risultati utilizzando un formato standard chiamato AWS Security Finding Format (ASFF), che elimina la necessità di lunghi sforzi di conversione dei dati. Quindi, correla i risultati acquisiti tra i prodotti per definire la priorità di quelli più importanti.

Argomenti

- [AWS Sintassi del Security Finding Format \(ASFF\)](#)
- [Impatto del consolidamento sui campi e sui valori ASFF](#)
- [Esempi ASFF](#)

AWS Sintassi del Security Finding Format (ASFF)

Questa pagina fornisce una descrizione completa del codice JSON per un risultato nel AWS Security Finding Format (ASFF). [Il formato è derivato da JSON Schema](#). Scegliete il nome di un oggetto collegato per visualizzare un esempio di ricerca per quell'oggetto. Puoi confrontare i risultati del Security Hub con le risorse e gli esempi mostrati qui per aiutarti a interpretare i risultati.

Per visualizzare le descrizioni degli attributi ASFF richiesti, vedere [the section called “Attributi di primo livello obbligatori”](#).

Per visualizzare le descrizioni degli altri attributi ASFF di primo livello, vedere. [the section called “Attributi opzionali di primo livello”](#)

```
"Findings": [  
  {  
    "Action": {  
      "ActionType": "string",  
      "AwsApiCallAction": {  
        "AffectedResources": {  
          "string": "string"  
        },  
        "Api": "string",  
        "CallerType": "string",  
        "DomainDetails": {  
          "Domain": "string"  
        },  
        "FirstSeen": "string",  
        "LastSeen": "string",  
        "RemoteIpDetails": {  
          "City": {  
            "CityName": "string"  
          },  
          "Country": {  
            "CountryCode": "string",  
            "CountryName": "string"  
          },  
          "IpAddressV4": "string",  
          "Geolocation": {  
            "Lat": number,  
            "Lon": number  
          },  
          "Organization": {  
            "Asn": number,  
            "AsnOrg": "string",  
            "Isp": "string",  
            "Org": "string"  
          }  
        },  
        "ServiceName": "string"  
      },  
      "DnsRequestAction": {  
        "Blocked": boolean,  
        "Domain": "string",
```

```
"Protocol": "string"
},
"NetworkConnectionAction": {
  "Blocked": boolean,
  "ConnectionDirection": "string",
  "LocalPortDetails": {
    "Port": number,
    "PortName": "string"
  },
  "Protocol": "string",
  "RemoteIpDetails": {
    "City": {
      "CityName": "string"
    },
    "Country": {
      "CountryCode": "string",
      "CountryName": "string"
    },
    "IpAddressV4": "string",
    "Geolocation": {
      "Lat": number,
      "Lon": number
    },
    "Organization": {
      "Asn": number,
      "AsnOrg": "string",
      "Isp": "string",
      "Org": "string"
    }
  },
  "RemotePortDetails": {
    "Port": number,
    "PortName": "string"
  }
},
"PortProbeAction": {
  "Blocked": boolean,
  "PortProbeDetails": [{
    "LocalIpDetails": {
      "IpAddressV4": "string"
    },
    "LocalPortDetails": {
      "Port": number,
      "PortName": "string"
    }
  }
}
```

```
    },
    "RemoteIpDetails": {
      "City": {
        "CityName": "string"
      },
      "Country": {
        "CountryCode": "string",
        "CountryName": "string"
      },
      "GeoLocation": {
        "Lat": number,
        "Lon": number
      },
      "IpAddressV4": "string",
      "Organization": {
        "Asn": number,
        "AsnOrg": "string",
        "Isp": "string",
        "Org": "string"
      }
    }
  ]
},
"AwsAccountId": "string",
"AwsAccountName": "string",
"CompanyName": "string",
"Compliance": {
  "AssociatedStandards": [{
    "StandardsId": "string"
  }],
  "RelatedRequirements": ["string"],
  "SecurityControlId": "string",
  "SecurityControlParameters": [
    {
      "Name": "string",
      "Value": ["string"]
    }
  ],
  "Status": "string",
  "StatusReasons": [
    {
      "Description": "string",
      "ReasonCode": "string"
    }
  ]
}
```

```
    }
  ]
},
"Confidence": number,
"CreatedAt": "string",
"Criticality": number,
"Description": "string",
"FindingProviderFields": {
  "Confidence": number,
  "Criticality": number,
  "RelatedFindings": [{
    "ProductArn": "string",
    "Id": "string"
  }],
  "Severity": {
    "Label": "string",
    "Normalized": number,
    "Original": "string"
  },
  "Types": ["string"]
},
"FirstObservedAt": "string",
"GeneratorId": "string",
"Id": "string",
"LastObservedAt": "string",
"Malware": [{
  "Name": "string",
  "Path": "string",
  "State": "string",
  "Type": "string"
}],
"Network": {
  "DestinationDomain": "string",
  "DestinationIPv4": "string",
  "DestinationIPv6": "string",
  "DestinationPort": number,
  "Direction": "string",
  "OpenPortRange": {
    "Begin": integer,
    "End": integer
  },
  "Protocol": "string",
  "SourceDomain": "string",
  "SourceIPv4": "string",
```

```
"SourceIPv6": "string",
"SourceMac": "string",
"SourcePort": number
},
"NetworkPath": [{
  "ComponentId": "string",
  "ComponentType": "string",
  "Egress": {
    "Destination": {
      "Address": ["string"],
      "PortRanges": [{
        "Begin": integer,
        "End": integer
      }]
    },
    "Protocol": "string",
    "Source": {
      "Address": ["string"],
      "PortRanges": [{
        "Begin": integer,
        "End": integer
      }]
    }
  },
  "Ingress": {
    "Destination": {
      "Address": ["string"],
      "PortRanges": [{
        "Begin": integer,
        "End": integer
      }]
    },
    "Protocol": "string",
    "Source": {
      "Address": ["string"],
      "PortRanges": [{
        "Begin": integer,
        "End": integer
      }]
    }
  },
  "Note": {
    "Text": "string",
```

```
"UpdatedAt": "string",
"UpdatedBy": "string"
},
"PatchSummary": {
  "FailedCount": number,
  "Id": "string",
  "InstalledCount": number,
  "InstalledOtherCount": number,
  "InstalledPendingReboot": number,
  "InstalledRejectedCount": number,
  "MissingCount": number,
  "Operation": "string",
  "OperationEndTime": "string",
  "OperationStartTime": "string",
  "RebootOption": "string"
},
"Process": {
  "LaunchedAt": "string",
  "Name": "string",
  "ParentPid": number,
  "Path": "string",
  "Pid": number,
  "TerminatedAt": "string"
},
"ProductArn": "string",
"ProductFields": {
  "string": "string"
},
"ProductName": "string",
"RecordState": "string",
"Region": "string",
"RelatedFindings": [{
  "Id": "string",
  "ProductArn": "string"
}],
"Remediation": {
  "Recommendation": {
    "Text": "string",
    "Url": "string"
  }
},
"Resources": [{
  "ApplicationArn": "string",
  "ApplicationName": "string",
```



```
"DataClassification": {
  "DetailedResultsLocation": "string",
  "Result": {
    "AdditionalOccurrences": boolean,
    "CustomDataIdentifiers": {
      "Detections": [{
        "Arn": "string",
        "Count": integer,
        "Name": "string",
        "Occurrences": {
          "Cells": [{
            "CellReference": "string",
            "Column": integer,
            "ColumnName": "string",
            "Row": integer
          }],
          "LineRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
          }],
          "OffsetRanges": [{
            "End": integer,
            "Start": integer,
            "StartColumn": integer
          }],
          "Pages": [{
            "LineRange": {
              "End": integer,
              "Start": integer,
              "StartColumn": integer
            },
            "OffsetRange": {
              "End": integer,
              "Start": integer,
              "StartColumn": integer
            },
            "PageNumber": integer
          }],
          "Records": [{
            "JsonPath": "string",
            "RecordIndex": integer
          }
        ]
      }
    }
  }
}
```

```
    ]],
    "TotalCount": integer
  },
  "MimeType": "string",
  "SensitiveData": [{
    "Category": "string",
    "Detections": [{
      "Count": integer,
      "Occurrences": {
        "Cells": [{
          "CellReference": "string",
          "Column": integer,
          "ColumnName": "string",
          "Row": integer
        }],
        "LineRanges": [{
          "End": integer,
          "Start": integer,
          "StartColumn": integer
        }],
        "OffsetRanges": [{
          "End": integer,
          "Start": integer,
          "StartColumn": integer
        }],
        "Pages": [{
          "LineRange": {
            "End": integer,
            "Start": integer,
            "StartColumn": integer
          },
          "OffsetRange": {
            "End": integer,
            "Start": integer,
            "StartColumn": integer
          }
        },
        "PageNumber": integer
      }],
    "Records": [{
      "JsonPath": "string",
      "RecordIndex": integer
    }],
  },
  "Type": "string"
```

```
    ]],
    "TotalCount": integer
  ]],
  "SizeClassified": integer,
  "Status": {
    "Code": "string",
    "Reason": "string"
  }
}
},
"Details": {
  "AwsAmazonMQBroker": {
    "AutoMinorVersionUpgrade": boolean,
    "BrokerArn": "string",
    "BrokerId": "string",
    "BrokerName": "string",
    "Configuration": {
      "Id": "string",
      "Revision": integer
    },
    "DeploymentMode": "string",
    "EncryptionOptions": {
      "UseAwsOwnedKey": boolean
    },
    "EngineType": "string",
    "EngineVersion": "string",
    "HostInstanceType": "string",
    "Logs": {
      "Audit": boolean,
      "AuditLogGroup": "string",
      "General": boolean,
      "GeneralLogGroup": "string"
    },
    "MaintenanceWindowStartTime": {
      "DayOfWeek": "string",
      "TimeOfDay": "string",
      "TimeZone": "string"
    },
    "PubliclyAccessible": boolean,
    "SecurityGroups": [
      "string"
    ],
    "StorageType": "string",
    "SubnetIds": [
```

```
    "string",
    "string"
  ],
  "Users": [{
    "Username": "string"
  }]
},
"AwsApiGatewayRestApi": {
  "ApiKeySource": "string",
  "BinaryMediaTypes": ["string"],
  "CreatedDate": "string",
  "Description": "string",
  "EndpointConfiguration": {
    "Types": ["string"]
  },
  "Id": "string",
  "MinimumCompressionSize": number,
  "Name": "string",
  "Version": "string"
},
"AwsApiGatewayStage": {
  "AccessLogSettings": {
    "DestinationArn": "string",
    "Format": "string"
  },
  "CacheClusterEnabled": boolean,
  "CacheClusterSize": "string",
  "CacheClusterStatus": "string",
  "CanarySettings": {
    "DeploymentId": "string",
    "PercentTraffic": number,
    "StageVariableOverrides": [{
      "string": "string"
    }],
    "UseStageCache": boolean
  },
  "ClientCertificateId": "string",
  "CreatedDate": "string",
  "DeploymentId": "string",
  "Description": "string",
  "DocumentationVersion": "string",
  "LastUpdatedDate": "string",
  "MethodSettings": [{
    "CacheDataEncrypted": boolean,
```

```

    "CachingEnabled": boolean,
    "CacheTtlInSeconds": number,
    "DataTraceEnabled": boolean,
    "HttpMethod": "string",
    "LoggingLevel": "string",
    "MetricsEnabled": boolean,
    "RequireAuthorizationForCacheControl": boolean,
    "ResourcePath": "string",
    "ThrottlingBurstLimit": number,
    "ThrottlingRateLimit": number,
    "UnauthorizedCacheControlHeaderStrategy": "string"
  ]],
  "StageName": "string",
  "TracingEnabled": boolean,
  "Variables": {
    "string": "string"
  },
  "WebAclArn": "string"
},
"AwsApiGatewayV2Api": {
  "ApiEndpoint": "string",
  "ApiId": "string",
  "ApiKeySelectionExpression": "string",
  "CorsConfiguration": {
    "AllowCredentials": boolean,
    "AllowHeaders": ["string"],
    "AllowMethods": ["string"],
    "AllowOrigins": ["string"],
    "ExposeHeaders": ["string"],
    "MaxAge": number
  },
  "CreatedDate": "string",
  "Description": "string",
  "Name": "string",
  "ProtocolType": "string",
  "RouteSelectionExpression": "string",
  "Version": "string"
},
"AwsApiGatewayV2Stage": {
  "AccessLogSettings": {
    "DestinationArn": "string",
    "Format": "string"
  },
  "ApiGatewayManaged": boolean,

```

```
"AutoDeploy": boolean,
"ClientCertificateId": "string",
"CreateDate": "string",
"DefaultRouteSettings": {
  "DataTraceEnabled": boolean,
  "DetailedMetricsEnabled": boolean,
  "LoggingLevel": "string",
  "ThrottlingBurstLimit": number,
  "ThrottlingRateLimit": number
},
"DeploymentId": "string",
"Description": "string",
"LastDeploymentStatusMessage": "string",
"LastUpdatedDate": "string",
"RouteSettings": {
  "DetailedMetricsEnabled": boolean,
  "LoggingLevel": "string",
  "DataTraceEnabled": boolean,
  "ThrottlingBurstLimit": number,
  "ThrottlingRateLimit": number
},
"StageName": "string",
"StageVariables": [{
  "string": "string"
}]
},
"AwsAppSyncGraphQLApi": {
  "AwsAppSyncGraphQLApi": {
    "AdditionalAuthenticationProviders": [
      {
        "AuthenticationType": "string",
        "LambdaAuthorizerConfig": {
          "AuthorizerResultTtlInSeconds": integer,
          "AuthorizerUri": "string"
        }
      }
    ],
    {
      "AuthenticationType": "string"
    }
  ],
  "ApiId": "string",
  "Arn": "string",
  "AuthenticationType": "string",
  "Id": "string",
```

```
"LogConfig": {
  "CloudWatchLogsRoleArn": "string",
  "ExcludeVerboseContent": boolean,
  "FieldLogLevel": "string"
},
"Name": "string",
"XrayEnabled": boolean
}
},
"AwsAthenaWorkGroup": {
  "Description": "string",
  "Name": "string",
  "WorkgroupConfiguration": {
    "ResultConfiguration": {
      "EncryptionConfiguration": {
        "EncryptionOption": "string",
        "KmsKey": "string"
      }
    }
  },
  "State": "string"
},
"AwsAutoScalingAutoScalingGroup": {
  "AvailabilityZones": [{
    "Value": "string"
  }],
  "CreatedTime": "string",
  "HealthCheckGracePeriod": integer,
  "HealthCheckType": "string",
  "LaunchConfigurationName": "string",
  "LoadBalancerNames": ["string"],
  "LaunchTemplate": {
    "LaunchTemplateId": "string",
    "LaunchTemplateName": "string",
    "Version": "string"
  },
  "MixedInstancesPolicy": {
    "InstancesDistribution": {
      "OnDemandAllocationStrategy": "string",
      "OnDemandBaseCapacity": number,
      "OnDemandPercentageAboveBaseCapacity": number,
      "SpotAllocationStrategy": "string",
      "SpotInstancePools": number,
      "SpotMaxPrice": "string"
    }
  }
}
```

```
    },
    "LaunchTemplate": {
      "LaunchTemplateSpecification": {
        "LaunchTemplateId": "string",
        "LaunchTemplateName": "string",
        "Version": "string"
      },
      "CapacityRebalance": boolean,
      "Overrides": [{
        "InstanceType": "string",
        "WeightedCapacity": "string"
      }]
    }
  }
},
"AwsAutoScalingLaunchConfiguration": {
  "AssociatePublicIpAddress": boolean,
  "BlockDeviceMappings": [{
    "DeviceName": "string",
    "Ebs": {
      "DeleteOnTermination": boolean,
      "Encrypted": boolean,
      "Iops": number,
      "SnapshotId": "string",
      "VolumeSize": number,
      "VolumeType": "string"
    },
    "NoDevice": boolean,
    "VirtualName": "string"
  }],
  "ClassicLinkVpcId": "string",
  "ClassicLinkVpcSecurityGroups": ["string"],
  "CreatedTime": "string",
  "EbsOptimized": boolean,
  "IamInstanceProfile": "string"
},
"ImageId": "string",
"InstanceMonitoring": {
  "Enabled": boolean
},
"InstanceType": "string",
"KernelId": "string",
"KeyName": "string",
"LaunchConfigurationName": "string",
```



```

"MetadataOptions": {
  "HttpEndPoint": "string",
  "HttpPutReponseHopLimit": number,
  "HttpTokens": "string"
},
"PlacementTenancy": "string",
"RamdiskId": "string",
"SecurityGroups": ["string"],
"SpotPrice": "string",
"UserData": "string"
},
"AwsBackupBackupPlan": {
  "BackupPlan": {
    "AdvancedBackupSettings": [{
      "BackupOptions": {
        "WindowsVSS": "string"
      },
      "ResourceType": "string"
    }],
    "BackupPlanName": "string",
    "BackupPlanRule": [{
      "CompletionWindowMinutes": integer,
      "CopyActions": [{
        "DestinationBackupVaultArn": "string",
        "Lifecycle": {
          "DeleteAfterDays": integer,
          "MoveToColdStorageAfterDays": integer
        }
      }],
      "Lifecycle": {
        "DeleteAfterDays": integer
      },
      "RuleName": "string",
      "ScheduleExpression": "string",
      "StartWindowMinutes": integer,
      "TargetBackupVault": "string"
    }],
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "VersionId": "string"
  },
  "AwsBackupBackupVault": {
    "AccessPolicy": {

```

```

    "Statement": [{
      "Action": ["string"],
      "Effect": "string",
      "Principal": {
        "AWS": "string"
      },
      "Resource": "string"
    }],
    "Version": "string"
  },
  "BackupVaultArn": "string",
  "BackupVaultName": "string",
  "EncryptionKeyArn": "string",
  "Notifications": {
    "BackupVaultEvents": ["string"],
    "SNSTopicArn": "string"
  }
},
"AwsBackupRecoveryPoint": {
  "BackupSizeInBytes": integer,
  "BackupVaultName": "string",
  "BackupVaultArn": "string",
  "CalculatedLifecycle": {
    "DeleteAt": "string",
    "MoveToColdStorageAt": "string"
  },
  "CompletionDate": "string",
  "CreatedBy": {
    "BackupPlanArn": "string",
    "BackupPlanId": "string",
    "BackupPlanVersion": "string",
    "BackupRuleId": "string"
  },
  "CreationDate": "string",
  "EncryptionKeyArn": "string",
  "IamRoleArn": "string",
  "IsEncrypted": boolean,
  "LastRestoreTime": "string",
  "Lifecycle": {
    "DeleteAfterDays": integer,
    "MoveToColdStorageAfterDays": integer
  },
  "RecoveryPointArn": "string",
  "ResourceArn": "string",

```

```

    "ResourceType": "string",
    "SourceBackupVaultArn": "string",
    "Status": "string",
    "StatusMessage": "string",
    "StorageClass": "string"
  },
  "AwsCertificateManagerCertificate": {
    "CertificateAuthorityArn": "string",
    "CreatedAt": "string",
    "DomainName": "string",
    "DomainValidationOptions": [{
      "DomainName": "string",
      "ResourceRecord": {
        "Name": "string",
        "Type": "string",
        "Value": "string"
      },
      "ValidationDomain": "string",
      "ValidationEmails": ["string"],
      "ValidationMethod": "string",
      "ValidationStatus": "string"
    }],
    "ExtendedKeyUsages": [{
      "Name": "string",
      "Oid": "string"
    }],
    "FailureReason": "string",
    "ImportedAt": "string",
    "InUseBy": ["string"],
    "IssuedAt": "string",
    "Issuer": "string",
    "KeyAlgorithm": "string",
    "KeyUsages": [{
      "Name": "string"
    }],
    "NotAfter": "string",
    "NotBefore": "string",
    "Options": {
      "CertificateTransparencyLoggingPreference": "string"
    },
    "RenewalEligibility": "string",
    "RenewalSummary": {
      "DomainValidationOptions": [{
        "DomainName": "string",

```

```
    "ResourceRecord": {
      "Name": "string",
      "Type": "string",
      "Value": "string"
    },
    "ValidationDomain": "string",
    "ValidationEmails": ["string"],
    "ValidationMethod": "string",
    "ValidationStatus": "string"
  ]],
  "RenewalStatus": "string",
  "RenewalStatusReason": "string",
  "UpdatedAt": "string"
},
"Serial": "string",
"SignatureAlgorithm": "string",
"Status": "string",
"Subject": "string",
"SubjectAlternativeNames": ["string"],
"Type": "string"
},
"AwsCloudFormationStack": {
  "Capabilities": ["string"],
  "CreationTime": "string",
  "Description": "string",
  "DisableRollback": boolean,
  "DriftInformation": {
    "StackDriftStatus": "string"
  },
  "EnableTerminationProtection": boolean,
  "LastUpdatedTime": "string",
  "NotificationArns": ["string"],
  "Outputs": [{
    "Description": "string",
    "OutputKey": "string",
    "OutputValue": "string"
  }],
  "RoleArn": "string",
  "StackId": "string",
  "StackName": "string",
  "StackStatus": "string",
  "StackStatusReason": "string",
  "TimeoutInMinutes": number
},
```

```
"AwsCloudFrontDistribution": {
  "CacheBehaviors": {
    "Items": [{
      "ViewerProtocolPolicy": "string"
    }]
  },
  "DefaultCacheBehavior": {
    "ViewerProtocolPolicy": "string"
  },
  "DefaultRootObject": "string",
  "DomainName": "string",
  "Etag": "string",
  "LastModifiedTime": "string",
  "Logging": {
    "Bucket": "string",
    "Enabled": boolean,
    "IncludeCookies": boolean,
    "Prefix": "string"
  },
  "OriginGroups": {
    "Items": [{
      "FailoverCriteria": {
        "StatusCodes": {
          "Items": [number],
          "Quantity": number
        }
      }
    }]
  },
  "Origins": {
    "Items": [{
      "CustomOriginConfig": {
        "HttpPort": number,
        "HttpsPort": number,
        "OriginKeepaliveTimeout": number,
        "OriginProtocolPolicy": "string",
        "OriginReadTimeout": number,
        "OriginSslProtocols": {
          "Items": ["string"],
          "Quantity": number
        }
      }
    }],
    "DomainName": "string",
    "Id": "string",
```

```
    "OriginPath": "string",
    "S3OriginConfig": {
      "OriginAccessIdentity": "string"
    }
  ]
},
"Status": "string",
"ViewerCertificate": {
  "AcmCertificateArn": "string",
  "Certificate": "string",
  "CertificateSource": "string",
  "CloudFrontDefaultCertificate": boolean,
  "IamCertificateId": "string",
  "MinimumProtocolVersion": "string",
  "SslSupportMethod": "string"
},
"WebAclId": "string"
},
"AwsCloudTrailTrail": {
  "CloudWatchLogsLogGroupArn": "string",
  "CloudWatchLogsRoleArn": "string",
  "HasCustomEventSelectors": boolean,
  "HomeRegion": "string",
  "IncludeGlobalServiceEvents": boolean,
  "IsMultiRegionTrail": boolean,
  "IsOrganizationTrail": boolean,
  "KmsKeyId": "string",
  "LogFileValidationEnabled": boolean,
  "Name": "string",
  "S3BucketName": "string",
  "S3KeyPrefix": "string",
  "SnsTopicArn": "string",
  "SnsTopicName": "string",
  "TrailArn": "string"
},
"AwsCloudWatchAlarm": {
  "ActionsEnabled": boolean,
  "AlarmActions": ["string"],
  "AlarmArn": "string",
  "AlarmConfigurationUpdatedTimestamp": "string",
  "AlarmDescription": "string",
  "AlarmName": "string",
  "ComparisonOperator": "string",
  "DatapointsToAlarm": number,
```

```

"Dimensions": [{
  "Name": "string",
  "Value": "string"
}],
"EvaluateLowSampleCountPercentile": "string",
"EvaluationPeriods": number,
"ExtendedStatistic": "string",
"InsufficientDataActions": ["string"],
"MetricName": "string",
"Namespace": "string",
"OkActions": ["string"],
"Period": number,
"Statistic": "string",
"Threshold": number,
"ThresholdMetricId": "string",
"TreatMissingData": "string",
"Unit": "string"
},
"AwsCodeBuildProject": {
  "Artifacts": [{
    "ArtifactIdentifier": "string",
    "EncryptionDisabled": boolean,
    "Location": "string",
    "Name": "string",
    "NamespaceType": "string",
    "OverrideArtifactName": boolean,
    "Packaging": "string",
    "Path": "string",
    "Type": "string"
  }],
  "SecondaryArtifacts": [{
    "ArtifactIdentifier": "string",
    "Type": "string",
    "Location": "string",
    "Name": "string",
    "NamespaceType": "string",
    "Packaging": "string",
    "Path": "string",
    "EncryptionDisabled": boolean,
    "OverrideArtifactName": boolean
  }],
  "EncryptionKey": "string",
  "Certificate": "string",
  "Environment": {

```

```
"Certificate": "string",
"EnvironmentVariables": [{
  "Name": "string",
  "Type": "string",
  "Value": "string"
}],
"ImagePullCredentialsType": "string",
"PrivilegedMode": boolean,
"RegistryCredential": {
  "Credential": "string",
  "CredentialProvider": "string"
},
"Type": "string"
},
"LogsConfig": {
  "CloudWatchLogs": {
    "GroupName": "string",
    "Status": "string",
    "StreamName": "string"
  },
  "S3Logs": {
    "EncryptionDisabled": boolean,
    "Location": "string",
    "Status": "string"
  }
},
"Name": "string",
"ServiceRole": "string",
"Source": {
  "Type": "string",
  "Location": "string",
  "GitCloneDepth": integer
},
"VpcConfig": {
  "VpcId": "string",
  "Subnets": ["string"],
  "SecurityGroupIds": ["string"]
}
},
"AwsDmsEndpoint": {
  "CertificateArn": "string",
  "DatabaseName": "string",
  "EndpointArn": "string",
  "EndpointIdentifier": "string",
```



```
"EndpointType": "string",
"EngineName": "string",
"KmsKeyId": "string",
"Port": integer,
"ServerName": "string",
"SslMode": "string",
"Username": "string"
},
"AwsDmsReplicationInstance": {
  "AllocatedStorage": integer,
  "AutoMinorVersionUpgrade": boolean,
  "AvailabilityZone": "string",
  "EngineVersion": "string",
  "KmsKeyId": "string",
  "MultiAZ": boolean,
  "PreferredMaintenanceWindow": "string",
  "PubliclyAccessible": boolean,
  "ReplicationInstanceClass": "string",
  "ReplicationInstanceIdentifier": "string",
  "ReplicationSubnetGroup": {
    "ReplicationSubnetGroupIdentifier": "string"
  },
  "VpcSecurityGroups": [
    {
      "VpcSecurityGroupId": "string"
    }
  ]
},
"AwsDmsReplicationTask": {
  "CdcStartPosition": "string",
  "Id": "string",
  "MigrationType": "string",
  "ReplicationInstanceArn": "string",
  "ReplicationTaskIdentifier": "string",
  "ReplicationTaskSettings": {
    "string": "string"
  },
  "SourceEndpointArn": "string",
  "TableMappings": {
    "string": "string"
  },
  "TargetEndpointArn": "string"
},
"AwsDynamoDbTable": {
```

```
"AttributeDefinitions": [{
  "AttributeName": "string",
  "AttributeType": "string"
}],
"BillingModeSummary": {
  "BillingMode": "string",
  "LastUpdateToPayPerRequestDateTime": "string"
},
"CreationDateTime": "string",
"DeletionProtectionEnabled": boolean,
"GlobalSecondaryIndexes": [{
  "Backfilling": boolean,
  "IndexArn": "string",
  "IndexName": "string",
  "IndexSizeBytes": number,
  "IndexStatus": "string",
  "ItemCount": number,
  "KeySchema": [{
    "AttributeName": "string",
    "KeyType": "string"
  }],
  "Projection": {
    "NonKeyAttributes": ["string"],
    "ProjectionType": "string"
  },
  "ProvisionedThroughput": {
    "LastDecreaseDateTime": "string",
    "LastIncreaseDateTime": "string",
    "NumberOfDecreasesToday": number,
    "ReadCapacityUnits": number,
    "WriteCapacityUnits": number
  }
}],
"GlobalTableVersion": "string",
"ItemCount": number,
"KeySchema": [{
  "AttributeName": "string",
  "KeyType": "string"
}],
"LatestStreamArn": "string",
"LatestStreamLabel": "string",
"LocalSecondaryIndexes": [{
  "IndexArn": "string",
  "IndexName": "string",
```

```
"KeySchema": [{
  "AttributeName": "string",
  "KeyType": "string"
}],
"Projection": {
  "NonKeyAttributes": ["string"],
  "ProjectionType": "string"
}
}],
"ProvisionedThroughput": {
  "LastDecreaseDateTime": "string",
  "LastIncreaseDateTime": "string",
  "NumberOfDecreasesToday": number,
  "ReadCapacityUnits": number,
  "WriteCapacityUnits": number
},
"Replicas": [{
  "GlobalSecondaryIndexes": [{
    "IndexName": "string",
    "ProvisionedThroughputOverride": {
      "ReadCapacityUnits": number
    }
  }
}],
  "KmsMasterKeyId": "string",
  "ProvisionedThroughputOverride": {
    "ReadCapacityUnits": number
  },
  "RegionName": "string",
  "ReplicaStatus": "string",
  "ReplicaStatusDescription": "string"
}],
"RestoreSummary": {
  "RestoreDateTime": "string",
  "RestoreInProgress": boolean,
  "SourceBackupArn": "string",
  "SourceTableArn": "string"
},
"SseDescription": {
  "InaccessibleEncryptionDateTime": "string",
  "KmsMasterKeyArn": "string",
  "SseType": "string",
  "Status": "string"
},
"StreamSpecification": {
```

```
"StreamEnabled": boolean,
"StreamViewType": "string"
},
"TableId": "string",
"TableName": "string",
"TableSizeBytes": number,
"TableStatus": "string"
},
"AwsEc2ClientVpnEndpoint": {
  "AuthenticationOptions": [
    {
      "MutualAuthentication": {
        "ClientRootCertificateChainArn": "string"
      },
      "Type": "string"
    }
  ],
  "ClientCidrBlock": "string",
  "ClientConnectOptions": {
    "Enabled": boolean
  },
  "ClientLoginBannerOptions": {
    "Enabled": boolean
  },
  "ClientVpnEndpointId": "string",
  "ConnectionLogOptions": {
    "Enabled": boolean
  },
  "Description": "string",
  "DnsServer": ["string"],
  "ServerCertificateArn": "string",
  "SecurityGroupIdSet": [
    "string"
  ],
  "SelfServicePortalUrl": "string",
  "SessionTimeoutHours": "integer",
  "SplitTunnel": boolean,
  "TransportProtocol": "string",
  "VpcId": "string",
  "VpnPort": integer
},
"AwsEc2Eip": {
  "AllocationId": "string",
  "AssociationId": "string",
```

```
"Domain": "string",
"InstanceId": "string",
"NetworkBorderGroup": "string",
"NetworkInterfaceId": "string",
"NetworkInterfaceOwnerId": "string",
"PrivateIpAddress": "string",
"PublicIp": "string",
"PublicIpv4Pool": "string"
},
"AwsEc2Instance": {
  "IamInstanceProfileArn": "string",
  "ImageId": "string",
  "IPv4Addresses": ["string"],
  "IPv6Addresses": ["string"],
  "KeyName": "string",
  "LaunchedAt": "string",
  "MetadataOptions": {
    "HttpEndpoint": "string",
    "HttpProtocolIpv6": "string",
    "HttpPutResponseHopLimit": number,
    "HttpTokens": "string",
    "InstanceMetadataTags": "string"
  },
  "Monitoring": {
    "State": "string"
  },
  "NetworkInterfaces": [{
    "NetworkInterfaceId": "string"
  }],
  "SubnetId": "string",
  "Type": "string",
  "VirtualizationType": "string",
  "VpcId": "string"
},
"AwsEc2LaunchTemplate": {
  "DefaultVersionNumber": "string",
  "ElasticGpuSpecifications": ["string"],
  "ElasticInferenceAccelerators": ["string"],
  "Id": "string",
  "ImageId": "string",
  "LatestVersionNumber": "string",
  "LaunchTemplateData": {
    "BlockDeviceMappings": [{
      "DeviceName": "string",
```

```
"Ebs": {
  "DeleteonTermination": boolean,
  "Encrypted": boolean,
  "SnapshotId": "string",
  "VolumeSize": number,
  "VolumeType": "string"
}
}],
"MetadataOptions": {
  "HttpTokens": "string",
  "HttpPutResponseHopLimit" : number
},
"Monitoring": {
  "Enabled": boolean
},
"NetworkInterfaces": [{
  "AssociatePublicIpAddress" : boolean
}]
},
"LaunchTemplateName": "string",
"LicenseSpecifications": ["string"],
"SecurityGroupIds": ["string"],
"SecurityGroups": ["string"],
"TagSpecifications": ["string"]
},
"AwsEc2NetworkAcl": {
  "Associations": [{
    "NetworkAclAssociationId": "string",
    "NetworkAclId": "string",
    "SubnetId": "string"
  }],
  "Entries": [{
    "CidrBlock": "string",
    "Egress": boolean,
    "IcmpTypeCode": {
      "Code": number,
      "Type": number
    },
    "Ipv6CidrBlock": "string",
    "PortRange": {
      "From": number,
      "To": number
    },
    "Protocol": "string",
```

```
    "RuleAction": "string",
    "RuleNumber": number
  ]],
  "IsDefault": boolean,
  "NetworkAclId": "string",
  "OwnerId": "string",
  "VpcId": "string"
},
"AwsEc2NetworkInterface": {
  "Attachment": {
    "AttachmentId": "string",
    "AttachTime": "string",
    "DeleteOnTermination": boolean,
    "DeviceIndex": number,
    "InstanceId": "string",
    "InstanceOwnerId": "string",
    "Status": "string"
  },
  "Ipv6Addresses": [{
    "Ipv6Address": "string"
  }],
  "NetworkInterfaceId": "string",
  "PrivateIpAddresses": [{
    "PrivateDnsName": "string",
    "PrivateIpAddress": "string"
  }],
  "PublicDnsName": "string",
  "PublicIp": "string",
  "SecurityGroups": [{
    "GroupId": "string",
    "GroupName": "string"
  }],
  "SourceDestCheck": boolean
},
"AwsEc2RouteTable": {
  "AssociationSet": [{
    "AssociationState": {
      "State": "string"
    },
    "Main": boolean,
    "RouteTableAssociationId": "string",
    "RouteTableId": "string"
  }],
  "PropogatingVgwSet": [],
```

```

"RouteTableId": "string",
"RouteSet": [
  {
    "DestinationCidrBlock": "string",
    "GatewayId": "string",
    "Origin": "string",
    "State": "string"
  },
  {
    "DestinationCidrBlock": "string",
    "GatewayId": "string",
    "Origin": "string",
    "State": "string"
  }
],
"VpcId": "string"
},
"AwsEc2SecurityGroup": {
  "GroupId": "string",
  "GroupName": "string",
  "IpPermissions": [{
    "FromPort": number,
    "IpProtocol": "string",
    "IpRanges": [{
      "CidrIp": "string"
    }],
    "Ipv6Ranges": [{
      "CidrIpv6": "string"
    }],
    "PrefixListIds": [{
      "PrefixListId": "string"
    }],
    "ToPort": number,
    "UserIdGroupPairs": [{
      "GroupId": "string",
      "GroupName": "string",
      "PeeringStatus": "string",
      "UserId": "string",
      "VpcId": "string",
      "VpcPeeringConnectionId": "string"
    }
  ]
}],
"IpPermissionsEgress": [{
  "FromPort": number,

```



```

    "IpProtocol": "string",
    "IpRanges": [{
      "CidrIp": "string"
    }],
    "Ipv6Ranges": [{
      "CidrIpv6": "string"
    }],
    "PrefixListIds": [{
      "PrefixListId": "string"
    }],
    "ToPort": number,
    "UserIdGroupPairs": [{
      "GroupId": "string",
      "GroupName": "string",
      "PeeringStatus": "string",
      "UserId": "string",
      "VpcId": "string",
      "VpcPeeringConnectionId": "string"
    }
  ]],
  "OwnerId": "string",
  "VpcId": "string"
},
"AwsEc2Subnet": {
  "AssignIpv6AddressOnCreation": boolean,
  "AvailabilityZone": "string",
  "AvailabilityZoneId": "string",
  "AvailableIpAddressCount": number,
  "CidrBlock": "string",
  "DefaultForAz": boolean,
  "Ipv6CidrBlockAssociationSet": [{
    "AssociationId": "string",
    "Ipv6CidrBlock": "string",
    "CidrBlockState": "string"
  }],
  "MapPublicIpOnLaunch": boolean,
  "OwnerId": "string",
  "State": "string",
  "SubnetArn": "string",
  "SubnetId": "string",
  "VpcId": "string"
},
"AwsEc2TransitGateway": {
  "AmazonSideAsn": number,

```

```

    "AssociationDefaultRouteTableId": "string",
    "AutoAcceptSharedAttachments": "string",
    "DefaultRouteTableAssociation": "string",
    "DefaultRouteTablePropagation": "string",
    "Description": "string",
    "DnsSupport": "string",
    "Id": "string",
    "MulticastSupport": "string",
    "PropagationDefaultRouteTableId": "string",
    "TransitGatewayCidrBlocks": ["string"],
    "VpnEcmpSupport": "string"
  },
  "AwsEc2Volume": {
    "Attachments": [{
      "AttachTime": "string",
      "DeleteOnTermination": boolean,
      "InstanceId": "string",
      "Status": "string"
    }],
    "CreateTime": "string",
    "DeviceName": "string",
    "Encrypted": boolean,
    "KmsKeyId": "string",
    "Size": number,
    "SnapshotId": "string",
    "Status": "string",
    "VolumeId": "string",
    "VolumeScanStatus": "string",
    "VolumeType": "string"
  },
  "AwsEc2Vpc": {
    "CidrBlockAssociationSet": [{
      "AssociationId": "string",
      "CidrBlock": "string",
      "CidrBlockState": "string"
    }],
    "DhcpOptionsId": "string",
    "Ipv6CidrBlockAssociationSet": [{
      "AssociationId": "string",
      "CidrBlockState": "string",
      "Ipv6CidrBlock": "string"
    }],
    "State": "string"
  },
},

```

```
"AwsEc2VpcEndpointService": {
  "AcceptanceRequired": boolean,
  "AvailabilityZones": ["string"],
  "BaseEndpointDnsNames": ["string"],
  "ManagesVpcEndpoints": boolean,
  "GatewayLoadBalancerArns": ["string"],
  "NetworkLoadBalancerArns": ["string"],
  "PrivateDnsName": "string",
  "ServiceId": "string",
  "ServiceName": "string",
  "ServiceState": "string",
  "ServiceType": [{
    "ServiceType": "string"
  }]
},
"AwsEc2VpcPeeringConnection": {
  "AcceptorVpcInfo": {
    "CidrBlock": "string",
    "CidrBlockSet": [{
      "CidrBlock": "string"
    }],
    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "string"
    }],
    "OwnerId": "string",
    "PeeringOptions": {
      "AllowDnsResolutionFromRemoteVpc": boolean,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
      "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
    },
    "Region": "string",
    "VpcId": "string"
  },
  "ExpirationTime": "string",
  "RequesterVpcInfo": {
    "CidrBlock": "string",
    "CidrBlockSet": [{
      "CidrBlock": "string"
    }],
    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "string"
    }],
    "OwnerId": "string",
    "PeeringOptions": {
```

```

    "AllowDnsResolutionFromRemoteVpc": boolean,
    "AllowEgressFromLocalClassicLinkToRemoteVpc": boolean,
    "AllowEgressFromLocalVpcToRemoteClassicLink": boolean
  },
  "Region": "string",
  "VpcId": "string"
},
"Status": {
  "Code": "string",
  "Message": "string"
},
"VpcPeeringConnectionId": "string"
},
"AwsEc2VpnConnection": {
  "Category": "string",
  "CustomerGatewayConfiguration": "string",
  "CustomerGatewayId": "string",
  "Options": {
    "StaticRoutesOnly": boolean,
    "TunnelOptions": [{
      "DpdTimeoutSeconds": number,
      "IkeVersions": ["string"],
      "OutsideIpAddress": "string",
      "Phase1DhGroupNumbers": [number],
      "Phase1EncryptionAlgorithms": ["string"],
      "Phase1IntegrityAlgorithms": ["string"],
      "Phase1LifetimeSeconds": number,
      "Phase2DhGroupNumbers": [number],
      "Phase2EncryptionAlgorithms": ["string"],
      "Phase2IntegrityAlgorithms": ["string"],
      "Phase2LifetimeSeconds": number,
      "PreSharedKey": "string",
      "RekeyFuzzPercentage": number,
      "RekeyMarginTimeSeconds": number,
      "ReplayWindowSize": number,
      "TunnelInsideCidr": "string"
    }]
  },
  "Routes": [{
    "DestinationCidrBlock": "string",
    "State": "string"
  }],
  "State": "string",
  "TransitGatewayId": "string",

```

```

    "Type": "string",
    "VgwTelemetry": [{
      "AcceptedRouteCount": number,
      "CertificateArn": "string",
      "LastStatusChange": "string",
      "OutsideIpAddress": "string",
      "Status": "string",
      "StatusMessage": "string"
    }],
    "VpnConnectionId": "string",
    "VpnGatewayId": "string"
  },
  "AwsEcrContainerImage": {
    "Architecture": "string",
    "ImageDigest": "string",
    "ImagePublishedAt": "string",
    "ImageTags": ["string"],
    "RegistryId": "string",
    "RepositoryName": "string"
  },
  "AwsEcrRepository": {
    "Arn": "string",
    "ImageScanningConfiguration": {
      "ScanOnPush": boolean
    },
    "ImageTagMutability": "string",
    "LifecyclePolicy": {
      "LifecyclePolicyText": "string",
      "RegistryId": "string"
    },
    "RepositoryName": "string",
    "RepositoryPolicyText": "string"
  },
  "AwsEcsCluster": {
    "ActiveServicesCount": number,
    "CapacityProviders": ["string"],
    "ClusterArn": "string",
    "ClusterName": "string",
    "ClusterSettings": [{
      "Name": "string",
      "Value": "string"
    }],
    "Configuration": {
      "ExecuteCommandConfiguration": {

```

```
"KmsKeyId": "string",
"LogConfiguration": {
  "CloudWatchEncryptionEnabled": boolean,
  "CloudWatchLogGroupName": "string",
  "S3BucketName": "string",
  "S3EncryptionEnabled": boolean,
  "S3KeyPrefix": "string"
},
"Logging": "string"
}
},
"DefaultCapacityProviderStrategy": [{
  "Base": number,
  "CapacityProvider": "string",
  "Weight": number
}],
"RegisteredContainerInstancesCount": number,
"RunningTasksCount": number,
"Status": "string"
},
"AwsEcsContainer": {
  "Image": "string",
  "MountPoints": [{
    "ContainerPath": "string",
    "SourceVolume": "string"
  }],
  "Name": "string",
  "Privileged": boolean
},
"AwsEcsService": {
  "CapacityProviderStrategy": [{
    "Base": number,
    "CapacityProvider": "string",
    "Weight": number
  }],
  "Cluster": "string",
  "DeploymentConfiguration": {
    "DeploymentCircuitBreaker": {
      "Enable": boolean,
      "Rollback": boolean
    },
    "MaximumPercent": number,
    "MinimumHealthyPercent": number
  }
},
```

```
"DeploymentController": {
  "Type": "string"
},
"DesiredCount": number,
"EnableEcsManagedTags": boolean,
"EnableExecuteCommand": boolean,
"HealthCheckGracePeriodSeconds": number,
"LaunchType": "string",
"LoadBalancers": [{
  "ContainerName": "string",
  "ContainerPort": number,
  "LoadBalancerName": "string",
  "TargetGroupArn": "string"
}],
"Name": "string",
"NetworkConfiguration": {
  "AwsVpcConfiguration": {
    "AssignPublicIp": "string",
    "SecurityGroups": ["string"],
    "Subnets": ["string"]
  }
},
"PlacementConstraints": [{
  "Expression": "string",
  "Type": "string"
}],
"PlacementStrategies": [{
  "Field": "string",
  "Type": "string"
}],
"PlatformVersion": "string",
"PropagateTags": "string",
"Role": "string",
"SchedulingStrategy": "string",
"ServiceArn": "string",
"ServiceName": "string",
"ServiceRegistries": [{
  "ContainerName": "string",
  "ContainerPort": number,
  "Port": number,
  "RegistryArn": "string"
}],
"TaskDefinition": "string"
},
```

```
"AwsEcsTask": {
  "CreatedAt": "string",
  "ClusterArn": "string",
  "Group": "string",
  "StartedAt": "string",
  "StartedBy": "string",
  "TaskDefinitionArn": "string",
  "Version": number,
  "Volumes": [{
    "Name": "string",
    "Host": {
      "SourcePath": "string"
    }
  ]},
  "Containers": [{
    "Image": "string",
    "MountPoints": [{
      "ContainerPath": "string",
      "SourceVolume": "string"
    }],
    "Name": "string",
    "Privileged": boolean
  ]
},
"AwsEcsTaskDefinition": {
  "ContainerDefinitions": [{
    "Command": ["string"],
    "Cpu": number,
    "DependsOn": [{
      "Condition": "string",
      "ContainerName": "string"
    }],
    "DisableNetworking": boolean,
    "DnsSearchDomains": ["string"],
    "DnsServers": ["string"],
    "DockerLabels": {
      "string": "string"
    },
    "DockerSecurityOptions": ["string"],
    "EntryPoint": ["string"],
    "Environment": [{
      "Name": "string",
      "Value": "string"
    }],
  ]},
```



```
"EnvironmentFiles": [{
  "Type": "string",
  "Value": "string"
}],
"Essential": boolean,
"ExtraHosts": [{
  "Hostname": "string",
  "IpAddress": "string"
}],
"FirelensConfiguration": {
  "Options": {
    "string": "string"
  },
  "Type": "string"
},
"HealthCheck": {
  "Command": ["string"],
  "Interval": number,
  "Retries": number,
  "StartPeriod": number,
  "Timeout": number
},
"Hostname": "string",
"Image": "string",
"Interactive": boolean,
"Links": ["string"],
"LinuxParameters": {
  "Capabilities": {
    "Add": ["string"],
    "Drop": ["string"]
  },
  "Devices": [{
    "ContainerPath": "string",
    "HostPath": "string",
    "Permissions": ["string"]
  }
],
"InitProcessEnabled": boolean,
"MaxSwap": number,
"SharedMemorySize": number,
"Swappiness": number,
"Tmpfs": [{
  "ContainerPath": "string",
  "MountOptions": ["string"],
  "Size": number
```

```
    ]]  
  },  
  "LogConfiguration": {  
    "LogDriver": "string",  
    "Options": {  
      "string": "string"  
    },  
    "SecretOptions": [{  
      "Name": "string",  
      "ValueFrom": "string"  
    }]  
  },  
  "Memory": number,  
  "MemoryReservation": number,  
  "MountPoints": [{  
    "ContainerPath": "string",  
    "ReadOnly": boolean,  
    "SourceVolume": "string"  
  }],  
  "Name": "string",  
  "PortMappings": [{  
    "ContainerPort": number,  
    "HostPort": number,  
    "Protocol": "string"  
  }],  
  "Privileged": boolean,  
  "PseudoTerminal": boolean,  
  "ReadOnlyRootFilesystem": boolean,  
  "RepositoryCredentials": {  
    "CredentialsParameter": "string"  
  },  
  "ResourceRequirements": [{  
    "Type": "string",  
    "Value": "string"  
  }],  
  "Secrets": [{  
    "Name": "string",  
    "ValueFrom": "string"  
  }],  
  "StartTimeout": number,  
  "StopTimeout": number,  
  "SystemControls": [{  
    "Namespace": "string",  
    "Value": "string"
```

```
    ]],
    "Ulimits": [{
      "HardLimit": number,
      "Name": "string",
      "SoftLimit": number
    }],
    "User": "string",
    "VolumesFrom": [{
      "ReadOnly": boolean,
      "SourceContainer": "string"
    }],
    "WorkingDirectory": "string"
  ]],
  "Cpu": "string",
  "ExecutionRoleArn": "string",
  "Family": "string",
  "InferenceAccelerators": [{
    "DeviceName": "string",
    "DeviceType": "string"
  }],
  "IpcMode": "string",
  "Memory": "string",
  "NetworkMode": "string",
  "PidMode": "string",
  "PlacementConstraints": [{
    "Expression": "string",
    "Type": "string"
  }],
  "ProxyConfiguration": {
    "ContainerName": "string",
    "ProxyConfigurationProperties": [{
      "Name": "string",
      "Value": "string"
    }],
    "Type": "string"
  },
  "RequiresCompatibilities": ["string"],
  "Status": "string",
  "TaskRoleArn": "string",
  "Volumes": [{
    "DockerVolumeConfiguration": {
      "Autoprovision": boolean,
      "Driver": "string",
      "DriverOpts": {
```

```

    "string": "string"
  },
  "Labels": {
    "string": "string"
  },
  "Scope": "string"
},
"EfsVolumeConfiguration": {
  "AuthorizationConfig": {
    "AccessPointId": "string",
    "Iam": "string"
  },
  "FilesystemId": "string",
  "RootDirectory": "string",
  "TransitEncryption": "string",
  "TransitEncryptionPort": number
},
"Host": {
  "SourcePath": "string"
},
"Name": "string"
}]
},
"AwsEfsAccessPoint": {
  "AccessPointId": "string",
  "Arn": "string",
  "ClientToken": "string",
  "FilesystemId": "string",
  "PosixUser": {
    "Gid": "string",
    "SecondaryGids": ["string"],
    "Uid": "string"
  },
  "RootDirectory": {
    "CreationInfo": {
      "OwnerGid": "string",
      "OwnerUid": "string",
      "Permissions": "string"
    },
    "Path": "string"
  }
},
"AwsEksCluster": {
  "Arn": "string",

```

```

    "CertificateAuthorityData": "string",
    "ClusterStatus": "string",
    "Endpoint": "string",
    "Logging": {
      "ClusterLogging": [{
        "Enabled": boolean,
        "Types": ["string"]
      }]
    },
    "Name": "string",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": boolean,
      "SecurityGroupIds": ["string"],
      "SubnetIds": ["string"]
    },
    "RoleArn": "string",
    "Version": "string"
  },
  "AwsElasticBeanstalkEnvironment": {
    "ApplicationName": "string",
    "Cname": "string",
    "DateCreated": "string",
    "DateUpdated": "string",
    "Description": "string",
    "EndpointUrl": "string",
    "EnvironmentArn": "string",
    "EnvironmentId": "string",
    "EnvironmentLinks": [{
      "EnvironmentName": "string",
      "LinkName": "string"
    }],
    "EnvironmentName": "string",
    "OptionSettings": [{
      "Namespace": "string",
      "OptionName": "string",
      "ResourceName": "string",
      "Value": "string"
    }],
    "PlatformArn": "string",
    "SolutionStackName": "string",
    "Status": "string",
    "Tier": {
      "Name": "string",
      "Type": "string",

```

```
"Version": "string",
},
"VersionLabel": "string",
},
"AwsElasticSearchDomain": {
  "AccessPolicies": "string",
  "DomainStatus": {
    "DomainId": "string",
    "DomainName": "string",
    "Endpoint": "string",
    "Endpoints": {
      "string": "string"
    }
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "ElasticsearchClusterConfig": {
    "DedicatedMasterCount": number,
    "DedicatedMasterEnabled": boolean,
    "DedicatedMasterType": "string",
    "InstanceCount": number,
    "InstanceType": "string",
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": number
    },
    "ZoneAwarenessEnabled": boolean
  },
  "ElasticsearchVersion": "string",
  "EncryptionAtRestOptions": {
    "Enabled": boolean,
    "KmsKeyId": "string"
  },
  "LogPublishingOptions": {
    "AuditLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    },
    "IndexSlowLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    },
    "SearchSlowLogs": {
```

```
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  }
},
"NodeToNodeEncryptionOptions": {
  "Enabled": boolean
},
"ServiceSoftwareOptions": {
  "AutomatedUpdateDate": "string",
  "Cancellable": boolean,
  "CurrentVersion": "string",
  "Description": "string",
  "NewVersion": "string",
  "UpdateAvailable": boolean,
  "UpdateStatus": "string"
},
"VPCOptions": {
  "AvailabilityZones": [
    "string"
  ],
  "SecurityGroupIds": [
    "string"
  ],
  "SubnetIds": [
    "string"
  ],
  "VPCId": "string"
}
},
"AwsElbLoadBalancer": {
  "AvailabilityZones": ["string"],
  "BackendServerDescriptions": [{
    "InstancePort": number,
    "PolicyNames": ["string"]
  }],
  "CanonicalHostedZoneName": "string",
  "CanonicalHostedZoneNameID": "string",
  "CreatedTime": "string",
  "DnsName": "string",
  "HealthCheck": {
    "HealthyThreshold": number,
    "Interval": number,
    "Target": "string",
    "Timeout": number,
```

```
    "UnhealthyThreshold": number
  },
  "Instances": [{
    "InstanceId": "string"
  }],
  "ListenerDescriptions": [{
    "Listener": {
      "InstancePort": number,
      "InstanceProtocol": "string",
      "LoadBalancerPort": number,
      "Protocol": "string",
      "SslCertificateId": "string"
    },
    "PolicyNames": ["string"]
  }],
  "LoadBalancerAttributes": {
    "AccessLog": {
      "EmitInterval": number,
      "Enabled": boolean,
      "S3BucketName": "string",
      "S3BucketPrefix": "string"
    },
    "ConnectionDraining": {
      "Enabled": boolean,
      "Timeout": number
    },
    "ConnectionSettings": {
      "IdleTimeout": number
    },
    "CrossZoneLoadBalancing": {
      "Enabled": boolean
    },
    "AdditionalAttributes": [{
      "Key": "string",
      "Value": "string"
    }]
  },
  "LoadBalancerName": "string",
  "Policies": {
    "AppCookieStickinessPolicies": [{
      "CookieName": "string",
      "PolicyName": "string"
    }],
    "LbCookieStickinessPolicies": [{
```



```
    "CookieExpirationPeriod": number,
    "PolicyName": "string"
  ]],
  "OtherPolicies": ["string"]
},
"Scheme": "string",
"SecurityGroups": ["string"],
"SourceSecurityGroup": {
  "GroupName": "string",
  "OwnerAlias": "string"
},
"Subnets": ["string"],
"VpcId": "string"
},
"AwsElbv2LoadBalancer": {
  "AvailabilityZones": {
    "SubnetId": "string",
    "ZoneName": "string"
  },
  "CanonicalHostedZoneId": "string",
  "CreatedTime": "string",
  "DNSName": "string",
  "IpAddressType": "string",
  "LoadBalancerAttributes": [{
    "Key": "string",
    "Value": "string"
  }],
  "Scheme": "string",
  "SecurityGroups": ["string"],
  "State": {
    "Code": "string",
    "Reason": "string"
  },
  "Type": "string",
  "VpcId": "string"
},
"AwsEventSchemasRegistry": {
  "Description": "string",
  "RegistryArn": "string",
  "RegistryName": "string"
},
"AwsEventsEndpoint": {
  "Arn": "string",
  "Description": "string",
```

```
"EndpointId": "string",
"EndpointUrl": "string",
"EventBuses": [
  {
    "EventBusArn": "string"
  },
  {
    "EventBusArn": "string"
  }
],
"Name": "string",
"ReplicationConfig": {
  "State": "string"
},
"RoleArn": "string",
"RoutingConfig": {
  "FailoverConfig": {
    "Primary": {
      "HealthCheck": "string"
    },
    "Secondary": {
      "Route": "string"
    }
  }
},
"State": "string"
},
"AwsEventsEventBus": {
  "Arn": "string",
  "Name": "string",
  "Policy": "string"
},
"AwsGuardDutyDetector": {
  "FindingPublishingFrequency": "string",
  "ServiceRole": "string",
  "Status": "string",
  "DataSources": {
    "CloudTrail": {
      "Status": "string"
    }
  },
  "DnsLogs": {
    "Status": "string"
  },
  "FlowLogs": {
```

```
    "Status": "string"
  },
  "S3Logs": {
    "Status": "string"
  },
  "Kubernetes": {
    "AuditLogs": {
      "Status": "string"
    }
  },
  "MalwareProtection": {
    "ScanEc2InstanceWithFindings": {
      "EbsVolumes": {
        "Status": "string"
      }
    }
  },
  "ServiceRole": "string"
}
},
"AwsIamAccessKey": {
  "AccessKeyId": "string",
  "AccountId": "string",
  "CreatedAt": "string",
  "PrincipalId": "string",
  "PrincipalName": "string",
  "PrincipalType": "string",
  "SessionContext": {
    "Attributes": {
      "CreationDate": "string",
      "MfaAuthenticated": boolean
    }
  },
  "SessionIssuer": {
    "AccountId": "string",
    "Arn": "string",
    "PrincipalId": "string",
    "Type": "string",
    "UserName": "string"
  }
},
"Status": "string"
},
"AwsIamGroup": {
  "AttachedManagedPolicies": [{
```

```
    "PolicyArn": "string",
    "PolicyName": "string"
  }],
  "CreateDate": "string",
  "GroupId": "string",
  "GroupName": "string",
  "GroupPolicyList": [{
    "PolicyName": "string"
  }],
  "Path": "string"
},
"AwsIamPolicy": {
  "AttachmentCount": number,
  "CreateDate": "string",
  "DefaultVersionId": "string",
  "Description": "string",
  "IsAttachable": boolean,
  "Path": "string",
  "PermissionsBoundaryUsageCount": number,
  "PolicyId": "string",
  "PolicyName": "string",
  "PolicyVersionList": [{
    "CreateDate": "string",
    "IsDefaultVersion": boolean,
    "VersionId": "string"
  }],
  "UpdateDate": "string"
},
"AwsIamRole": {
  "AssumeRolePolicyDocument": "string",
  "AttachedManagedPolicies": [{
    "PolicyArn": "string",
    "PolicyName": "string"
  }],
  "CreateDate": "string",
  "InstanceProfileList": [{
    "Arn": "string",
    "CreateDate": "string",
    "InstanceProfileId": "string",
    "InstanceProfileName": "string",
    "Path": "string",
    "Roles": [{
      "Arn": "string",
      "AssumeRolePolicyDocument": "string",
```

```
    "CreateDate": "string",
    "Path": "string",
    "RoleId": "string",
    "RoleName": "string"
  ]
}],
"MaxSessionDuration": number,
"Path": "string",
"PermissionsBoundary": {
  "PermissionsBoundaryArn": "string",
  "PermissionsBoundaryType": "string"
},
"RoleId": "string",
"RoleName": "string",
"RolePolicyList": [{
  "PolicyName": "string"
}]
},
"AwsIamUser": {
  "AttachedManagedPolicies": [{
    "PolicyArn": "string",
    "PolicyName": "string"
  }],
  "CreateDate": "string",
  "GroupList": ["string"],
  "Path": "string",
  "PermissionsBoundary": {
    "PermissionsBoundaryArn": "string",
    "PermissionsBoundaryType": "string"
  },
  "UserId": "string",
  "UserName": "string",
  "UserPolicyList": [{
    "PolicyName": "string"
  }]
},
"AwsKinesisStream": {
  "Arn": "string",
  "Name": "string",
  "RetentionPeriodHours": number,
  "ShardCount": number,
  "StreamEncryption": {
    "EncryptionType": "string",
    "KeyId": "string"
  }
}
```

```
    }
  },
  "AwsKmsKey": {
    "AWSAccountId": "string",
    "CreationDate": "string",
    "Description": "string",
    "KeyId": "string",
    "KeyManager": "string",
    "KeyRotationStatus": boolean,
    "KeyState": "string",
    "Origin": "string"
  },
  "AwsLambdaFunction": {
    "Architectures": [
      "string"
    ],
    "Code": {
      "S3Bucket": "string",
      "S3Key": "string",
      "S3ObjectVersion": "string",
      "ZipFile": "string"
    },
    "CodeSha256": "string",
    "DeadLetterConfig": {
      "TargetArn": "string"
    },
    "Environment": {
      "Variables": {
        "Stage": "string"
      }
    },
    "Error": {
      "ErrorCode": "string",
      "Message": "string"
    }
  },
  "FunctionName": "string",
  "Handler": "string",
  "KmsKeyArn": "string",
  "LastModified": "string",
  "Layers": {
    "Arn": "string",
    "CodeSize": number
  },
  "PackageType": "string",
```

```
"RevisionId": "string",
"Role": "string",
"Runtime": "string",
"Timeout": integer,
"TracingConfig": {
  "Mode": "string"
},
"Version": "string",
"VpcConfig": {
  "SecurityGroupIds": ["string"],
  "SubnetIds": ["string"]
},
"MasterArn": "string",
"MemorySize": number
},
"AwsLambdaLayerVersion": {
  "CompatibleRuntimes": [
    "string"
  ],
  "CreateDate": "string",
  "Version": number
},
"AwsMskCluster": {
  "ClusterInfo": {
    "ClientAuthentication": {
      "Sasl": {
        "Scram": {
          "Enabled": boolean
        },
        "Iam": {
          "Enabled": boolean
        }
      }
    },
    "Tls": {
      "CertificateAuthorityArnList": [],
      "Enabled": boolean
    },
    "Unauthenticated": {
      "Enabled": boolean
    }
  },
  "ClusterName": "string",
  "CurrentVersion": "string",
  "EncryptionInfo": {
```

```

    "EncryptionAtRest": {
      "DataVolumeKMSKeyId": "string"
    },
    "EncryptionInTransit": {
      "ClientBroker": "string",
      "InCluster": boolean
    }
  },
  "EnhancedMonitoring": "string",
  "NumberOfBrokerNodes": integer
}
},
"AwsNetworkFirewallFirewall": {
  "DeleteProtection": boolean,
  "Description": "string",
  "FirewallArn": "string",
  "FirewallId": "string",
  "FirewallName": "string",
  "FirewallPolicyArn": "string",
  "FirewallPolicyChangeProtection": boolean,
  "SubnetChangeProtection": boolean,
  "SubnetMappings": [{
    "SubnetId": "string"
  }],
  "VpcId": "string"
},
"AwsNetworkFirewallFirewallPolicy": {
  "Description": "string",
  "FirewallPolicy": {
    "StatefulRuleGroupReferences": [{
      "ResourceArn": "string"
    }],
    "StatelessCustomActions": [{
      "ActionDefinition": {
        "PublishMetricAction": {
          "Dimensions": [{
            "Value": "string"
          }]
        }
      }
    ]
  },
  "ActionName": "string"
}],
  "StatelessDefaultActions": ["string"],
  "StatelessFragmentDefaultActions": ["string"],

```



```

    "StatelessRuleGroupReferences": [{
      "Priority": number,
      "ResourceArn": "string"
    }]
  },
  "FirewallPolicyArn": "string",
  "FirewallPolicyId": "string",
  "FirewallPolicyName": "string"
},
"AwsNetworkFirewallRuleGroup": {
  "Capacity": number,
  "Description": "string",
  "RuleGroup": {
    "RulesSource": {
      "RulesSourceList": {
        "GeneratedRulesType": "string",
        "Targets": ["string"],
        "TargetTypes": ["string"]
      },
      "RulesString": "string",
      "StatefulRules": [{
        "Action": "string",
        "Header": {
          "Destination": "string",
          "DestinationPort": "string",
          "Direction": "string",
          "Protocol": "string",
          "Source": "string",
          "SourcePort": "string"
        },
        "RuleOptions": [{
          "Keyword": "string",
          "Settings": ["string"]
        }]
      }],
      "StatelessRulesAndCustomActions": {
        "CustomActions": [{
          "ActionDefinition": {
            "PublishMetricAction": {
              "Dimensions": [{
                "Value": "string"
              }]
            }
          }
        ]
      }
    }
  }
},

```

```
    "ActionName": "string"
  ]],
  "StatelessRules": [{
    "Priority": number,
    "RuleDefinition": {
      "Actions": ["string"],
      "MatchAttributes": {
        "DestinationPorts": [{
          "FromPort": number,
          "ToPort": number
        }],
        "Destinations": [{
          "AddressDefinition": "string"
        }],
        "Protocols": [number],
        "SourcePorts": [{
          "FromPort": number,
          "ToPort": number
        }],
        "Sources": [{
          "AddressDefinition": "string"
        }],
        "TcpFlags": [{
          "Flags": ["string"],
          "Masks": ["string"]
        }]
      }
    }
  ]
},
"RuleVariables": {
  "IpSets": {
    "Definition": ["string"]
  },
  "PortSets": {
    "Definition": ["string"]
  }
}
},
"RuleGroupArn": "string",
"RuleGroupId": "string",
"RuleGroupName": "string",
"Type": "string"
```

```
},
"AwsOpenSearchServiceDomain": {
  "AccessPolicies": "string",
  "AdvancedSecurityOptions": {
    "Enabled": boolean,
    "InternalUserDatabaseEnabled": boolean,
    "MasterUserOptions": {
      "MasterUserArn": "string",
      "MasterUserName": "string",
      "MasterUserPassword": "string"
    }
  },
  "Arn": "string",
  "ClusterConfig": {
    "DedicatedMasterCount": number,
    "DedicatedMasterEnabled": boolean,
    "DedicatedMasterType": "string",
    "InstanceCount": number,
    "InstanceType": "string",
    "WarmCount": number,
    "WarmEnabled": boolean,
    "WarmType": "string",
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": number
    },
    "ZoneAwarenessEnabled": boolean
  },
  "DomainEndpoint": "string",
  "DomainEndpointOptions": {
    "CustomEndpoint": "string",
    "CustomEndpointCertificateArn": "string",
    "CustomEndpointEnabled": boolean,
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "DomainEndpoints": {
    "string": "string"
  },
  "DomainName": "string",
  "EncryptionAtRestOptions": {
    "Enabled": boolean,
    "KmsKeyId": "string"
  },
  "EngineVersion": "string",
```

```
"Id": "string",
"LogPublishingOptions": {
  "AuditLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  },
  "IndexSlowLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  },
  "SearchSlowLogs": {
    "CloudWatchLogsLogGroupArn": "string",
    "Enabled": boolean
  }
},
"NodeToNodeEncryptionOptions": {
  "Enabled": boolean
},
"ServiceSoftwareOptions": {
  "AutomatedUpdateDate": "string",
  "Cancellable": boolean,
  "CurrentVersion": "string",
  "Description": "string",
  "NewVersion": "string",
  "OptionalDeployment": boolean,
  "UpdateAvailable": boolean,
  "UpdateStatus": "string"
},
"VpcOptions": {
  "SecurityGroupIds": ["string"],
  "SubnetIds": ["string"]
},
"AwsRdsDbCluster": {
  "ActivityStreamStatus": "string",
  "AllocatedStorage": number,
  "AssociatedRoles": [{
    "RoleArn": "string",
    "Status": "string"
  }],
  "AutoMinorVersionUpgrade": boolean,
  "AvailabilityZones": ["string"],
  "BackupRetentionPeriod": integer,
  "ClusterCreateTime": "string",
```

```
"CopyTagsToSnapshot": boolean,
"CrossAccountClone": boolean,
"CustomEndpoints": ["string"],
"DatabaseName": "string",
"DbClusterIdentifier": "string",
"DbClusterMembers": [{
  "DbClusterParameterGroupStatus": "string",
  "DbInstanceIdentifier": "string",
  "IsClusterWriter": boolean,
  "PromotionTier": integer
}],
"DbClusterOptionGroupMemberships": [{
  "DbClusterOptionGroupName": "string",
  "Status": "string"
}],
"DbClusterParameterGroup": "string",
"DbClusterResourceId": "string",
"DbSubnetGroup": "string",
"DeletionProtection": boolean,
"DomainMemberships": [{
  "Domain": "string",
  "Fqdn": "string",
  "IamRoleName": "string",
  "Status": "string"
}],
"EnabledCloudwatchLogsExports": ["string"],
"Endpoint": "string",
"Engine": "string",
"EngineMode": "string",
"EngineVersion": "string",
"HostedZoneId": "string",
"HttpEndpointEnabled": boolean,
"IamDatabaseAuthenticationEnabled": boolean,
"KmsKeyId": "string",
"MasterUsername": "string",
"MultiAz": boolean,
"Port": integer,
"PreferredBackupWindow": "string",
"PreferredMaintenanceWindow": "string",
"ReaderEndpoint": "string",
"ReadReplicaIdentifiers": ["string"],
"Status": "string",
"StorageEncrypted": boolean,
"VpcSecurityGroups": [{
```

```
    "Status": "string",
    "VpcSecurityGroupId": "string"
  ]
},
"AwsRdsDbClusterSnapshot": {
  "AllocatedStorage": integer,
  "AvailabilityZones": ["string"],
  "ClusterCreateTime": "string",
  "DbClusterIdentifier": "string",
  "DbClusterSnapshotAttributes": [{
    "AttributeName": "string",
    "AttributeValues": ["string"]
  }],
  "DbClusterSnapshotIdentifier": "string",
  "Engine": "string",
  "EngineVersion": "string",
  "IamDatabaseAuthenticationEnabled": boolean,
  "KmsKeyId": "string",
  "LicenseModel": "string",
  "MasterUsername": "string",
  "PercentProgress": integer,
  "Port": integer,
  "SnapshotCreateTime": "string",
  "SnapshotType": "string",
  "Status": "string",
  "StorageEncrypted": boolean,
  "VpcId": "string"
},
"AwsRdsDbInstance": {
  "AllocatedStorage": number,
  "AssociatedRoles": [{
    "RoleArn": "string",
    "FeatureName": "string",
    "Status": "string"
  }],
  "AutoMinorVersionUpgrade": boolean,
  "AvailabilityZone": "string",
  "BackupRetentionPeriod": number,
  "CACertificateIdentifier": "string",
  "CharacterSetName": "string",
  "CopyTagsToSnapshot": boolean,
  "DBClusterIdentifier": "string",
  "DBInstanceClass": "string",
  "DBInstanceIdentifier": "string",
```

```
"DbInstancePort": number,
"DbInstanceStatus": "string",
"DbiResourceId": "string",
"DBName": "string",
"DbParameterGroups": [{
  "DbParameterGroupName": "string",
  "ParameterApplyStatus": "string"
}],
"DbSecurityGroups": ["string"],
"DbSubnetGroup": {
  "DbSubnetGroupArn": "string",
  "DbSubnetGroupDescription": "string",
  "DbSubnetGroupName": "string",
  "SubnetGroupStatus": "string",
  "Subnets": [{
    "SubnetAvailabilityZone": {
      "Name": "string"
    },
    "SubnetIdentifier": "string",
    "SubnetStatus": "string"
  }],
  "VpcId": "string"
},
"DeletionProtection": boolean,
"Endpoint": {
  "Address": "string",
  "Port": number,
  "HostedZoneId": "string"
},
"DomainMemberships": [{
  "Domain": "string",
  "Fqdn": "string",
  "IamRoleName": "string",
  "Status": "string"
}],
"EnabledCloudwatchLogsExports": ["string"],
"Engine": "string",
"EngineVersion": "string",
"EnhancedMonitoringResourceArn": "string",
"IAMDatabaseAuthenticationEnabled": boolean,
"InstanceCreateTime": "string",
"Iops": number,
"KmsKeyId": "string",
"LatestRestorableTime": "string",
```

```
"LicenseModel": "string",
"ListenerEndpoint": {
  "Address": "string",
  "HostedZoneId": "string",
  "Port": number
},
"MasterUsername": "admin",
"MaxAllocatedStorage": number,
"MonitoringInterval": number,
"MonitoringRoleArn": "string",
"MultiAz": boolean,
"OptionGroupMemberships": [{
  "OptionGroupName": "string",
  "Status": "string"
}],
"PendingModifiedValues": {
  "AllocatedStorage": number,
  "BackupRetentionPeriod": number,
  "CaCertificateIdentifier": "string",
  "DbInstanceClass": "string",
  "DbInstanceIdentifier": "string",
  "DbSubnetGroupName": "string",
  "EngineVersion": "string",
  "Iops": number,
  "LicenseModel": "string",
  "MasterUserPassword": "string",
  "MultiAZ": boolean,
  "PendingCloudWatchLogsExports": {
    "LogTypesToDisable": ["string"],
    "LogTypesToEnable": ["string"]
  },
  "Port": number,
  "ProcessorFeatures": [{
    "Name": "string",
    "Value": "string"
  }],
  "StorageType": "string"
},
"PerformanceInsightsEnabled": boolean,
"PerformanceInsightsKmsKeyId": "string",
"PerformanceInsightsRetentionPeriod": number,
"PreferredBackupWindow": "string",
"PreferredMaintenanceWindow": "string",
"ProcessorFeatures": [{
```



```
    "Name": "string",
    "Value": "string"
  ]],
  "PromotionTier": number,
  "PubliclyAccessible": boolean,
  "ReadReplicaDBClusterIdentifiers": ["string"],
  "ReadReplicaDBInstanceIdentifiers": ["string"],
  "ReadReplicaSourceDBInstanceIdentifier": "string",
  "SecondaryAvailabilityZone": "string",
  "StatusInfos": [{
    "Message": "string",
    "Normal": boolean,
    "Status": "string",
    "StatusType": "string"
  }],
  "StorageEncrypted": boolean,
  "TdeCredentialArn": "string",
  "Timezone": "string",
  "VpcSecurityGroups": [{
    "VpcSecurityGroupId": "string",
    "Status": "string"
  }]
},
"AwsRdsDbSecurityGroup": {
  "DbSecurityGroupArn": "string",
  "DbSecurityGroupDescription": "string",
  "DbSecurityGroupName": "string",
  "Ec2SecurityGroups": [{
    "Ec2SecurityGroupuId": "string",
    "Ec2SecurityGroupName": "string",
    "Ec2SecurityGroupOwnerId": "string",
    "Status": "string"
  }],
  "IpRanges": [{
    "CidrIp": "string",
    "Status": "string"
  }],
  "OwnerId": "string",
  "VpcId": "string"
},
"AwsRdsDbSnapshot": {
  "AllocatedStorage": integer,
  "AvailabilityZone": "string",
  "DbInstanceIdentifier": "string",
```

```
"DbiResourceId": "string",
"DbSnapshotIdentifier": "string",
"Encrypted": boolean,
"Engine": "string",
"EngineVersion": "string",
"IamDatabaseAuthenticationEnabled": boolean,
"InstanceCreateTime": "string",
"Iops": number,
"KmsKeyId": "string",
"LicenseModel": "string",
"MasterUsername": "string",
"OptionGroupName": "string",
"PercentProgress": integer,
"Port": integer,
"ProcessorFeatures": [],
"SnapshotCreateTime": "string",
"SnapshotType": "string",
"SourceDbSnapshotIdentifier": "string",
"SourceRegion": "string",
"Status": "string",
"StorageType": "string",
"TdeCredentialArn": "string",
"Timezone": "string",
"VpcId": "string"
},
"AwsRdsEventSubscription": {
  "CustomerAwsId": "string",
  "CustSubscriptionId": "string",
  "Enabled": boolean,
  "EventCategoriesList": ["string"],
  "EventSubscriptionArn": "string",
  "SnsTopicArn": "string",
  "SourceIdsList": ["string"],
  "SourceType": "string",
  "Status": "string",
  "SubscriptionCreationTime": "string"
},
"AwsRedshiftCluster": {
  "AllowVersionUpgrade": boolean,
  "AutomatedSnapshotRetentionPeriod": number,
  "AvailabilityZone": "string",
  "ClusterAvailabilityStatus": "string",
  "ClusterCreateTime": "string",
  "ClusterIdentifier": "string",
```

```
"ClusterNodes": [{
  "NodeRole": "string",
  "PrivateIPAddress": "string",
  "PublicIPAddress": "string"
}],
"ClusterParameterGroups": [{
  "ClusterParameterStatusList": [{
    "ParameterApplyErrorDescription": "string",
    "ParameterApplyStatus": "string",
    "ParameterName": "string"
  }],
  "ParameterApplyStatus": "string",
  "ParameterGroupName": "string"
}],
"ClusterPublicKey": "string",
"ClusterRevisionNumber": "string",
"ClusterSecurityGroups": [{
  "ClusterSecurityGroupName": "string",
  "Status": "string"
}],
"ClusterSnapshotCopyStatus": {
  "DestinationRegion": "string",
  "ManualSnapshotRetentionPeriod": number,
  "RetentionPeriod": number,
  "SnapshotCopyGrantName": "string"
},
"ClusterStatus": "string",
"ClusterSubnetGroupName": "string",
"ClusterVersion": "string",
"DBName": "string",
"DeferredMaintenanceWindows": [{
  "DeferMaintenanceEndTime": "string",
  "DeferMaintenanceIdentifier": "string",
  "DeferMaintenanceStartTime": "string"
}],
"ElasticIpStatus": {
  "ElasticIp": "string",
  "Status": "string"
},
"ElasticResizeNumberOfNodeOptions": "string",
"Encrypted": boolean,
"Endpoint": {
  "Address": "string",
  "Port": number
}
```

```
},
"EnhancedVpcRouting": boolean,
"ExpectedNextSnapshotScheduleTime": "string",
"ExpectedNextSnapshotScheduleTimeStatus": "string",
"HsmStatus": {
  "HsmClientCertificateIdentifier": "string",
  "HsmConfigurationIdentifier": "string",
  "Status": "string"
},
"IamRoles": [{
  "ApplyStatus": "string",
  "IamRoleArn": "string"
}],
"KmsKeyId": "string",
"LoggingStatus":{
  "BucketName": "string",
  "LastFailureMessage": "string",
  "LastFailureTime": "string",
  "LastSuccessfulDeliveryTime": "string",
  "LoggingEnabled": boolean,
  "S3KeyPrefix": "string"
},
"MaintenanceTrackName": "string",
"ManualSnapshotRetentionPeriod": number,
"MasterUsername": "string",
"NextMaintenanceWindowStartTime": "string",
"NodeType": "string",
"NumberOfNodes": number,
"PendingActions": ["string"],
"PendingModifiedValues": {
  "AutomatedSnapshotRetentionPeriod": number,
  "ClusterIdentifier": "string",
  "ClusterType": "string",
  "ClusterVersion": "string",
  "EncryptionType": "string",
  "EnhancedVpcRouting": boolean,
  "MaintenanceTrackName": "string",
  "MasterUserPassword": "string",
  "NodeType": "string",
  "NumberOfNodes": number,
  "PubliclyAccessible": "string"
},
"PreferredMaintenanceWindow": "string",
"PubliclyAccessible": boolean,
```

```
"ResizeInfo": {
  "AllowCancelResize": boolean,
  "ResizeType": "string"
},
"RestoreStatus": {
  "CurrentRestoreRateInMegaBytesPerSecond": number,
  "ElapsedTimeInSeconds": number,
  "EstimatedTimeToCompletionInSeconds": number,
  "ProgressInMegaBytes": number,
  "SnapshotSizeInMegaBytes": number,
  "Status": "string"
},
"SnapshotScheduleIdentifier": "string",
"SnapshotScheduleState": "string",
"VpcId": "string",
"VpcSecurityGroups": [{
  "Status": "string",
  "VpcSecurityGroupId": "string"
}]
},
"AwsRoute53HostedZone": {
  "HostedZone": {
    "Id": "string",
    "Name": "string",
    "Config": {
      "Comment": "string"
    }
  },
  "NameServers": ["string"],
  "QueryLoggingConfig": {
    "CloudWatchLogsLogGroupArn": {
      "CloudWatchLogsLogGroupArn": "string",
      "Id": "string",
      "HostedZoneId": "string"
    }
  },
  "Vpcs": [
    {
      "Id": "string",
      "Region": "string"
    }
  ]
},
"AwsS3AccessPoint": {
```

```
"AccessPointArn": "string",
"Alias": "string",
"Bucket": "string",
"BucketAccountId": "string",
"Name": "string",
"NetworkOrigin": "string",
"PublicAccessBlockConfiguration": {
  "BlockPublicAcls": boolean,
  "BlockPublicPolicy": boolean,
  "IgnorePublicAcls": boolean,
  "RestrictPublicBuckets": boolean
},
"VpcConfiguration": {
  "VpcId": "string"
}
},
"AwsS3AccountPublicAccessBlock": {
  "BlockPublicAcls": boolean,
  "BlockPublicPolicy": boolean,
  "IgnorePublicAcls": boolean,
  "RestrictPublicBuckets": boolean
},
"AwsS3Bucket": {
  "AccessControlList": "string",
  "BucketLifecycleConfiguration": {
    "Rules": [{
      "AbortIncompleteMultipartUpload": {
        "DaysAfterInitiation": number
      },
      "ExpirationDate": "string",
      "ExpirationInDays": number,
      "ExpiredObjectDeleteMarker": boolean,
      "Filter": {
        "Predicate": {
          "Operands": [{
            "Prefix": "string",
            "Type": "string"
          },
          {
            "Tag": {
              "Key": "string",
              "Value": "string"
            },
            "Type": "string"
          }
        ]
      }
    }
  ]
}
```

```

    }
  ],
  "Type": "string"
}
},
"Id": "string",
"NoncurrentVersionExpirationInDays": number,
"NoncurrentVersionTransitions": [{
  "Days": number,
  "StorageClass": "string"
}],
"Prefix": "string",
"Status": "string",
"Transitions": [{
  "Date": "string",
  "Days": number,
  "StorageClass": "string"
}]
}]
},
"BucketLoggingConfiguration": {
  "DestinationBucketName": "string",
  "LogFilePrefix": "string"
},
"BucketName": "string",
"BucketNotificationConfiguration": {
  "Configurations": [{
    "Destination": "string",
    "Events": ["string"],
    "Filter": {
      "S3KeyFilter": {
        "FilterRules": [{
          "Name": "string",
          "Value": "string"
        }]
      }
    }
  ]
},
"Type": "string"
}]
},
"BucketVersioningConfiguration": {
  "IsMfaDeleteEnabled": boolean,
  "Status": "string"
},

```

```
"BucketWebsiteConfiguration": {
  "ErrorDocument": "string",
  "IndexDocumentSuffix": "string",
  "RedirectAllRequestsTo": {
    "HostName": "string",
    "Protocol": "string"
  },
  "RoutingRules": [{
    "Condition": {
      "HttpErrorCodeReturnedEquals": "string",
      "KeyPrefixEquals": "string"
    },
    "Redirect": {
      "HostName": "string",
      "HttpRedirectCode": "string",
      "Protocol": "string",
      "ReplaceKeyPrefixWith": "string",
      "ReplaceKeyWith": "string"
    }
  }]
},
"CreatedAt": "string",
"ObjectLockConfiguration": {
  "ObjectLockEnabled": "string",
  "Rule": {
    "DefaultRetention": {
      "Days": integer,
      "Mode": "string",
      "Years": integer
    }
  }
},
"OwnerAccountId": "string",
"OwnerId": "string",
"OwnerName": "string",
"PublicAccessBlockConfiguration": {
  "BlockPublicAcls": boolean,
  "BlockPublicPolicy": boolean,
  "IgnorePublicAcls": boolean,
  "RestrictPublicBuckets": boolean
},
"ServerSideEncryptionConfiguration": {
  "Rules": [{
    "ApplyServerSideEncryptionByDefault": {
```



```

        "KMSMasterKeyId": "string",
        "SSEAlgorithm": "string"
    }
  ]
}
},
"AwsS3Object": {
  "ContentType": "string",
  "ETag": "string",
  "LastModified": "string",
  "ServerSideEncryption": "string",
  "SSEKMSKeyId": "string",
  "VersionId": "string"
},
"AwsSagemakerNotebookInstance": {
  "DirectInternetAccess": "string",
  "InstanceMetadataServiceConfiguration": {
    "MinimumInstanceMetadataServiceVersion": "string"
  },
  "InstanceType": "string",
  "LastModifiedTime": "string",
  "NetworkInterfaceId": "string",
  "NotebookInstanceArn": "string",
  "NotebookInstanceName": "string",
  "NotebookInstanceStatus": "string",
  "PlatformIdentifier": "string",
  "RoleArn": "string",
  "RootAccess": "string",
  "SecurityGroups": ["string"],
  "SubnetId": "string",
  "Url": "string",
  "VolumeSizeInGB": number
},
"AwsSecretsManagerSecret": {
  "Deleted": boolean,
  "Description": "string",
  "KmsKeyId": "string",
  "Name": "string",
  "RotationEnabled": boolean,
  "RotationLambdaArn": "string",
  "RotationOccurredWithinFrequency": boolean,
  "RotationRules": {
    "AutomaticallyAfterDays": integer
  }
}

```

```
},
  "AwsSnsTopic": {
    "ApplicationSuccessFeedbackRoleArn": "string",
    "FirehoseFailureFeedbackRoleArn": "string",
    "FirehoseSuccessFeedbackRoleArn": "string",
    "HttpFailureFeedbackRoleArn": "string",
    "HttpSuccessFeedbackRoleArn": "string",
    "KmsMasterKeyId": "string",
    "Owner": "string",
    "SqsFailureFeedbackRoleArn": "string",
    "SqsSuccessFeedbackRoleArn": "string",
    "Subscription": {
      "Endpoint": "string",
      "Protocol": "string"
    },
    "TopicName": "string"
  },
  "AwsSqsQueue": {
    "DeadLetterTargetArn": "string",
    "KmsDataKeyReusePeriodSeconds": number,
    "KmsMasterKeyId": "string",
    "QueueName": "string"
  },
  "AwsSsmPatchCompliance": {
    "Patch": {
      "ComplianceSummary": {
        "ComplianceType": "string",
        "CompliantCriticalCount": integer,
        "CompliantHighCount": integer,
        "CompliantInformationalCount": integer,
        "CompliantLowCount": integer,
        "CompliantMediumCount": integer,
        "CompliantUnspecifiedCount": integer,
        "ExecutionType": "string",
        "NonCompliantCriticalCount": integer,
        "NonCompliantHighCount": integer,
        "NonCompliantInformationalCount": integer,
        "NonCompliantLowCount": integer,
        "NonCompliantMediumCount": integer,
        "NonCompliantUnspecifiedCount": integer,
        "OverallSeverity": "string",
        "PatchBaselineId": "string",
        "PatchGroup": "string",
        "Status": "string"
      }
    }
  }
}
```

```
    }
  }
},
"AwsStepFunctionStateMachine": {
  "StateMachineArn": "string",
  "Name": "string",
  "Status": "string",
  "RoleArn": "string",
  "Type": "string",
  "LoggingConfiguration": {
    "Level": "string",
    "IncludeExecutionData": boolean
  },
  "TracingConfiguration": {
    "Enabled": boolean
  }
},
"AwsWafRateBasedRule": {
  "MatchPredicates": [{
    "DataId": "string",
    "Negated": boolean,
    "Type": "string"
  }],
  "MetricName": "string",
  "Name": "string",
  "RateKey": "string",
  "RateLimit": number,
  "RuleId": "string"
},
"AwsWafRegionalRateBasedRule": {
  "MatchPredicates": [{
    "DataId": "string",
    "Negated": boolean,
    "Type": "string"
  }],
  "MetricName": "string",
  "Name": "string",
  "RateKey": "string",
  "RateLimit": number,
  "RuleId": "string"
},
"AwsWafRegionalRule": {
  "MetricName": "string",
  "Name": "string",
```

```

    "RuleId": "string",
    "PredicateList": [{
      "DataId": "string",
      "Negated": boolean,
      "Type": "string"
    }]
  },
  "AwsWafRegionalRuleGroup": {
    "MetricName": "string",
    "Name": "string",
    "RuleGroupId": "string",
    "Rules": [{
      "Action": {
        "Type": "string"
      },
      "Priority": number,
      "RuleId": "string",
      "Type": "string"
    }]
  },
  "AwsWafRegionalWebAcl": {
    "DefaultAction": "string",
    "MetricName": "string",
    "Name": "string",
    "RulesList": [{
      "Action": {
        "Type": "string"
      },
      "Priority": number,
      "RuleId": "string",
      "Type": "string",
      "ExcludedRules": [{
        "ExclusionType": "string",
        "RuleId": "string"
      }],
      "OverrideAction": {
        "Type": "string"
      }
    }],
    "WebAclId": "string"
  },
  "AwsWafRule": {
    "MetricName": "string",
    "Name": "string",

```

```
"PredicateList": [{
  "DataId": "string",
  "Negated": boolean,
  "Type": "string"
}],
"RuleId": "string"
},
"AwsWafRuleGroup": {
  "MetricName": "string",
  "Name": "string",
  "RuleGroupId": "string",
  "Rules": [{
    "Action": {
      "Type": "string"
    },
    "Priority": number,
    "RuleId": "string",
    "Type": "string"
  }]
},
"AwsWafv2RuleGroup": {
  "Arn": "string",
  "Capacity": number,
  "Description": "string",
  "Id": "string",
  "Name": "string",
  "Rules": [{
    "Action": {
      "Allow": {
        "CustomRequestHandling": {
          "InsertHeaders": [
            {
              "Name": "string",
              "Value": "string"
            },
            {
              "Name": "string",
              "Value": "string"
            }
          ]
        }
      }
    }
  ]
},
  "Name": "string",
```

```
"Priority": number,
"VisibilityConfig": {
  "CloudWatchMetricsEnabled": boolean,
  "MetricName": "string",
  "SampledRequestsEnabled": boolean
}
}],
"VisibilityConfig": {
  "CloudWatchMetricsEnabled": boolean,
  "MetricName": "string",
  "SampledRequestsEnabled": boolean
}
},
"AwsWafWebAcl": {
  "DefaultAction": "string",
  "Name": "string",
  "Rules": [{
    "Action": {
      "Type": "string"
    },
    "ExcludedRules": [{
      "RuleId": "string"
    }],
    "OverrideAction": {
      "Type": "string"
    },
    "Priority": number,
    "RuleId": "string",
    "Type": "string"
  }],
  "WebAclId": "string"
},
"AwsWafv2WebAcl": {
  "Arn": "string",
  "Capacity": number,
  "CaptchaConfig": {
    "ImmunityTimeProperty": {
      "ImmunityTime": number
    }
  },
  "DefaultAction": {
    "Block": {}
  },
  "Description": "string",
```

```
"ManagedbyFirewallManager": boolean,
"Name": "string",
"Rules": [{
  "Action": {
    "RuleAction": {
      "Block": {}
    }
  },
  "Name": "string",
  "Priority": number,
  "VisibilityConfig": {
    "SampledRequestsEnabled": boolean,
    "CloudWatchMetricsEnabled": boolean,
    "MetricName": "string"
  }
}],
"VisibilityConfig": {
  "SampledRequestsEnabled": boolean,
  "CloudWatchMetricsEnabled": boolean,
  "MetricName": "string"
},
"AwsXrayEncryptionConfig": {
  "KeyId": "string",
  "Status": "string",
  "Type": "string"
},
"Container": {
  "ContainerRuntime": "string",
  "ImageId": "string",
  "ImageName": "string",
  "LaunchedAt": "string",
  "Name": "string",
  "Privileged": boolean,
  "VolumeMounts": [{
    "Name": "string",
    "MountPath": "string"
  }]
},
"Other": {
  "string": "string"
},
"Id": "string",
"Partition": "string",
```

```
"Region": "string",
"ResourceRole": "string",
"Tags": {
  "string": "string"
},
>Type": "string"
}],
"SchemaVersion": "string",
"Severity": {
  "Label": "string",
  "Normalized": number,
  "Original": "string"
},
"Sample": boolean,
"SourceUrl": "string",
"Threats": [{
  "FilePaths": [{
    "FileName": "string",
    "FilePath": "string",
    "Hash": "string",
    "ResourceId": "string"
  }],
  "ItemCount": number,
  "Name": "string",
  "Severity": "string"
}],
"ThreatIntelIndicators": [{
  "Category": "string",
  "LastObservedAt": "string",
  "Source": "string",
  "SourceUrl": "string",
  "Type": "string",
  "Value": "string"
}],
>Title": "string",
"Types": ["string"],
"UpdatedAt": "string",
"UserDefinedFields": {
  "string": "string"
},
"VerificationState": "string",
"Vulnerabilities": [{
  "CodeVulnerabilities": [{
    "Cwes": [
```



```
"string",
"string"
],
"FilePath": {
  "EndLine": integer,
  "FileName": "string",
  "FilePath": "string",
  "StartLine": integer
},
"SourceArn": "string"
}],
"Cvss": [{
  "Adjustments": [{
    "Metric": "string",
    "Reason": "string"
  }],
  "BaseScore": number,
  "BaseVector": "string",
  "Source": "string",
  "Version": "string"
}],
"EpssScore": number,
"ExploitAvailable": "string",
"FixAvailable": "string",
"Id": "string",
"LastKnownExploitAt": "string",
"ReferenceUrls": ["string"],
"RelatedVulnerabilities": ["string"],
"Vendor": {
  "Name": "string",
  "Url": "string",
  "VendorCreatedAt": "string",
  "VendorSeverity": "string",
  "VendorUpdatedAt": "string"
},
"VulnerablePackages": [{
  "Architecture": "string",
  "Epoch": "string",
  "FilePath": "string",
  "FixedInVersion": "string",
  "Name": "string",
  "PackageManager": "string",
  "Release": "string",
  "Remediation": "string",
```

```
    "SourceLayerArn": "string",
    "SourceLayerHash": "string",
    "Version": "string"
  ]
}],
"Workflow": {
  "Status": "string"
},
"WorkflowState": "string"
}
]
```

Impatto del consolidamento sui campi e sui valori ASFF

Security Hub offre due tipi di consolidamento:

- Visualizzazione dei controlli consolidati (sempre attiva; non può essere disattivata): ogni controllo ha un unico identificatore per tutti gli standard. La pagina Controlli della console Security Hub mostra tutti i controlli tra gli standard.
- Risultati di controllo consolidati (possono essere attivati o disattivati): quando i risultati del controllo consolidato sono attivati, Security Hub produce un singolo risultato per un controllo di sicurezza anche quando un controllo è condiviso tra più standard. Questo ha lo scopo di ridurre il rumore di rilevamento. I risultati del controllo consolidato sono attivati per impostazione predefinita se hai abilitato Security Hub il 23 febbraio 2023 o dopo tale data. Altrimenti, è disattivata per impostazione predefinita. Tuttavia, i risultati del controllo consolidato sono attivati negli account dei membri di Security Hub solo se sono attivati nell'account amministratore. Se la funzionalità è disattivata nell'account amministratore, è disattivata negli account dei membri. Per istruzioni sull'attivazione di questa funzionalità, consulta [Attivazione dei risultati del controllo consolidato](#).

Entrambe le funzionalità apportano modifiche al controllo della ricerca di campi e valori in [AWS Formato ASFF \(Security Finding Format\)](#). Questa sezione riassume tali modifiche.

Visualizzazione dei controlli consolidati: modifiche ASFF

La funzionalità di visualizzazione dei controlli consolidati ha introdotto le seguenti modifiche al controllo dei campi e dei valori di ricerca nell'ASFF.

Se i flussi di lavoro non si basano sui valori di questi campi di ricerca dei controlli, non è richiesta alcuna azione.

Se disponi di flussi di lavoro che si basano sui valori specifici di questi campi di ricerca dei controlli, aggiorna i flussi di lavoro per utilizzare i valori correnti.

Campo ASFF	Valore di esempio prima della visualizzazione dei controlli consolidati	Valore di esempio dopo la visualizzazione dei controlli consolidati, più descrizione della modifica
Conformità. SecurityControlId	Non applicabile (nuovo campo)	<p>EC2.2</p> <p>Introduce un unico ID di controllo per tutti gli standard. <code>ProductFields.RuleId</code> fornisce ancora l'ID di controllo basato su standard per i controlli CIS v1.2.0. <code>ProductFields.ControlId</code> fornisce ancora l'ID di controllo basato su standard per i controlli di altri standard.</p>
Conformità. AssociatedStandards	Non applicabile (nuovo campo)	<p><code>[{» StandardsId «: «standards/ aws-foundational-security-best -practices/v/1.0.0 "}]</code></p> <p>Mostra in quali standard è abilitato un controllo.</p>

Campo ASFF	Valore di esempio prima della visualizzazione dei controlli consolidati	Valore di esempio dopo la visualizzazione dei controlli consolidati, più descrizione della modifica
ProductFields. ArchivalReasons. ----SEP----:0/ Descrizione	Non applicabile (nuovo campo)	<p>«Il risultato è in uno stato ARCHIVIATO perché i risultati del controllo consolidato sono stati attivati o disattivati. Ciò fa sì che i risultati dello stato precedente vengano archiviati quando vengono generati nuovi risultati».</p> <p>Descrive perché Security Hub ha archiviato i risultati esistenti.</p>
ProductFields. ArchivalReasons. ----set----:0/ ReasonCode	Non applicabile (nuovo campo)	<p>«CONSOLIDATED_CONTROLS_FINDINGS_UPDATE»</p> <p>Fornisce il motivo per cui Security Hub ha archiviato i risultati esistenti.</p>

Campo ASFF	Valore di esempio prima della visualizzazione dei controlli consolidati	Valore di esempio dopo la visualizzazione dei controlli consolidati, più descrizione della modifica
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Questo campo non fa più riferimento a uno standard.
Rimediazione.Raccomandazione.Testo	«Per istruzioni su come risolvere questo problema, consulta la documentazione PCI DSS AWS di Security Hub.»	«Per istruzioni su come correggere questo problema, consulta la documentazione sui controlli del AWS Security Hub». Questo campo non fa più riferimento a uno standard.
Remediation.Recommendation.Url	https://docs.aws.amazon.com/console/securityhub/PCI.EC2.2/remediation	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation Questo campo non fa più riferimento a uno standard.

Risultati di controllo consolidati: modifiche ASFF

Se attivi i risultati del controllo consolidato, potresti essere interessato dalle seguenti modifiche al controllo dei campi e dei valori di ricerca nell'ASFF. Queste modifiche si aggiungono alle modifiche precedentemente descritte per la visualizzazione dei controlli consolidati.

Se i flussi di lavoro non si basano sui valori di questi campi di ricerca dei controlli, non è richiesta alcuna azione.

Se disponi di flussi di lavoro che si basano sui valori specifici di questi campi di ricerca dei controlli, aggiorna i flussi di lavoro per utilizzare i valori correnti.

Note

[Automated Security Response nella versione AWS 2.0.0 supporta](#) risultati di controllo consolidati. Se si utilizza questa versione della soluzione, è possibile mantenere i flussi di lavoro attivando i risultati del controllo consolidato.

Campo ASFF	Valore di esempio prima di attivare i risultati del controllo consolidato	Valore di esempio dopo aver attivato i risultati del controllo consolidato e descrizione della modifica
GeneratorId	aws-foundational-security-best-Pratiche/v/1.0.0/config.1	Controllo di sicurezza/config.1 Questo campo non fa più riferimento a uno standard.
Title	PCI.config.1 dovrebbe AWS Config essere abilitato	AWS Config dovrebbe essere abilitato Questo campo non fa più riferimento a informazioni specifiche dello standard.
Id	arn:aws:securityhub:eu-central-1:123456789012:subscription/pci-DSS/v/3.2.1/pci.iam.5/finding/A	arn:aws:securityhub:eu-central-1:123456789012: security-

Campo ASFF	Valore di esempio prima di attivare i risultati del controllo consolidato	Valore di esempio dopo aver attivato i risultati del controllo consolidato e descrizione della modifica
	B6D6A26-A156-48F0-9403-115983E5A956	control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956 Questo campo non fa più riferimento a uno standard.
ProductFields.ControlId	PCI.EC2.2	Rimosso. Vedi <code>Compliance.SecurityControlId</code> invece. Questo campo viene rimosso a favore di un unico ID di controllo indipendente dagli standard.
ProductFields.RuleId	1.3	Rimosso. Vedi <code>Compliance.SecurityControlId</code> invece. Questo campo viene rimosso a favore di un unico ID di controllo indipendente dagli standard.
Descrizione	Questo controllo PCI DSS verifica se AWS Config è abilitato nell'account e nella regione correnti.	Questo AWS controllo verifica se AWS Config è abilitato nell'account e nella regione correnti. Questo campo non fa più riferimento a uno standard.

Campo ASFF	Valore di esempio prima di attivare i risultati del controllo consolidato	Valore di esempio dopo aver attivato i risultati del controllo consolidato e descrizione della modifica
Gravità	<pre>«Severità»: { «Prodotto»: 90, «Etichetta»: «CRITICAL», «Normalizzato»: 90, «Originale»: «CRITICO» }</pre>	<pre>«Severità»: { «Etichetta»: «CRITICAL», «Normalizzato»: 90, «Originale»: «CRITICO» }</pre> <p>Security Hub non utilizza più il campo Prodotto per descrivere la gravità di un risultato.</p>
Tipi	["Controlli del software e della configurazione/Standard di settore e normativi/PCI-DSS"]	["Controlli del software e della configurazione/Standard normativi e di settore"] <p>Questo campo non fa più riferimento a uno standard.</p>
Conformità. RelatedRequirements	["PCI DSS 10.5.2", «PCI DSS 11,5", «Fondamenti CIS 2.5"] AWS	["PCI DSS versione 3.2.1/10.5.2", «PCI DSS versione 3.2.1/11.5", «Benchmark AWS CIS Foundations v1.2.0/2.5"] <p>Questo campo mostra i requisiti correlati in tutti gli standard abilitati.</p>

Campo ASFF	Valore di esempio prima di attivare i risultati del controllo consolidato	Valore di esempio dopo aver attivato i risultati del controllo consolidato e descrizione della modifica
CreatedAt	2022-05-05T 08:18:13.138 Z	2022-09-25T 08:18:13,138 Z Il formato rimane lo stesso, ma il valore viene reimpostato quando si attivano i risultati del controllo consolidato.
FirstObservedAt	2022-05-07T 08:18:13.138 Z	2022-09-28T 08:18:13.138 Z Il formato rimane lo stesso, ma il valore viene reimpostato quando si attivano i risultati del controllo consolidato.
ProductFields.RecommendationUrl	https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation	Rimosso. Vedi Remediation.Recommendation.Url invece.
ProductFields.StandardsArn	arn:aws:securityhub::standards/-practices/v/1.0.0 aws-foundational-security-best	Rimosso. Vedi Compliance.AssociatedStandards invece.
ProductFields.StandardsControlArn	arn:aws:securityhub:us-east-1:123456789012:control/-practices/v/1.0.0/config.1 aws-foundational-security-best	Rimosso. Security Hub genera un risultato per un controllo di sicurezza tra gli standard.
ProductFields.StandardsGuideArn	arn:aws:securityhub::ruleset/v/1.2.0 cis-aws-foundations-benchmark	Rimosso. Vedi Compliance.AssociatedStandards invece.

Campo ASFF	Valore di esempio prima di attivare i risultati del controllo consolidato	Valore di esempio dopo aver attivato i risultati del controllo consolidato e descrizione della modifica
ProductFields.StandardsGuideSubscriptionArn	arn:aws:securityhub:us-east-2:123456789012:subscription/v/1.2.0 cis-aws-foundations-benchmark	Rimosso. Security Hub genera un risultato per un controllo di sicurezza tra gli standard.
ProductFields.StandardsSubscriptionArn	arn:aws:securityhub:us-east-1:123456789012:subscription/-practices/v/1.0.0 aws-foundational-security-best	Rimosso. Security Hub genera un risultato per un controllo di sicurezza tra gli standard.
ProductFields.aws/securityhub/ FindingId	arn:aws:securityhub:us-east-1: :product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/-practices/v/1.0.0/config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 aws-foundational-security-best	arn:aws:securityhub:us-east-1: :product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:security-control/config.1/finding/751c2173-7372-4e12-8656-a5210dfb1d67 Questo campo non fa più riferimento a uno standard.

Valori per i campi ASFF forniti dal cliente dopo l'attivazione dei risultati del controllo consolidato

Se attivi i [risultati del controllo consolidato](#), Security Hub genera un risultato per tutti gli standard e archivia i risultati originali (risultati separati per ogni standard). Per visualizzare i risultati archiviati, puoi visitare la pagina Findings della console Security Hub con il filtro Record state impostato su ARCHIVED oppure utilizzare l'azione [GetFindingsAPI](#). Gli aggiornamenti che hai apportato ai risultati originali nella console di Security Hub o utilizzando l'[BatchUpdateFindingsAPI](#) non verranno conservati nei nuovi risultati (se necessario, puoi recuperare questi dati facendo riferimento ai risultati archiviati).

Campo ASFF fornito dal cliente	Descrizione della modifica dopo l'attivazione dei risultati del controllo consolidato
Confidence	Ripristina lo stato vuoto.
Criticità	Ripristina lo stato vuoto.
Nota	Si ripristina allo stato vuoto.
RelatedFindings	Si ripristina allo stato vuoto.
Gravità	Gravità predefinita del risultato (corrisponde alla gravità del controllo).
Tipi	Ripristina il valore indipendente dallo standard.
UserDefinedFields	Ripristina lo stato vuoto.
VerificationState	Si ripristina allo stato vuoto.
Flusso di lavoro	Il valore predefinito dei nuovi risultati non riusciti è. NEW I nuovi risultati passati hanno un valore predefinito diRESOLVED.

ID del generatore prima e dopo l'attivazione dei risultati del controllo consolidato

Ecco un elenco delle modifiche all'ID del generatore per i controlli quando attivi i risultati del controllo consolidato. Si applicano ai controlli supportati da Security Hub a partire dal 15 febbraio 2023.

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
arn:aws:securityhub: :ruleset/ /v/1.2.0/rule/1.1 cis-aws-foundations-benchmark	controllo di sicurezza/ 1. CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.10 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.16

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.11 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.17
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.12 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.4
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.13 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.9
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.14 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.6
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.16 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.2
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.2 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.5
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.20 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.18
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.22 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.1
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.3 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.8
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.4 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.3
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.5 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.11
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.6 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.12

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.7 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.13
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.8 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.14
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/1.9 cis-aws-foundations-benchmark	Controllo di sicurezza/IAM.15
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.1 cis-aws-foundations-benchmark	controllo di sicurezza/ 1. CloudTrail
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.2 cis-aws-foundations-benchmark	controllo di sicurezza/ 4. CloudTrail
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.3 cis-aws-foundations-benchmark	controllo di sicurezza/ 6. CloudTrail
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.4 cis-aws-foundations-benchmark	controllo di sicurezza/ 5. CloudTrail
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.5 cis-aws-foundations-benchmark	Controllo di sicurezza/config.1
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.6 cis-aws-foundations-benchmark	controllo di sicurezza/ .7 CloudTrail
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.7 cis-aws-foundations-benchmark	controllo di sicurezza/ 2. CloudTrail
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.8 cis-aws-foundations-benchmark	Controllo di sicurezza/KMS.4
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/2.9 cis-aws-foundations-benchmark	Controllo di sicurezza/EC2.6

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.1 cis-aws-foundations-benchmark	controllo di sicurezza/ 2. CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.2 cis-aws-foundations-benchmark	controllo di sicurezza/ 3. CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.3 cis-aws-foundations-benchmark	controllo di sicurezza/ 1. CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.4 cis-aws-foundations-benchmark	controllo di sicurezza/4. CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.5 cis-aws-foundations-benchmark	controllo di sicurezza/ 5. CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.6 cis-aws-foundations-benchmark	controllo di sicurezza/ 6. CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.7 cis-aws-foundations-benchmark	controllo di sicurezza/ .7 CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.8 cis-aws-foundations-benchmark	controllo di sicurezza/ .8 CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.9 cis-aws-foundations-benchmark	controllo di sicurezza/ .9 CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.10 cis-aws-foundations-benchmark	controllo di sicurezza/ 1.0 CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.11 cis-aws-foundations-benchmark	controllo di sicurezza/ .11 CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.12 cis-aws-foundations-benchmark	controllo di sicurezza/ 1.2 CloudWatch

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.13 cis-aws-foundations-benchmark	controllo di sicurezza/ .13 CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/3.14 cis-aws-foundations-benchmark	controllo di sicurezza/ 1.4 CloudWatch
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/4.1 cis-aws-foundations-benchmark	Controllo di sicurezza/EC2.13
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/4.2 cis-aws-foundations-benchmark	Controllo di sicurezza/EC2.14
arn:aws:securityhub: ::ruleset/ /v/1.2.0/rule/4.3 cis-aws-foundations-benchmark	Controllo di sicurezza/EC2.2
cis-aws-foundations-benchmark/v/1.4.0/1.10	Controllo di sicurezza/IAM.5
cis-aws-foundations-benchmark/v/1.4.0/1.14	Controllo di sicurezza/IAM.3
cis-aws-foundations-benchmark/v/1.4.0/1.16	Controllo di sicurezza/IAM.1
cis-aws-foundations-benchmark/v/1.4.0/1.17	Controllo di sicurezza/IAM.18
cis-aws-foundations-benchmark/v/1.4.0/1.4	Controllo di sicurezza/IAM.4
cis-aws-foundations-benchmark/v/1.4.0/1.5	Controllo di sicurezza/IAM.9
cis-aws-foundations-benchmark/v/1.4.0/1.6	Controllo di sicurezza/IAM.6
cis-aws-foundations-benchmark/v/1.4.0/1.7	controllo di sicurezza/ 1CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/1.8	Controllo di sicurezza/IAM.15
cis-aws-foundations-benchmark/v/1.4.0/1.9	Controllo di sicurezza/IAM.16
cis-aws-foundations-benchmark/v/1.4.0/2.1.2	Controlli di sicurezza/s3.5
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.1	Controlli di sicurezza/s3.1

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
cis-aws-foundations-benchmark/v/1.4.0/2.1.5.2	Controllo di sicurezza/s3.8
cis-aws-foundations-benchmark/v/1.4.0/2.2.1	Controllo di sicurezza/EC2.7
cis-aws-foundations-benchmark/v/1.4.0/2.3.1	Controllo di sicurezza/RDS.3
cis-aws-foundations-benchmark/v/1.4.0/3.1	controllo di sicurezza/ 1CloudTrail.
cis-aws-foundations-benchmark/v/1.4.0/3.2	controllo di sicurezza/ 4. CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.4	controllo di sicurezza/ 5. CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.5	Controllo di sicurezza/config.1
cis-aws-foundations-benchmark/v/1.4.0/3.6	Controllo di sicurezza/s3.9
cis-aws-foundations-benchmark/v/1.4.0/3.7	controllo di sicurezza/ 2. CloudTrail
cis-aws-foundations-benchmark/v/1.4.0/3.8	Controllo di sicurezza/KMS.4
cis-aws-foundations-benchmark/v/1.4.0/3.9	Controllo di sicurezza/EC2.6
cis-aws-foundations-benchmark/v/1.4.0/4.3	controllo di sicurezza/ 1CloudWatch.
cis-aws-foundations-benchmark/v/1.4.0/4.4	controllo di sicurezza/ 4. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.5	controllo di sicurezza/ 5. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.6	controllo di sicurezza/ 6. CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.7	controllo di sicurezza/ .7 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.8	controllo di sicurezza/ .8 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.9	controllo di sicurezza/ .9 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.10	controllo di sicurezza/ .10 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.11	controllo di sicurezza/ .11 CloudWatch

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
cis-aws-foundations-benchmark/v/1.4.0/4.12	controllo di sicurezza/ .12 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.13	controllo di sicurezza/ .13 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/4.14	controllo di sicurezza/ 1.4 CloudWatch
cis-aws-foundations-benchmark/v/1.4.0/5.1	Controllo di sicurezza/EC2.21
cis-aws-foundations-benchmark/v/1.4.0/5.3	Controllo di sicurezza/EC2.2
aws-foundational-security-best-Pratiche/v/1.0.0/Account.1	Security-Control/Account.1
aws-foundational-security-best-Pratiche/v/1.0.0/ACM.1	Controllo di sicurezza/ACM.1
aws-foundational-security-best-Pratiche/v/1.0.0/APIGateway.1	Controllo di sicurezza/API Gateway.1
aws-foundational-security-best-Pratiche/v/1.0.0/ApiGateway.2	Controllo di sicurezza/API Gateway.2
aws-foundational-security-best-Pratiche/v/1.0.0/ApiGateway.3	Controllo di sicurezza/API Gateway.3
aws-foundational-security-best-Pratiche/v/1.0.0/ApiGateway.4	Controllo di sicurezza/API Gateway.4
aws-foundational-security-best-Pratiche/v/1.0.0/ApiGateway.5	Controllo di sicurezza/API Gateway.5
aws-foundational-security-best-Pratiche/v/1.0.0/ApiGateway.8	Controllo di sicurezza/API Gateway.8
aws-foundational-security-best-Pratiche/v/1.0.0/ApiGateway.9	Controllo di sicurezza/API Gateway.9

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-pratiche/v/1.0.0/ .1 AutoScaling	controllo di sicurezza/ .1 AutoScaling
aws-foundational-security-best-pratiche/v/1.0.0/ .2 AutoScaling	controllo di sicurezza/ .2 AutoScaling
aws-foundational-security-best-pratiche/v/1.0.0/ .3 AutoScaling	controllo di sicurezza/ .3 AutoScaling
aws-foundational-security-best-Practices/v/1.0.0/AutoScaling.5	Controllo di sicurezza/scalabilità automatica. 5
aws-foundational-security-best-pratiche/v/1.0.0/ .6 AutoScaling	controllo di sicurezza/ .6 AutoScaling
aws-foundational-security-best-pratiche/v/1.0.0/ .9 AutoScaling	controllo di sicurezza/ .9 AutoScaling
aws-foundational-security-best-pratiche/v/1.0.0/ .1 CloudFront	controllo di sicurezza/ .1 CloudFront
aws-foundational-security-best-pratiche/v/1.0.0/ .3 CloudFront	controllo di sicurezza/ .3 CloudFront
aws-foundational-security-best-pratiche/v/1.0.0/ .4 CloudFront	controllo di sicurezza/ .4 CloudFront
aws-foundational-security-best-pratiche/v/1.0.0/ .5 CloudFront	controllo di sicurezza/ .5 CloudFront
aws-foundational-security-best-pratiche/v/1.0.0/ .6 CloudFront	controllo di sicurezza/ .6 CloudFront
aws-foundational-security-best-pratiche/v/1.0.0/ .7 CloudFront	controllo di sicurezza/ .7 CloudFront

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-pratiche/v/1.0 .0/ .8 CloudFront	controllo di sicurezza/ .8 CloudFront
aws-foundational-security-best-pratiche/v/1.0 .0/ .9 CloudFront	controllo di sicurezza/ .9 CloudFront
aws-foundational-security-best-pratiche/v/1.0 .0/ .10 CloudFront	controllo di sicurezza/ .10 CloudFront
aws-foundational-security-best-pratiche/v/1.0 .0/ .12 CloudFront	controllo di sicurezza/ .12 CloudFront
aws-foundational-security-best-pratiche/v/1.0 .0/ .1 CloudTrail	controllo di sicurezza/ .1 CloudTrail
aws-foundational-security-best-pratiche/v/1.0 .0/ .2 CloudTrail	controllo di sicurezza/ .2 CloudTrail
aws-foundational-security-best-pratiche/v/1.0 .0/ .4 CloudTrail	controllo di sicurezza/ .4 CloudTrail
aws-foundational-security-best-pratiche/v/1.0 .0/ .5 CloudTrail	controllo di sicurezza/ .5 CloudTrail.
aws-foundational-security-best-pratiche/v/1.0 .0/ .1 CodeBuild	controllo di sicurezza/ .1 CodeBuild
aws-foundational-security-best-pratiche/v/1.0 .0/ .2 CodeBuild	controllo di sicurezza/ .2 CodeBuild
aws-foundational-security-best-pratiche/v/1.0 .0/ .3 CodeBuild	controllo di sicurezza/ .3 CodeBuild
aws-foundational-security-best-pratiche/v/1.0 .0/ .4 CodeBuild	controllo di sicurezza/ .4 CodeBuild

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-Pratiche/v/1.0.0/config.1	Controllo di sicurezza/config.1
aws-foundational-security-best-Pratiche/v/1.0.0/DMS.1	Controllo di sicurezza/DMS.1
aws-foundational-security-best-Pratiche/v/1.0.0/DynamoDB.1	Controllo della sicurezza/DynamoDB.1
aws-foundational-security-best-Pratiche/V/1.0.0/DynamoDB.2	Controllo della sicurezza/DynamoDB.2
aws-foundational-security-best-Pratiche/v/1.0.0/DynamoDB.3	Controllo di sicurezza/DynamoDB.3
aws-foundational-security-best-Pratiche/v/1.0.0/EC2.1	Controllo di sicurezza/EC 2.1
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.3	Controllo di sicurezza/EC2.3
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.4	Controllo di sicurezza/EC2.4
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.6	Controllo di sicurezza/EC2.6
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.7	Controllo di sicurezza/EC2.7
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.8	Controllo di sicurezza/EC2.8
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.9	Controllo di sicurezza/EC2.9

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.10	Controllo di sicurezza/EC2.10
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.15	Controllo di sicurezza/EC2.15
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.16	Controllo di sicurezza/EC2.16
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.17	Controllo di sicurezza/EC2.17
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.18	Controllo di sicurezza/EC2.18
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.19	Controllo di sicurezza/EC2.19
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.2	Controllo di sicurezza/EC2.2
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.20	Controllo di sicurezza/EC2.20
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.21	Controllo di sicurezza/EC2.21
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.23	Controllo di sicurezza/EC2.23
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.24	Controllo di sicurezza/EC2.24
aws-foundational-security-best-Pratiche/V/1.0.0/EC2.25	Controllo di sicurezza/EC2.25

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-Pratiche/V/1.0.0/ECR.1	Controllo di sicurezza/ECR.1
aws-foundational-security-best-Pratiche/V/1.0.0/ECR.2	Controllo di sicurezza/ECR.2
aws-foundational-security-best-Pratiche/V/1.0.0/ECR.3	Controllo di sicurezza/ECR.3
aws-foundational-security-best-Pratiche/V/1.0.0/ECS.1	Controllo di sicurezza/ECS.1
aws-foundational-security-best-Pratiche/v/1.0.0/ECS.10	Controllo di sicurezza/ECS.10
aws-foundational-security-best-Pratiche/v/1.0.0/ECS.12	Controllo di sicurezza/ECS.12
aws-foundational-security-best-Pratiche/v/1.0.0/ECS.2	Controllo di sicurezza/ECS.2
aws-foundational-security-best-Pratiche/V/1.0.0/ECS.3	Controllo di sicurezza/ECS.3
aws-foundational-security-best-Pratiche/V/1.0.0/ECS.4	Controllo di sicurezza/ECS.4
aws-foundational-security-best-Pratiche/V/1.0.0/ECS.5	Controllo di sicurezza/ECS.5
aws-foundational-security-best-Pratiche/v/1.0.0/ECS.8	Controllo di sicurezza/ECS.8
aws-foundational-security-best-Pratiche/V/1.0.0/EFS.1	Controllo di sicurezza/EFS.1

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-Pratiche/V/1.0.0/EFS.2	Controllo di sicurezza/EFS.2
aws-foundational-security-best-Pratiche/V/1.0.0/EFS.3	Controllo di sicurezza/EFS.3
aws-foundational-security-best-Pratiche/V/1.0.0/EFS.4	Controllo di sicurezza/EFS.4
aws-foundational-security-best-Pratiche/v/1.0.0/EKS.2	Controllo di sicurezza/EKS.2
aws-foundational-security-best-pratiche/v/1.0.0/.1 ElasticBeanstalk	controllo di sicurezza/.1 ElasticBeanstalk
aws-foundational-security-best-pratiche/v/1.0.0/.2 ElasticBeanstalk	controllo di sicurezza/.2 ElasticBeanstalk
aws-foundational-security-best-Pratiche/v/1.0.0/ELBV2.1	Controllo di sicurezza/ELB.1
aws-foundational-security-best-Pratiche/V/1.0.0/ELB.2	Controllo di sicurezza/ELB.2
aws-foundational-security-best-Pratiche/V/1.0.0/ELB.3	Controllo di sicurezza/ELB.3
aws-foundational-security-best-Pratiche/V/1.0.0/ELB.4	Controllo di sicurezza/ELB.4
aws-foundational-security-best-Pratiche/V/1.0.0/ELB.5	Controllo di sicurezza/ELB.5
aws-foundational-security-best-Pratiche/V/1.0.0/ELB.6	Controllo di sicurezza/ELB.6

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-Pratiche/V/1.0.0/ELB.7	Controllo di sicurezza/ELB.7
aws-foundational-security-best-Pratiche/V/1.0.0/ELB.8	Controllo di sicurezza/ELB.8
aws-foundational-security-best-Pratiche/V/1.0.0/ELB.9	Controllo di sicurezza/ELB.9
aws-foundational-security-best-Pratiche/v/1.0.0/ELB.10	Controllo di sicurezza/ELB.10
aws-foundational-security-best-Pratiche/v/1.0.0/ELB.11	Controllo di sicurezza/ELB.11
aws-foundational-security-best-Pratiche/v/1.0.0/ELB.12	Controllo di sicurezza/ELB.12
aws-foundational-security-best-Pratiche/v/1.0.0/ELB.13	Controllo di sicurezza/ELB.13
aws-foundational-security-best-Pratiche/v/1.0.0/ELB.14	Controllo di sicurezza/ELB.14
aws-foundational-security-best-Pratiche/V/1.0.0/EMR.1	Controllo di sicurezza/EMR.1
aws-foundational-security-best-Pratiche/v/1.0.0/ES.1	Controllo di sicurezza/ES.1
aws-foundational-security-best-Pratiche/v/1.0.0/ES.2	Controllo di sicurezza/ES.2
aws-foundational-security-best-Pratiche/v/1.0.0/ES.3	Controllo di sicurezza/ES.3

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-Pratiche/v/1.0.0/ES.4	Controllo di sicurezza/ES.4
aws-foundational-security-best-Pratiche/v/1.0.0/ES.5	Controllo di sicurezza/ES.5
aws-foundational-security-best-Pratiche/v/1.0.0/ES.6	Controllo di sicurezza/ES.6
aws-foundational-security-best-Pratiche/v/1.0.0/ES.7	Controllo di sicurezza/ES.7
aws-foundational-security-best-Pratiche/v/1.0.0/ES.8	Controllo di sicurezza/ES.8
aws-foundational-security-best-pratiche/v/1.0.0/.1 GuardDuty	controllo di sicurezza/.1 GuardDuty
aws-foundational-security-best-Pratiche/v/1.0.0/IAM.1	Controllo di sicurezza/IAM.1
aws-foundational-security-best-Pratiche/v/1.0.0/IAM.2	Controllo di sicurezza/IAM.2
aws-foundational-security-best-Pratiche/v/1.0.0/IAM.21	Controllo di sicurezza/IAM.21
aws-foundational-security-best-Pratiche/v/1.0.0/IAM.3	Controllo di sicurezza/IAM.3
aws-foundational-security-best-Pratiche/v/1.0.0/IAM.4	Controllo di sicurezza/IAM.4
aws-foundational-security-best-Pratiche/v/1.0.0/IAM.5	Controllo di sicurezza/IAM.5

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-Pratiche/v/1.0.0/IAM.6	Controllo di sicurezza/IAM.6
aws-foundational-security-best-Pratiche/v/1.0.0/IAM.7	Controllo di sicurezza/IAM.7
aws-foundational-security-best-Pratiche/v/1.0.0/IAM.8	Controllo di sicurezza/IAM.8
aws-foundational-security-best-Pratiche/v/1.0.0/Kinesis.1	Controllo di sicurezza/Kinesis.1
aws-foundational-security-best-Esercitazioni/v/1.0.0/KMS.1	Controllo di sicurezza/KMS.1
aws-foundational-security-best-Pratiche/v/1.0.0/KMS.2	Controllo di sicurezza/KMS.2
aws-foundational-security-best-Pratiche/v/1.0.0/KMS.3	Controllo di sicurezza/KMS.3
aws-foundational-security-best-Pratiche/V/1.0.0/Lambda.1	Controllo di sicurezza/LambdaA.1
aws-foundational-security-best-Pratiche/V/1.0.0/Lambda.2	Controllo di sicurezza/LambdaA.2
aws-foundational-security-best-Pratiche/V/1.0.0/Lambda.5	Controllo di sicurezza/LambdaA.5
aws-foundational-security-best-pratiche/v/1.0.0/.3 NetworkFirewall	controllo di sicurezza/.3 NetworkFirewall
aws-foundational-security-best-pratiche/v/1.0.0/.4 NetworkFirewall	controllo di sicurezza/.4 NetworkFirewall

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-pratiche/v/1.0.0/ .5 NetworkFirewall	controllo di sicurezza/ .5NetworkFirewall.
aws-foundational-security-best-pratiche/v/1.0.0/ .6 NetworkFirewall	controllo di sicurezza/ .6NetworkFirewall.
aws-foundational-security-best-Practices/v/1.0.0/openSearch.1	Security-Control/OpenSearch.1
aws-foundational-security-best-Practices/v/1.0.0/OpenSearch.2	Security-Control/OpenSearch.2
aws-foundational-security-best-Practices/v/1.0.0/OpenSearch.3	Security-Control/OpenSearch.3
aws-foundational-security-best-Practices/v/1.0.0/OpenSearch.4	Security-Control/OpenSearch.4
aws-foundational-security-best-Practices/v/1.0.0/OpenSearch.5	Security-Control/OpenSearch.5
aws-foundational-security-best-Practices/v/1.0.0/OpenSearch.6	Security-Control/OpenSearch.6
aws-foundational-security-best-Pratiche/v/1.0.0/ OpenSearch.7	Security-Control/OpenSearch.7
aws-foundational-security-best-Practices/v/1.0.0/OpenSearch.8	Security-Control/OpenSearch.8
aws-foundational-security-best-Pratiche/v/1.0.0/ RDS.1	Controllo di sicurezza/RDS.1
aws-foundational-security-best-Pratiche/v/1.0.0/ RDS.10	Controllo di sicurezza/RDS.10

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.11	Controllo di sicurezza/RDS.11
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.12	Controllo di sicurezza/RDS.12
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.13	Controllo di sicurezza/RDS.13
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.14	Controllo di sicurezza/RDS.14
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.15	Controllo di sicurezza/RDS.15
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.16	Controllo di sicurezza/RDS.16
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.17	Controllo di sicurezza/RDS.17
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.18	Controllo di sicurezza/RDS.18
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.19	Controllo di sicurezza/RDS.19
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.2	Controllo di sicurezza/RDS.2
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.20	Controllo di sicurezza/RDS.20
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.21	Controllo di sicurezza/RDS.21

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.22	Controllo di sicurezza/RDS.22
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.23	Controllo di sicurezza/RDS.23
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.24	Controllo di sicurezza/RDS.24
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.25	Controllo di sicurezza/RDS.25
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.3	Controllo di sicurezza/RDS.3
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.4	Controllo di sicurezza/RDS.4
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.5	Controllo di sicurezza/RDS.5
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.6	Controllo di sicurezza/RDS.6
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.7	Controllo di sicurezza/RDS.7
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.8	Controllo di sicurezza/RDS.8
aws-foundational-security-best-Pratiche/v/1.0.0/RDS.9	Controllo di sicurezza/RDS.9
aws-foundational-security-best-Pratiche/V/1.0.0/RedShift.1	Controllo di sicurezza/redshift.1

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-Pratiche/V/1.0.0/RedShift.2	Controllo di sicurezza/redshift.2
aws-foundational-security-best-Pratiche/V/1.0.0/RedShift.3	Controllo di sicurezza/redshift.3
aws-foundational-security-best-Pratiche/V/1.0.0/RedShift.4	Controllo di sicurezza/redshift.4
aws-foundational-security-best-Pratiche/V/1.0.0/RedShift.6	Controllo di sicurezza/redshift.6
aws-foundational-security-best-Pratiche/V/1.0.0/RedShift.7	Controllo di sicurezza/redshift.7
aws-foundational-security-best-Pratiche/V/1.0.0/RedShift.8	Controllo di sicurezza/redshift.8
aws-foundational-security-best-Pratiche/v/1.0.0/redshift.9	Controllo di sicurezza/redshift.9
aws-foundational-security-best-Pratiche/v/1.0.0/s3.1	Controlli di sicurezza/s3.1
aws-foundational-security-best-Pratiche/v/1.0.0/S3.12	Controlli di sicurezza/s3.12
aws-foundational-security-best-Pratiche/v/1.0.0/S3.13	Controlli di sicurezza/s3.13
aws-foundational-security-best-Pratiche/v/1.0.0/s3.2	Controlli di sicurezza/s3.2
aws-foundational-security-best-Pratiche/v/1.0.0/S3.3	Controlli di sicurezza/s3.3

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-Pratiche/v/1.0.0/s3.5	Controlli di sicurezza/s3.5
aws-foundational-security-best-Pratiche/v/1.0.0/S3.6	Controllo di sicurezza/s3.6
aws-foundational-security-best-Pratiche/v/1.0.0/s3.8	Controlli di sicurezza/s3.8
aws-foundational-security-best-Pratiche/v/1.0.0/s3.9	Controlli di sicurezza/s3.9
aws-foundational-security-best-pratiche/v/1.0.0/.1 SageMaker	controllo di sicurezza/.1 SageMaker
aws-foundational-security-best-pratiche/v/1.0.0/.2 SageMaker	controllo di sicurezza/.2 SageMaker
aws-foundational-security-best-pratiche/v/1.0.0/.3 SageMaker	controllo di sicurezza/.3 SageMaker
aws-foundational-security-best-pratiche/v/1.0.0/.1 SecretsManager	controllo di sicurezza/.1 SecretsManager
aws-foundational-security-best-pratiche/v/1.0.0/.2 SecretsManager	controllo di sicurezza/.2 SecretsManager
aws-foundational-security-best-pratiche/v/1.0.0/.3 SecretsManager	controllo di sicurezza/.3 SecretsManager
aws-foundational-security-best-pratiche/v/1.0.0/.4 SecretsManager	controllo di sicurezza/.4 SecretsManager
aws-foundational-security-best-Pratiche/v/1.0.0/sqs.1	Controllo di sicurezza/SQS.1

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
aws-foundational-security-best-Pratiche/v/1.0.0/SSM.1	Controllo di sicurezza/SSM.1
aws-foundational-security-best-Pratiche/v/1.0.0/SSM.2	Controllo di sicurezza/SSM.2
aws-foundational-security-best-Pratiche/v/1.0.0/SSM.3	Controllo di sicurezza/SSM.3
aws-foundational-security-best-Pratiche/v/1.0.0/SSM.4	Controllo di sicurezza/SSM.4
aws-foundational-security-best-Pratiche/v/1.0.0/WAF.1	Controllo di sicurezza/WAF.1
aws-foundational-security-best-Pratiche/v/1.0.0/WAF.2	Controllo di sicurezza/WAF.2
aws-foundational-security-best-Pratiche/v/1.0.0/WAF.3	Controllo di sicurezza/WAF.3
aws-foundational-security-best-Pratiche/v/1.0.0/WAF.4	Controllo di sicurezza/WAF.4
aws-foundational-security-best-Pratiche/v/1.0.0/WAF.6	Controllo di sicurezza/WAF.6
aws-foundational-security-best-Pratiche/v/1.0.0/WAF.7	Controllo di sicurezza/WAF.7
aws-foundational-security-best-Pratiche/v/1.0.0/WAF.8	Controllo di sicurezza/WAF.8
aws-foundational-security-best-Pratiche/v/1.0.0/WAF.10	Controllo di sicurezza/WAF.10
PCI-DSS/V/3.2.1/PCI. AutoScaling1.	controllo di sicurezza/ .1 AutoScaling

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
PCI-DSS/v/3.2.1/PCI.CloudTrail1.	controllo di sicurezza/.2CloudTrail.
PCI-DSS/v/3.2.1/PCI.CloudTrail2.	controllo di sicurezza/.3 CloudTrail
PCI-DSS/v/3.2.1/PCI.CloudTrail3.	controllo di sicurezza/.4 CloudTrail
PCI-DSS/v/3.2.1/PCI.CloudTrail4.	controllo di sicurezza/.5 CloudTrail
PCI-DSS/v/3.2.1/PCI.CodeBuild1.	controllo di sicurezza/.1 CodeBuild
PCI-DSS/v/3.2.1/PCI.CodeBuild2.	controllo di sicurezza/.2CodeBuild.
PCI-DSS/v/3.2.1/pci.config.1	Controllo di sicurezza/config.1
PCI-DSS/v/3.2.1/PCI.CW.1	controllo di sicurezza/ 1. CloudWatch
PCI-DSS/v/3.2.1/PCI.dms.1	Controllo di sicurezza/DMS.1
PCI-DSS/v/3.2.1/PCI.ec2.1	Controllo di sicurezza/EC 2.1
PCI-DSS/v/3.2.1/PCI.ec2.2	Controllo di sicurezza/EC 2.2
PCI-DSS/v/3.2.1/PCI.EC2.4	Controllo di sicurezza/EC 2.12
PCI-DSS/v/3.2.1/PCI.EC2.5	Controllo di sicurezza/EC 2.13
PCI-DSS/v/3.2.1/PCI.EC2.6	Controllo di sicurezza/EC2.6
PCI-DSS/v/3.2.1/PCI.ELB v2.1	Controllo di sicurezza/ELB.1
PCI-DSS/v/3.2.1/PCI.es.1	Controllo di sicurezza/ES.2
PCI-DSS/v/3.2.1/PCI.es.2	Controllo di sicurezza/ES.1
PCI-DSS/v/3.2.1/PCI.GuardDuty1.	controllo di sicurezza/.1 GuardDuty
PCI-DSS/v/3.2.1/PCI.IAM.1	Controllo di sicurezza/IAM.4
PCI-DSS/v/3.2.1/PCI.IAM.2	Controllo di sicurezza/IAM.2

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
PCI-DSS/v/3.2.1/PCI.IAM.3	Controllo di sicurezza/IAM.1
PCI-DSS/v/3.2.1/PCI.IAM.4	Controllo di sicurezza/IAM.6
PCI-DSS/v/3.2.1/PCI.IAM.5	Controllo di sicurezza/IAM.9
PCI-DSS/v/3.2.1/PCI.IAM.6	Controllo di sicurezza/IAM.19
PCI-DSS/v/3.2.1/PCI.IAM.7	Controllo di sicurezza/IAM.8
PCI-DSS/v/3.2.1/PCI.IAM.8	Controllo di sicurezza/IAM.10
PCI-DSS/v/3.2.1/PCI.kms.1	Controllo di sicurezza/KMS.4
PCI-DSS/V/3.2.1/PCI.Lambda.1	Controllo di sicurezza/Lambda.1
PCI-DSS/V/3.2.1/PCI.Lambda.2	Controllo di sicurezza/Lambda.3
PCI-DSS/V/3.2.1/pci.OpenSearch.1	Security-Control/OpenSearch.2
PCI-DSS/v/3.2.1/pci.openSearch.2	Security-Control/OpenSearch.1
PCI-DSS/v/3.2.1/PCI.RDS.1	Controllo di sicurezza/RDS.1
PCI-DSS/v/3.2.1/PCI.RDS.2	Controllo di sicurezza/RDS.2
PCI-DSS/v/3.2.1/pci.RedShift.1	Controllo di sicurezza/redshift.1
PCI-DSS/v/3.2.1/PCI.s3.1	Controlli di sicurezza/S3.3
PCI-DSS/v/3.2.1/PCI.s3.2	Controlli di sicurezza/s3.2
PCI-DSS/v/3.2.1/PCI.S3.3	Controllo di sicurezza/s3.7
PCI-DSS/v/3.2.1/PCI.s3.5	Controlli di sicurezza/s3.5
PCI-DSS/v/3.2.1/PCI.s3.6	Controlli di sicurezza/s3.1
PCI-DSS/V/3.2.1/PCI. SageMaker1.	controllo di sicurezza/ .1 SageMaker

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
PCI-DSS/v/3.2.1/PCI.ssm.1	Controllo di sicurezza/SSM.2
PCI-DSS/v/3.2.1/PCI.ssm.2	Controllo di sicurezza/SSM.3
PCI-DSS/v/3.2.1/PCI.ssm.3	Controllo di sicurezza/SSM.1
service-managed-aws-control-Torre/v/1.0.0/ACM.1	Controllo di sicurezza/ACM.1
service-managed-aws-control-Tower/v/1.0.0/APIGateway.1	Controllo di sicurezza/API Gateway.1
service-managed-aws-control-Torre/v/1.0.0/API Gateway.2	Controllo di sicurezza/API Gateway.2
service-managed-aws-control-Torre/v/1.0.0/API Gateway.3	Controllo di sicurezza/API Gateway.3
service-managed-aws-control-Torre/v/1.0.0/API Gateway.4	Controllo di sicurezza/API Gateway.4
service-managed-aws-control-Torre/v/1.0.0/API Gateway.5	Controllo di sicurezza/API Gateway.5
service-managed-aws-control-torre/v/1.0.0/ .1 AutoScaling	controllo di sicurezza/ .1 AutoScaling
service-managed-aws-control-torre/v/1.0.0/ .2 AutoScaling	controllo di sicurezza/ .2 AutoScaling
service-managed-aws-control-torre/v/1.0.0/ .3 AutoScaling	controllo di sicurezza/ .3 AutoScaling
service-managed-aws-control-torre/v/1.0.0/ .4 AutoScaling	controllo di sicurezza/ .4 AutoScaling

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-Tower/v/1.0.0/ AutoScaling.5	Controllo di sicurezza/scalabilità automatica. 5
service-managed-aws-control-torre/v/1.0.0/ .6 AutoScaling	controllo di sicurezza/ .6 AutoScaling
service-managed-aws-control-torre/v/1.0.0/ .9 AutoScaling	controllo di sicurezza/ .9 AutoScaling
service-managed-aws-control-torre/v/1.0.0/ .1 CloudTrail	controllo di sicurezza/ .1 CloudTrail
service-managed-aws-control-torre/v/1.0.0/ .2 CloudTrail	controllo di sicurezza/ .2 CloudTrail
service-managed-aws-control-torre/v/1.0.0/ .4 CloudTrail	controllo di sicurezza/ .4 CloudTrail
service-managed-aws-control-torre/v/1.0.0/ .5 CloudTrail	controllo di sicurezza/ .5 CloudTrail
service-managed-aws-control-torre/v/1.0.0/ .1 CodeBuild	controllo di sicurezza/ .1 CodeBuild
service-managed-aws-control-torre/v/1.0.0/ .2 CodeBuild	controllo di sicurezza/ .2 CodeBuild
service-managed-aws-control-torre/v/1.0.0/ .4 CodeBuild	controllo di sicurezza/ .4 CodeBuild
service-managed-aws-control-torre/v/1.0.0/ .5 CodeBuild	controllo di sicurezza/ .5 CodeBuild
service-managed-aws-control-Torre/v/1.0.0/ DMS.1	Controllo di sicurezza/DMS.1

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-Torre/V/1.0.0/DynamoDB.1	Controllo della sicurezza/DynamoDB.1
service-managed-aws-control-Torre/V/1.0.0/DynamoDB.2	Controllo della sicurezza/DynamoDB.2
service-managed-aws-control-Torre/V/1.0.0/EC2.1	Controllo di sicurezza/EC2.1
service-managed-aws-control-Torre/V/1.0.0/EC2.2	Controllo di sicurezza/EC2.2
service-managed-aws-control-Torre/V/1.0.0/EC2.3	Controllo di sicurezza/EC2.3
service-managed-aws-control-Torre/V/1.0.0/EC2.4	Controllo di sicurezza/EC2.4
service-managed-aws-control-Torre/V/1.0.0/EC2.6	Controllo di sicurezza/EC2.6
service-managed-aws-control-Torre/V/1.0.0/EC2.7	Controllo di sicurezza/EC2.7
service-managed-aws-control-Torre/V/1.0.0/EC2.8	Controllo di sicurezza/EC2.8
service-managed-aws-control-Torre/V/1.0.0/EC2.9	Controllo di sicurezza/EC2.9
service-managed-aws-control-Torre/V/1.0.0/EC2.10	Controllo di sicurezza/EC2.10
service-managed-aws-control-Torre/V/1.0.0/EC2.15	Controllo di sicurezza/EC2.15

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-Torre/V/1.0.0/EC2.16	Controllo di sicurezza/EC2.16
service-managed-aws-control-Torre/V/1.0.0/EC2.17	Controllo di sicurezza/EC2.17
service-managed-aws-control-Torre/V/1.0.0/EC2.18	Controllo di sicurezza/EC2.18
service-managed-aws-control-Torre/V/1.0.0/EC2.19	Controllo di sicurezza/EC2.19
service-managed-aws-control-Torre/V/1.0.0/EC2.20	Controllo di sicurezza/EC2.20
service-managed-aws-control-Torre/V/1.0.0/EC2.21	Controllo di sicurezza/EC2.21
service-managed-aws-control-Torre/V/1.0.0/EC2.22	Controllo di sicurezza/EC2.22
service-managed-aws-control-Torre/V/1.0.0/ECR.1	Controllo di sicurezza/ECR.1
service-managed-aws-control-Torre/V/1.0.0/ECR.2	Controllo di sicurezza/ECR.2
service-managed-aws-control-Torre/V/1.0.0/ECR.3	Controllo di sicurezza/ECR.3
service-managed-aws-control-Torre/V/1.0.0/ECS.1	Controllo di sicurezza/ECS.1
service-managed-aws-control-Torre/V/1.0.0/ECS.2	Controllo di sicurezza/ECS.2

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-Torre/V/1.0.0/ECS.3	Controllo di sicurezza/ECS.3
service-managed-aws-control-Torre/V/1.0.0/ECS.4	Controllo di sicurezza/ECS.4
service-managed-aws-control-Torre/V/1.0.0/ECS.5	Controllo di sicurezza/ECS.5
service-managed-aws-control-Torre/V/1.0.0/ECS.8	Controllo di sicurezza/ECS.8
service-managed-aws-control-Torre/V/1.0.0/ECS.10	Controllo di sicurezza/ECS.10
service-managed-aws-control-Torre/V/1.0.0/ECS.12	Controllo di sicurezza/ECS.12
service-managed-aws-control-Torre/V/1.0.0/EFS.1	Controllo di sicurezza/EFS.1
service-managed-aws-control-Torre/V/1.0.0/EFS.2	Controllo di sicurezza/EFS.2
service-managed-aws-control-Torre/V/1.0.0/EFS.3	Controllo di sicurezza/EFS.3
service-managed-aws-control-Torre/V/1.0.0/EFS.4	Controllo di sicurezza/EFS.4
service-managed-aws-control-Torre/V/1.0.0/EKS.2	Controllo di sicurezza/EKS.2
service-managed-aws-control-Torre/V/1.0.0/ELB.2	Controllo di sicurezza/ELB.2

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-Torre/V/1.0.0/ELB.3	Controllo di sicurezza/ELB.3
service-managed-aws-control-Torre/V/1.0.0/ELB.4	Controllo di sicurezza/ELB.4
service-managed-aws-control-Torre/V/1.0.0/ELB.5	Controllo di sicurezza/ELB.5
service-managed-aws-control-Torre/V/1.0.0/ELB.6	Controllo di sicurezza/ELB.6
service-managed-aws-control-Torre/V/1.0.0/ELB.7	Controllo di sicurezza/ELB.7
service-managed-aws-control-Torre/V/1.0.0/ELB.8	Controllo di sicurezza/ELB.8
service-managed-aws-control-Torre/V/1.0.0/ELB.9	Controllo di sicurezza/ELB.9
service-managed-aws-control-Torre/V/1.0.0/ELB.10	Controllo di sicurezza/ELB.10
service-managed-aws-control-Torre/V/1.0.0/ELB.12	Controllo di sicurezza/ELB.12
service-managed-aws-control-Torre/V/1.0.0/ELB.13	Controllo di sicurezza/ELB.13
service-managed-aws-control-Torre/V/1.0.0/ELB.14	Controllo di sicurezza/ELB.14
service-managed-aws-control-Torre/V/1.0.0/ELBV2.1	Controllo di sicurezza/ELBV2.1

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-Torre/v/1.0.0/EMR.1	Controllo di sicurezza/EMR.1
service-managed-aws-control-Torre/v/1.0.0/ES.1	Controllo di sicurezza/ES.1
service-managed-aws-control-Torre/v/1.0.0/ES.2	Controllo di sicurezza/ES.2
service-managed-aws-control-Torre/v/1.0.0/ES.3	Controllo di sicurezza/ES.3
service-managed-aws-control-Torre/v/1.0.0/ES.4	Controllo di sicurezza/ES.4
service-managed-aws-control-Torre/v/1.0.0/ES.5	Controllo di sicurezza/ES.5
service-managed-aws-control-Torre/v/1.0.0/ES.6	Controllo di sicurezza/ES.6
service-managed-aws-control-Torre/v/1.0.0/ES.7	Controllo di sicurezza/ES.7
service-managed-aws-control-Torre/v/1.0.0/ES.8	Controllo di sicurezza/ES.8
service-managed-aws-control-torre/v/1.0.0/ .1 ElasticBeanstalk	controllo di sicurezza/ .1 ElasticBeanstalk
service-managed-aws-control-torre/v/1.0.0/ .2 ElasticBeanstalk	controllo di sicurezza/ .2 ElasticBeanstalk
service-managed-aws-control-torre/v/1.0.0/ .1 GuardDuty	controllo di sicurezza/ .1 GuardDuty

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-torre/v/1.0.0/IAM.1	Controllo di sicurezza/IAM.1
service-managed-aws-control-Torre/v/1.0.0/IAM.2	Controllo di sicurezza/IAM.2
service-managed-aws-control-Torre/v/1.0.0/IAM.3	Controllo di sicurezza/IAM.3
service-managed-aws-control-Torre/v/1.0.0/IAM.4	Controllo di sicurezza/IAM.4
service-managed-aws-control-Torre/v/1.0.0/IAM.5	Controllo di sicurezza/IAM.5
service-managed-aws-control-Torre/v/1.0.0/IAM.6	Controllo di sicurezza/IAM.6
service-managed-aws-control-Torre/v/1.0.0/IAM.7	Controllo di sicurezza/IAM.7
service-managed-aws-control-Torre/v/1.0.0/IAM.8	Controllo di sicurezza/IAM.8
service-managed-aws-control-Torre/v/1.0.0/IAM.21	Controllo di sicurezza/IAM.21
service-managed-aws-control-Torre/V/1.0.0/Kinesis.1	Controllo di sicurezza/Kinesis.1
service-managed-aws-control-Torre/V/1.0.0/kms.1	Controllo di sicurezza/KMS.1
service-managed-aws-control-Torre/V/1.0.0/kms.2	Controllo di sicurezza/KMS.2

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-Torre/v/1.0.0/kms.3	Controllo di sicurezza/KMS.3
service-managed-aws-control-Torre/v/1.0.0/lambda.1	Controllo di sicurezza/Lambda.1
service-managed-aws-control-Torre/v/1.0.0/lambda.2	Controllo di sicurezza/Lambda.2
service-managed-aws-control-Torre/v/1.0.0/lambda.5	Controllo di sicurezza/Lambda.5
service-managed-aws-control-torre/v/1.0.0/.3 NetworkFirewall	controllo di sicurezza/.3 NetworkFirewall
service-managed-aws-control-torre/v/1.0.0/.4 NetworkFirewall	controllo di sicurezza/.4 NetworkFirewall
service-managed-aws-control-torre/v/1.0.0/.5 NetworkFirewall	controllo di sicurezza/.5 NetworkFirewall
service-managed-aws-control-torre/v/1.0.0/.6 NetworkFirewall	controllo di sicurezza/.6NetworkFirewall.
service-managed-aws-control-torre/v/1.0.0/openSearch.1	Security-Control/OpenSearch.1
service-managed-aws-control-Torre/v/1.0.0/openSearch.2	Security-Control/OpenSearch.2
service-managed-aws-control-Torre/v/1.0.0/OpenSearch.3	Security-Control/OpenSearch.3
service-managed-aws-control-Torre/v/1.0.0/OpenSearch.4	Security-Control/OpenSearch.4

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-Torre/v/1.0.0/OpenSearch.5	Security-Control/OpenSearch.5
service-managed-aws-control-Torre/v/1.0.0/OpenSearch.6	Security-Control/OpenSearch.6
service-managed-aws-control-Torre/v/1.0.0/OpenSearch.7	Security-Control/OpenSearch.7
service-managed-aws-control-Torre/v/1.0.0/OpenSearch.8	Security-Control/OpenSearch.8
service-managed-aws-control-Torre/v/1.0.0/RDS.1	Controllo di sicurezza/RDS.1
service-managed-aws-control-Torre/V/1.0.0/RDS.2	Controllo di sicurezza/RDS.2
service-managed-aws-control-Torre/V/1.0.0/RDS.3	Controllo di sicurezza/RDS.3
service-managed-aws-control-Torre/V/1.0.0/RDS.4	Controllo di sicurezza/RDS.4
service-managed-aws-control-Torre/V/1.0.0/RDS.5	Controllo di sicurezza/RDS.5
service-managed-aws-control-Torre/V/1.0.0/RDS.6	Controllo di sicurezza/RDS.6
service-managed-aws-control-Torre/V/1.0.0/RDS.8	Controllo di sicurezza/RDS.8
service-managed-aws-control-Torre/V/1.0.0/RDS.9	Controllo di sicurezza/RDS.9

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-Torre/v/1.0.0/RDS.10	Controllo di sicurezza/RDS.10
service-managed-aws-control-Torre/V/1.0.0/RDS.11	Controllo di sicurezza/RDS.11
service-managed-aws-control-Torre/v/1.0.0/RDS.13	Controllo di sicurezza/RDS.13
service-managed-aws-control-Torre/V/1.0.0/RDS.17	Controllo di sicurezza/RDS.17
service-managed-aws-control-Torre/v/1.0.0/RDS.18	Controllo di sicurezza/RDS.18
service-managed-aws-control-Torre/v/1.0.0/RDS.19	Controllo di sicurezza/RDS.19
service-managed-aws-control-Torre/V/1.0.0/RDS.20	Controllo di sicurezza/RDS.20
service-managed-aws-control-Torre/V/1.0.0/RDS.21	Controllo di sicurezza/RDS.21
service-managed-aws-control-Torre/V/1.0.0/RDS.22	Controllo di sicurezza/RDS.22
service-managed-aws-control-Torre/V/1.0.0/RDS.23	Controllo di sicurezza/RDS.23
service-managed-aws-control-Torre/V/1.0.0/RDS.25	Controllo di sicurezza/RDS.25
service-managed-aws-control-Torre/V/1.0.0/redshift.1	Controllo di sicurezza/redshift.1

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-Torre/V/1.0.0/redshift.2	Controllo di sicurezza/redshift.2
service-managed-aws-control-Torre/V/1.0.0/redshift.4	Controllo di sicurezza/redshift.4
service-managed-aws-control-Torre/V/1.0.0/RedShift.6	Controllo di sicurezza/redshift.6
service-managed-aws-control-Torre/V/1.0.0/redshift.7	Controllo di sicurezza/redshift.7
service-managed-aws-control-Torre/V/1.0.0/redshift.8	Controllo di sicurezza/redshift.8
service-managed-aws-control-Torre/V/1.0.0/redshift.9	Controllo di sicurezza/redshift.9
service-managed-aws-control-Torre/v/1.0.0/s3.1	Controlli di sicurezza/s3.1
service-managed-aws-control-Torre/v/1.0.0/s3.2	Controlli di sicurezza/s3.2
service-managed-aws-control-Torre/v/1.0.0/S3.3	Controlli di sicurezza/s3.3
service-managed-aws-control-Torre/v/1.0.0/s3.5	Controlli di sicurezza/s3.5
service-managed-aws-control-Torre/v/1.0.0/S3.6	Controllo di sicurezza/s3.6
service-managed-aws-control-Torre/v/1.0.0/s3.8	Controllo di sicurezza/s3.8

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-Torre/v/1.0.0/s3.9	Controllo di sicurezza/s3.9
service-managed-aws-control-Torre/v/1.0.0/S3.12	Controllo di sicurezza/S3.12
service-managed-aws-control-Torre/v/1.0.0/S3.13	Controllo di sicurezza/S3.13
service-managed-aws-control-torre/v/1.0.0/ .1 SageMaker	controllo di sicurezza/ .1 SageMaker
service-managed-aws-control-torre/v/1.0.0/ .1 SecretsManager	controllo di sicurezza/ .1 SecretsManager
service-managed-aws-control-torre/v/1.0.0/ .2 SecretsManager	controllo di sicurezza/ .2 SecretsManager
service-managed-aws-control-torre/v/1.0.0/ .3 SecretsManager	controllo di sicurezza/ .3 SecretsManager
service-managed-aws-control-torre/v/1.0.0/ .4 SecretsManager	controllo di sicurezza/ .4 SecretsManager
service-managed-aws-control-Torre/V/1.0.0/sq.1	Controllo di sicurezza/SQS.1
service-managed-aws-control-Torre/V/1.0.0/SSM.1	Controllo di sicurezza/SSM.1
service-managed-aws-control-Torre/V/1.0.0/SSM.2	Controllo di sicurezza/SSM.2
service-managed-aws-control-Torre/V/1.0.0/SSM.3	Controllo di sicurezza/SSM.3

GeneratorID prima di attivare i risultati del controllo consolidato	GeneratorID dopo aver attivato i risultati del controllo consolidato
service-managed-aws-control-Torre/V/1.0.0/SSM.4	Controllo di sicurezza/SSM.4
service-managed-aws-control-Torre/V/1.0.0/WAF.2	Controllo di sicurezza/WAF.2
service-managed-aws-control-Torre/V/1.0.0/WAF.3	Controllo di sicurezza/WAF.3
service-managed-aws-control-Torre/V/1.0.0/WAF.4	Controllo di sicurezza/WAF.4

In che modo il consolidamento influisce sugli ID e sui titoli di controllo

Controlli consolidati La visualizzazione e i risultati di controllo consolidati standardizzano gli ID e i titoli di controllo in tutti gli standard. I termini Security Control ID e Security Control Title si riferiscono a questi valori indipendenti dallo standard. La tabella seguente mostra la mappatura degli ID e dei titoli dei controlli di sicurezza agli ID e ai titoli di controllo specifici dello standard. Gli ID e i titoli dei controlli che appartengono allo standard AWS Foundational Security Best Practices (FSBP) sono rimasti invariati.

La console Security Hub mostra gli ID e i titoli dei controlli di sicurezza, indipendentemente dal fatto che i risultati del controllo consolidato siano attivati o disattivati nel tuo account. Tuttavia, i risultati di Security Hub contengono ID di controllo di sicurezza e titoli di controllo di sicurezza solo se i risultati del controllo consolidato sono attivati nel tuo account. Se i risultati del controllo consolidato sono disattivati nel tuo account, i risultati di Security Hub contengono ID e titoli di controllo specifici dello standard. Per ulteriori informazioni sull'impatto del consolidamento sui risultati del controllo, consulta.

[Esempi di risultati del controllo](#)

Per i controlli che fanno parte di [Service-Managed Standard: AWS Control Tower](#), il prefisso CT . viene rimosso dall'ID e dal titolo del controllo nei risultati quando i risultati del controllo consolidato sono attivati.

Per eseguire i tuoi script su questa tabella, [scaricala](#) come file.csv.

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.2.0	1.1 Evita l'uso dell'utente root	[CloudWatch.1] Dovrebbero esistere un filtro logmetrico e un allarme per l'utilizzo da parte dell'utente «root»
CIS versione 1.2.0	1.10 Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password	[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
CIS versione 1.2.0	1.11 Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno	[IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno
CIS versione 1.2.0	1.12 Assicurati che non esista alcuna chiave di accesso per l'utente root	[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
CIS versione 1.2.0	1.13 Assicurarsi che l'MFA sia abilitata per l'utente root	[IAM.9] L'MFA deve essere abilitata per l'utente root
CIS versione 1.2.0	1.14 Assicurarsi che l'MFA hardware sia abilitato per l'utente root	[IAM.6] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root
CIS versione 1.2.0	1.16 Assicurati che le policy IAM siano collegate solo a gruppi o ruoli	[IAM.2] Gli utenti IAM non devono avere policy IAM allegate
CIS versione 1.2.0	1.2 Assicurati che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti IAM che dispongono di una password di console	[IAM.5] MFA deve essere abilitata per tutti gli utenti IAM che dispongono o di una password della console
CIS versione 1.2.0	1.20 Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support	[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support
CIS versione 1.2.0	1.22 Assicurati che non vengano create politiche IAM che consentano privilegi amministrativi completi «*: *»	[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.2.0	1.3 Assicurati che le credenziali non utilizzate per 90 giorni o più siano disabilitate	[IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
CIS versione 1.2.0	1.4 Assicurati che le chiavi di accesso vengano ruotate ogni 90 giorni o meno	[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
CIS versione 1.2.0	1.5 Assicurati che la politica delle password di IAM richieda almeno una lettera maiuscola	[IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola
CIS versione 1.2.0	1.6 Assicurati che la politica delle password di IAM richieda almeno una lettera minuscola	[IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola
CIS versione 1.2.0	1.7 Assicurati che la politica delle password IAM richieda almeno un simbolo	[IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo
CIS versione 1.2.0	1.8 Assicurati che la politica delle password IAM richieda almeno un numero	[IAM.14] Assicurati che la politica delle password IAM richieda almeno un numero
CIS versione 1.2.0	1.9 Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14	[IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
CIS versione 1.2.0	2.1 Ensure CloudTrail è abilitato in tutte le regioni	[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura
CIS versione 1.2.0	2.2 Assicurarsi che la convalida dei file di CloudTrail registro sia abilitata	[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.2.0	2.3 Assicurati che il bucket S3 utilizzato per archiviare CloudTrail i log non sia accessibile al pubblico	[CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i log non sia accessibile al pubblico CloudTrail
CIS versione 1.2.0	2.4 Assicurati che i CloudTrail percorsi siano integrati con i log CloudWatch	[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch
CIS versione 1.2.0	2.5 Assicurati che AWS Config sia abilitato	[Config.1] AWS Config dovrebbe essere abilitato
CIS versione 1.2.0	2.6 Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail	[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail
CIS versione 1.2.0	2.7 Assicurati che i CloudTrail log siano crittografati quando sono inattivi utilizzando le CMK KMS	[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata
CIS versione 1.2.0	2.8 Assicurati che la rotazione per le CMK create dal cliente sia abilitata	[KMS.4] la rotazione dei tasti dovrebbe essere abilitata AWS KMS
CIS versione 1.2.0	2.9 Assicurati che la registrazione del flusso VPC sia abilitata in tutti i VPC	[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC
CIS versione 1.2.0	3.1 Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate	[CloudWatch.2] Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate
CIS versione 1.2.0	3.10 Assicurarsi che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza	[CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.2.0	3.11 Assicurarsi che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)	[CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)
CIS versione 1.2.0	3.12 Assicurarsi che esistano un filtro metrico di registro e un allarme per le modifiche ai gateway di rete	[CloudWatch.12] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche ai gateway di rete
CIS versione 1.2.0	3.13 Assicurarsi che esistano un filtro metrico di log e un allarme per le modifiche alla tabella di percorso	[CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte
CIS versione 1.2.0	3.14 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche al VPC	[CloudWatch.14] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche al VPC
CIS versione 1.2.0	3.2 Assicurarsi che esistano un filtro metrico di registro e un allarme per l'accesso alla Console di gestione senza MFA	[CloudWatch.3] Assicurarsi che esistano un filtro metrico di registro e un allarme per l'accesso alla Console di gestione senza MFA
CIS versione 1.2.0	3.3 Assicurarsi che esistano un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente root	[CloudWatch.1] Dovrebbero esistere un filtro logmetrico e un allarme per l'utilizzo da parte dell'utente «root»
CIS versione 1.2.0	3.4 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle politiche IAM	[CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.2.0	3.5 Assicurati che esistano un filtro metrico di registro e un allarme per le CloudTrail modifiche alla configurazione	[CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le CloudTrail AWS Config variazioni di durata
CIS versione 1.2.0	3.6 Assicurati che esistano un filtro metrico di registro e un allarme per gli errori di autenticazione AWS Management Console	[CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per gli AWS Management Console errori di autenticazione
CIS versione 1.2.0	3.7 Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione pianificata delle CMK create dal cliente	[CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione programmata delle chiavi gestite dal cliente
CIS versione 1.2.0	3.8 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy relative ai bucket S3	[CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3
CIS versione 1.2.0	3.9 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla configurazione AWS Config	[CloudWatch.9] Assicurati che esistano un filtro metrico di log e un allarme per le AWS Config modifiche alla configurazione
CIS versione 1.2.0	4.1 Assicurarsi che nessun gruppo di sicurezza consenta l'ingresso dalla porta 0.0.0.0/0 alla porta 22	[EC2.13] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22
CIS versione 1.2.0	4.2 Assicurarsi che nessun gruppo di sicurezza consenta l'ingresso dalla porta 0.0.0.0/0 alla porta 3389	[EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS versione 1.2.0	4.3 Assicurati che il gruppo di sicurezza predefinito di ogni VPC limiti tutto il traffico	[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita
CIS v1.4.0	1.10 Assicurati che l'autenticazione a più fattori (MFA) sia abilitata per tutti gli utenti IAM che dispongono di una password di console	[IAM.5] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console
CIS v1.4.0	1.14 Assicurati che le chiavi di accesso vengano ruotate ogni 90 giorni o meno	[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno
CIS v1.4.0	1.16 Assicurati che le politiche IAM che consentono i privilegi amministrativi «*: *» completi non siano allegare	[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
CIS v1.4.0	1.17 Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support	[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support
CIS v1.4.0	1.4 Assicurati che non esista alcuna chiave di accesso all'account utente root	[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
CIS v1.4.0	1.5 Assicurati che l'MFA sia abilitata per l'account utente root	[IAM.9] L'MFA deve essere abilitata per l'utente root
CIS v1.4.0	1.6 Assicurarsi che l'MFA hardware sia abilitata per l'account utente root	[IAM.6] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root
CIS v1.4.0	1.7 Eliminare l'uso dell'utente root per le attività amministrative e quotidiane	[CloudWatch.1] Dovrebbero esistere un filtro logmetrico e un allarme per l'utilizzo da parte dell'utente «root»

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS v1.4.0	1.8 Assicurati che la politica delle password IAM richieda una lunghezza minima di 14 o superiore	[IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14
CIS v1.4.0	1.9 Assicurati che la politica delle password IAM impedisca il riutilizzo delle password	[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password
CIS v1.4.0	2.1.2 Assicurati che S3 Bucket Policy sia impostata per negare le richieste HTTP	[S3.5] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL
CIS v1.4.0	2.1.5.1 L'impostazione S3 Block Public Access deve essere abilitata	[S3.1] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate
CIS v1.4.0	2.1.5.2 L'impostazione S3 Block Public Access deve essere abilitata a livello di bucket	[S3.8] I bucket generici S3 dovrebbero o bloccare l'accesso pubblico
CIS v1.4.0	2.2.1 Assicurarsi che la crittografia dei volumi EBS sia abilitata	[EC2.7] La crittografia predefinita di EBS deve essere abilitata
CIS v1.4.0	2.3.1 Assicurarsi che la crittografia sia abilitata per le istanze RDS	[RDS.3] Le istanze database RDS devono avere la crittografia dei dati inattivi abilitata
CIS v1.4.0	3.1 Ensure CloudTrail è abilitato in tutte le regioni	[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura
CIS v1.4.0	3.2 Assicurarsi che la convalida dei file di CloudTrail registro sia abilitata	[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS v1.4.0	3.4 Assicurati che i CloudTrail percorsi siano integrati con i registri CloudWatch	[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch
CIS v1.4.0	3.5 Ensure AWS Config è abilitato in tutte le regioni	[Config.1] AWS Config dovrebbe essere abilitato
CIS v1.4.0	3.6 Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail	[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail
CIS v1.4.0	3.7 Assicurati che i CloudTrail log siano crittografati quando sono inattivi utilizzando le CMK KMS	[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata
CIS v1.4.0	3.8 Assicurati che la rotazione per le CMK create dal cliente sia abilitata	[KMS.4] la rotazione dei tasti dovrebbe essere abilitata AWS KMS
CIS v1.4.0	3.9 Assicurati che la registrazione del flusso VPC sia abilitata in tutti i VPC	[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC
CIS v1.4.0	4.4 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM	[CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM
CIS v1.4.0	4.5 Assicurarsi che esistano un filtro metrico di log e un allarme per le modifiche alla configurazione CloudTrail	[CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le CloudTrail AWS Config variazioni di durata
CIS v1.4.0	4.6 Assicurarsi che esistano un filtro metrico di registro e un allarme per gli errori di autenticazione AWS Management Console	[CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per gli AWS Management Console errori di autenticazione

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS v1.4.0	4.7 Assicurati che esistano un filtro metrico di log e un allarme per la disabilitazione o l'eliminazione pianificata delle CMK create dal cliente	[CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione programmata delle chiavi gestite dal cliente
CIS v1.4.0	4.8 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla policy dei bucket S3	[CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3
CIS v1.4.0	4.9 Assicurarsi che esistano un filtro metrico di log e un allarme per le modifiche alla configurazione AWS Config	[CloudWatch.9] Assicurati che esistano un filtro metrico di log e un allarme per le AWS Config modifiche alla configurazione
CIS v1.4.0	4.10 Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza	[CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza
CIS v1.4.0	4.11 Assicurarsi che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)	[CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)
CIS v1.4.0	4.12 Assicurarsi che esistano un filtro metrico di log e un allarme per le modifiche ai gateway di rete	[CloudWatch.12] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche ai gateway di rete
CIS v1.4.0	4.13 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte	[CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
CIS v1.4.0	4.14 Assicurati che esistano un filtro metrico di log e un allarme per le modifiche al VPC	[CloudWatch.14] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche al VPC
CIS v1.4.0	5.1 Assicurarsi che nessun ACL di rete consenta l'accesso da 0.0.0.0/0 alle porte di amministrazione remota del server	[EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso dalla porta 0.0.0.0/0 alla porta 22 o alla porta 3389
CIS v1.4.0	5.3 Assicurati che il gruppo di sicurezza predefinito di ogni VPC limiti tutto il traffico	[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita
PCI DSS v3.2.1	PCI. AutoScaling.1 I gruppi di scalabilità automatica associati a un sistema di bilanciamento del carico devono utilizzare i controlli dello stato del sistema di bilanciamento del carico	[AutoScaling.1] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB
PCI DSS v3.2.1	PCI. CloudTrail.1 CloudTrail i log devono essere crittografati quando sono inattivi utilizzando CMK AWS KMS	[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata
PCI DSS v3.2.1	PCI. CloudTrail.2 CloudTrail dovrebbe essere abilitato	[CloudTrail.3] Almeno un trail deve essere abilitato CloudTrail
PCI DSS v3.2.1	PCI. CloudTrail.3 la convalida dei file di CloudTrail registro deve essere abilitata	[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata
PCI DSS v3.2.1	PCI. CloudTrail.4 i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch	[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
PCI DSS v3.2.1	PCI. CodeBuild.1 CodeBuild GitHub o gli URL del repository di origine Bitbucket devono utilizzare OAuth	[CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili
PCI DSS v3.2.1	PCI. CodeBuild.2 Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato	[CodeBuild.2] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato
PCI DSS v3.2.1	PCI.config.1 dovrebbe AWS Config essere abilitato	[Config.1] AWS Config dovrebbe essere abilitato
PCI DSS v3.2.1	PCI.CW.1 Dovrebbero esistere un filtro metrico di log e un allarme per l'utilizzo da parte dell'utente «root»	[CloudWatch.1] Dovrebbero esistere un filtro logmetrico e un allarme per l'utilizzo da parte dell'utente «root»
PCI DSS v3.2.1	Le istanze di replica PCI.DMS.1 Database Migration Service non devono essere pubbliche	[DMS.1] Le istanze di replica del Database Migration Service non devono essere pubbliche
PCI DSS v3.2.1	Le istantanee EBS PCI.EC2.1 non devono essere ripristinabili pubblicamente	[EC2.1] Gli snapshot di Amazon EBS non devono essere ripristinabili pubblicamente
PCI DSS v3.2.1	Il gruppo di sicurezza VPC predefinito PCI.EC2.2 dovrebbe vietare il traffico in entrata e in uscita	[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita
PCI DSS v3.2.1	PCI.EC2.4 Gli EIP EC2 non utilizzati devono essere rimossi	[EC2.12] Gli EIP Amazon EC2 non utilizzati devono essere rimossi
PCI DSS v3.2.1	I gruppi di sicurezza PCI.EC2.5 non dovrebbero consentire l'ingresso da 0.0.0.0/0 alla porta 22	[EC2.13] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o :/0 alla porta 22

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
PCI DSS v3.2.1	La registrazione del flusso VPC PCI.EC2.6 deve essere abilitata in tutti i VPC	[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC
PCI DSS v3.2.1	PCI.Elbv2.1 Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS	[ELB.1] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS
PCI DSS v3.2.1	I domini PCI.ES.1 Elasticsearch devono trovarsi in un VPC	[ES.2] I domini Elasticsearch non devono essere accessibili al pubblico
PCI DSS v3.2.1	I domini PCI.ES.2 Elasticsearch devono avere la crittografia a riposo abilitata	[ES.1] I domini Elasticsearch devono avere la crittografia a riposo abilitata
PCI DSS v3.2.1	PCI. GuardDuty.1 GuardDuty dovrebbe essere abilitato	[GuardDuty.1] GuardDuty dovrebbe essere abilitato
PCI DSS v3.2.1	La chiave di accesso utente root PCI.IAM.1 IAM non dovrebbe esistere	[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere
PCI DSS v3.2.1	Gli utenti IAM PCI.IAM.2 non devono avere policy IAM collegate	[IAM.2] Gli utenti IAM non devono avere policy IAM allegate
PCI DSS v3.2.1	Le politiche IAM PCI.IAM.3 non dovrebbero consentire privilegi amministrativi «*» completi	[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi
PCI DSS v3.2.1	L'MFA hardware PCI.IAM.4 deve essere abilitato per l'utente root	[IAM.6] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root
PCI DSS v3.2.1	La MFA virtuale PCI.IAM.5 deve essere abilitata per l'utente root	[IAM.9] L'MFA deve essere abilitata per l'utente root

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
PCI DSS v3.2.1	La MFA PCI.IAM.6 deve essere abilitata per tutti gli utenti IAM	[IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM
PCI DSS v3.2.1	Le credenziali utente IAM PCI.IAM.7 devono essere disabilitate se non utilizzate entro un numero predefinito di giorni	[IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse
PCI DSS v3.2.1	Le politiche di password PCI.IAM.8 per gli utenti IAM devono avere configurazioni avanzate	[IAM.10] Le politiche relative alle password per gli utenti IAM dovrebbero avere durate elevate AWS Config
PCI DSS v3.2.1	La rotazione della chiave principale del cliente (CMK) PCI.KMS.1 deve essere abilitata	[KMS.4] la rotazione dei tasti dovrebbe essere abilitata AWS KMS
PCI DSS v3.2.1	Le funzioni PCI.Lambda.1 Lambda dovrebbero vietare l'accesso pubblico	[Lambda.1] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico
PCI DSS v3.2.1	Le funzioni Lambda PCI.Lambda.2 devono essere in un VPC	[Lambda.3] Le funzioni Lambda devono trovarsi in un VPC
PCI DSS v3.2.1	I domini PCI.openSearch.1 OpenSearch devono trovarsi in un VPC	I OpenSearch domini [Opensearch.2] non devono essere accessibili al pubblico
PCI DSS v3.2.1	Le istantanee EBS PCI.OpenSearch.2 non dovrebbero essere ripristinabili pubblicamente	I OpenSearch domini [Opensearch.1] devono avere la crittografia a riposo abilitata
PCI DSS v3.2.1	Lo snapshot RDS PCI.RDS.1 deve essere privato	[RDS.1] L'istantanea RDS deve essere privata

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
PCI DSS v3.2.1	Le istanze DB RDS PCI.RDS.2 devono vietare l'accesso pubblico	[RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, in base alla durata PubliclyAccessible AWS Config
PCI DSS v3.2.1	PCI.Redshift.1 I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico	[Redshift.1] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico
PCI DSS v3.2.1	I bucket PCI.S3.1 S3 dovrebbero vietare l'accesso pubblico in scrittura	[S3.3] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura
PCI DSS v3.2.1	I bucket PCI.S3.2 S3 devono vietare l'accesso pubblico in lettura	[S3.2] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura
PCI DSS v3.2.1	I bucket PCI.S3.3 S3 devono avere la replica tra regioni abilitata	[S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni
PCI DSS v3.2.1	I bucket PCI.S3.5 S3 dovrebbero richiedere richieste per utilizzare Secure Socket Layer	[S3.5] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL
PCI DSS v3.2.1	L'impostazione PCI.S3.6 S3 Block Public Access deve essere abilitata	[S3.1] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate
PCI DSS v3.2.1	PCI. SageMaker.1 Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet	[SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet

Standard	ID e titolo di controllo standard	ID e titolo del controllo di sicurezza
PCI DSS v3.2.1	Le istanze PCI.SSM.1 EC2 gestite da Systems Manager dovrebbero avere uno stato di conformità alla patch pari a COMPLIANT dopo l'installazione della patch	[SSM.2] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch
PCI DSS v3.2.1	Le istanze PCI.SSM.2 EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT	[SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT
PCI DSS v3.2.1	Le istanze PCI.SSM.3 EC2 devono essere gestite da AWS Systems Manager	[SSM.1] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager

Aggiornamento dei flussi di lavoro per il consolidamento

Se i flussi di lavoro non si basano sul formato specifico di alcun campo di ricerca dei controlli, non è richiesta alcuna azione.

Se i flussi di lavoro si basano sul formato specifico di qualsiasi campo di ricerca dei controlli riportato nelle tabelle, è necessario aggiornare i flussi di lavoro. Ad esempio, se hai creato una regola Amazon CloudWatch Events che ha attivato un'azione per un ID di controllo specifico (come richiamare una AWS Lambda funzione se l'ID di controllo è uguale a CIS 2.7), aggiorna la regola per utilizzare CloudTrail .2, il campo per quel controllo. `Compliance.SecurityControlId`

Se hai creato [approfondimenti personalizzati](#) utilizzando uno dei campi o valori di ricerca del controllo che sono stati modificati, aggiorna tali approfondimenti per utilizzare i campi o i valori correnti.

Esempi ASFF

Le seguenti sezioni contengono esempi di attributi obbligatori e facoltativi nel AWS Security Finding Format (ASFF), nonché esempi di ogni risorsa supportata da ASFF.

Argomenti

- [Attributi di primo livello obbligatori](#)

- [Attributi opzionali di primo livello](#)
- [Resources](#)

Attributi di primo livello obbligatori

I seguenti attributi di primo livello nel AWS Security Finding Format (ASFF) sono necessari per tutti i risultati in Security Hub. Per ulteriori informazioni su questi attributi obbligatori, consulta l'AWS Security Hub API [AwsSecurityFindingReference](#).

AwsAccountId

L' Account AWS ID a cui si riferisce il risultato.

Esempio

```
"AwsAccountId": "111111111111"
```

CreatedAt

Indica quando è stato creato il potenziale problema di sicurezza rilevato da un risultato.

Esempio

```
"CreatedAt": "2017-03-22T13:22:13.933Z"
```

Note

Security Hub elimina i risultati 90 giorni dopo l'aggiornamento più recente o 90 giorni dopo la data di creazione se non si verifica alcun aggiornamento. Per archiviare i risultati per più di 90 giorni, puoi configurare una regola in Amazon EventBridge che indirizza i risultati al tuo bucket S3.

Descrizione

La descrizione di una ricerca. Questo campo può essere testo boilerplate non specifico o dettagli che sono specifici dell'istanza del risultato.

Per i risultati di controllo generati da Security Hub, questo campo fornisce una descrizione del controllo.

Questo campo non fa riferimento a uno standard se attivi i [risultati del controllo consolidato](#).

Esempio

```
"Description": "This AWS control checks whether AWS Config is enabled in the current account and Region."
```

GeneratorId

L'identificatore per il componente specifico della soluzione (un'unità di logica discreta) che ha generato un risultato.

Per i risultati di controllo generati da Security Hub, questo campo non fa riferimento a uno standard se attivi i [risultati del controllo consolidato](#).

Esempio

```
"GeneratorId": "security-control/Config.1"
```

Id

L'identificatore specifico del prodotto per un risultato. Per i risultati di controllo generati da Security Hub, questo campo fornisce l'Amazon Resource Name (ARN) del risultato.

Questo campo non fa riferimento a uno standard se attivi i risultati del [controllo consolidato](#).

Esempio

```
"Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/iam.9/finding/ab6d6a26-a156-48f0-9403-115983e5a956"
```

```
"
```

ProductArn

L'Amazon Resource Name (ARN) generato da Security Hub che identifica in modo univoco un prodotto di ricerca di terze parti dopo la registrazione del prodotto presso Security Hub.

Il formato di questo campo è `arn:partition:securityhub:region:account-id:product/company-id/product-id`.

- Per AWS i servizi integrati con Security Hub, `company-id` deve essere "aws" e `product-id` deve essere il nome del servizio AWS pubblico. Poiché AWS i prodotti e i servizi non sono associati a un account, la `account-id` sezione dell'ARN è vuota. AWS i servizi che non sono ancora integrati con Security Hub sono considerati prodotti di terze parti.
- Per prodotti pubblici, `company-id` e `product-id` devono essere i valori ID specificati al momento della registrazione.
- Per prodotti privati, `company-id` deve essere l'ID account. `product-id` deve essere la parola riservata "default" o l'ID specificato al momento della registrazione.

Esempio

```
// Private ARN
  "ProductArn": "arn:aws:securityhub:us-east-1:111111111111:product/111111111111/default"

// Public ARN

  "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty"
  "ProductArn": "arn:aws:securityhub:us-west-2:222222222222:product/generico/secure-pro"
```

Risorse

L'[Resource](#) oggetto fornisce un insieme di tipi di dati relativi alle risorse che descrivono le AWS risorse a cui si riferisce il risultato.

Esempio

```
"Resources": [
  {
    "ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/SampleApp/1234567890abcdef0",
    "ApplicationName": "SampleApp",
    "DataClassification": {
      "DetailedResultsLocation": "Path_to_Folder_Or_File",
      "Result": {
        "MimeType": "text/plain",
        "SizeClassified": 2966026,
        "AdditionalOccurrences": false,
        "Status": {
```

```

    "Code": "COMPLETE",
    "Reason": "Unsupportedfield"
  },
  "SensitiveData": [
    {
      "Category": "PERSONAL_INFORMATION",
      "Detections": [
        {
          "Count": 34,
          "Type": "GE_PERSONAL_ID",
          "Occurrences": {
            "LineRanges": [
              {
                "Start": 1,
                "End": 10,
                "StartColumn": 20
              }
            ],
            "Pages": [],
            "Records": [],
            "Cells": []
          }
        },
        {
          "Count": 59,
          "Type": "EMAIL_ADDRESS",
          "Occurrences": {
            "Pages": [
              {
                "PageNumber": 1,
                "OffsetRange": {
                  "Start": 1,
                  "End": 100,
                  "StartColumn": 10
                },
                "LineRange": {
                  "Start": 1,
                  "End": 100,
                  "StartColumn": 10
                }
              }
            ]
          }
        }
      ]
    }
  ],

```

```
    {
      "Count": 2229,
      "Type": "URL",
      "Occurrences": {
        "LineRanges": [
          {
            "Start": 1,
            "End": 13
          }
        ]
      }
    },
    {
      "Count": 13826,
      "Type": "NameDetection",
      "Occurrences": {
        "Records": [
          {
            "RecordIndex": 1,
            "JsonPath": "$.ssn.value"
          }
        ]
      }
    },
    {
      "Count": 32,
      "Type": "AddressDetection"
    }
  ],
  "TotalCount": 32
},
"CustomDataIdentifiers": {
  "Detections": [
    {
      "Arn": "1712be25e7c7f53c731fe464f1c869b8",
      "Name": "1712be25e7c7f53c731fe464f1c869b8",
      "Count": 2,
    }
  ],
  "TotalCount": 2
}
},
```

```
"Type": "AwsEc2Instance",
"Id": "arn:aws:ec2:us-west-2:123456789012:instance/i-abcdef01234567890",
"Partition": "aws",
"Region": "us-west-2",
"ResourceRole": "Target",
"Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": true
},
"Details": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
  "ImageId": "ami-79fd7eee",
  "IPv4Addresses": ["1.1.1.1"],
  "IPv6Addresses": ["2001:db8:1234:1a2b::123"],
  "KeyName": "testkey",
  "LaunchedAt": "2018-09-29T01:25:54Z",
  "MetadataOptions": {
    "HttpEndpoint": "enabled",
    "HttpProtocolIpv6": "enabled",
    "HttpPutResponseHopLimit": 1,
    "HttpTokens": "optional",
    "InstanceMetadataTags": "disabled"
  }
},
"NetworkInterfaces": [
  {
    "NetworkInterfaceId": "eni-e5aa89a3"
  }
],
"SubnetId": "PublicSubnet",
"Type": "i3.xlarge",
"VirtualizationType": "hvm",
"VpcId": "TestVPCIPv6"
}
```

SchemaVersion

La versione dello schema per cui un risultato è formattato. Il valore di questo campo deve essere una delle versioni pubblicate ufficialmente identificate da AWS. Nella versione corrente, la versione dello schema AWS Security Finding Format è 2018-10-08.

Esempio

```
"SchemaVersion": "2018-10-08"
```

Gravità

Definisce l'importanza di un risultato. Per i dettagli su questo oggetto, [Severity](#) consulta l'AWS Security Hub API Reference.

Severity è sia un oggetto di primo livello in una ricerca che annidato sotto l'FindingProviderFields oggetto.

Il valore dell'Severity oggetto di primo livello per un risultato deve essere aggiornato solo dall'API. [BatchUpdateFindings](#)

Per fornire informazioni sulla gravità, i provider di ricerca devono aggiornare l'Severity oggetto sotto FindingProviderFields quando effettuano una richiesta [BatchImportFindings](#) API.

Se una BatchImportFindings richiesta per un nuovo risultato fornisce solo Label o fornisce solo Normalized, Security Hub compila automaticamente il valore dell'altro campo. Il Product campo sottostante FindingProviderFields è stato ritirato e non è compilato nei risultati correnti. Utilizza invece il Original campo.

La gravità del risultato non considera la criticità degli asset coinvolti o della risorsa sottostante. La criticità è definita come il livello di importanza delle risorse associate al risultato. Ad esempio, una risorsa associata a un'applicazione mission critical ha una criticità maggiore di quella associata ai test non di produzione. Per acquisire informazioni sulla criticità delle risorse, utilizza il campo Criticality.

Si consiglia di utilizzare le seguenti indicazioni per tradurre i punteggi di gravità nativi dei risultati nel valore dell'ASFF. Severity.Label

- **INFORMATIONAL**— Questa categoria può includere un risultato relativo all'identificazione PASSED di WARNING dati sensibili o di NOT AVAILABLE controllo.
- **LOW**— Risultati che potrebbero portare a future compromessi. Ad esempio, questa categoria può includere vulnerabilità, punti deboli di configurazione e password esposte.
- **MEDIUM**— Risultati che indicano un compromesso attivo, ma nessuna indicazione che un avversario abbia raggiunto i propri obiettivi. Ad esempio, questa categoria può includere attività legate a malware, attività di hacking e rilevamento di comportamenti insoliti.

- **HIGH**pure **CRITICAL** — Risultati che indicano che un avversario ha raggiunto i propri obiettivi, come la perdita o la compromissione attiva dei dati o l'interruzione del servizio.

Esempio

```
"Severity": {
  "Label": "CRITICAL",
  "Normalized": 90,
  "Original": "CRITICAL"
}
```

Title

Il titolo di un risultato. Questo campo può contenere testo boilerplate non specifico o dettagli specifici per l'istanza del risultato.

Per i risultati del controllo, questo campo fornisce il titolo del controllo.

Questo campo non fa riferimento a uno standard se attivi i [risultati del controllo consolidato](#).

Esempio

```
"Title": "AWS Config should be enabled"
```

Tipi

Uno o più tipi di risultati nel formato *namespace/category/classifier* che classificano un risultato. Questo campo non fa riferimento a uno standard se attivi i risultati del [controllo consolidato](#).

Types deve essere aggiornato solo utilizzando [BatchUpdateFindings](#).

La ricerca di fornitori che desiderano fornire un valore per Types dovrebbe utilizzare l'Types attributo sotto [FindingProviderFields](#).

Nell'elenco seguente, i punti elenco di primo livello sono namespace, i punti elenco di secondo livello sono categorie e i punti elenco di terzo livello sono classificatori. Consigliamo che i provider di ricerca utilizzino namespace definiti per ordinare e raggruppare i risultati. È possibile utilizzare anche le categorie e i classificatori definiti, ma non sono obbligatori. Solo lo spazio dei nomi Software and Configuration Checks dispone di classificatori definiti.

È possibile definire un percorso parziale per namespace/categoria/classificatore. Ad esempio, i seguenti tipi di ricerca sono tutti validi:

- TTPs
- TTPs/Defense Evasion
- TTPs/Evasione dalla difesa/ CloudTrailStopped

Le categorie di tattiche, tecniche e procedure (TTP) nell'elenco seguente si allineano al [MITRE ATT&CK Matrix](#)TM. Lo spazio dei nomi Unusual Behaviors riflette comportamenti insoliti generali, come anomalie statistiche generali, e non è allineato con un TTP specifico. Tuttavia, è possibile classificare un risultato con entrambi i tipi di risultato Unusual Behaviors e TTPs.

Elenco di namespace, categorie e classificatori:

- Software and Configuration Checks
 - Vulnerabilità
 - CVE
 - AWS Migliori pratiche di sicurezza
 - Network Reachability
 - Runtime Behavior Analysis
 - Industry and Regulatory Standards
 - AWS Migliori pratiche di sicurezza di base
 - CIS Host Hardening Benchmarks
 - Benchmark CIS Foundations AWS
 - PCI-DSS
 - Controlli Cloud Security Alliance
 - Controlli ISO 90001
 - Controlli ISO 27001
 - Controlli ISO 27017
 - Controlli ISO 27018
 - SOC 1
 - SOC 2
 - Controlli HIPAA (USA)

- Controlli NIST 800-53 (USA)
- Controlli NIST CSF (USA)
- Controlli IRAP (Australia)
- Controlli K-ISMS (Corea)
- Controlli MTCS (Singapore)
- Controlli FISC (Giappone)
- Controlli My Number Act (Giappone)
- Controlli ENS (Spagna)
- Controlli Cyber Essentials Plus (Regno Unito)
- Controlli G-Cloud (Regno Unito)
- Controlli C5 (Germania)
- Controlli IT-Grundschutz (Germania)
- Controlli GDPR (Europa)
- Controlli TISAX (Europa)
- Gestione delle patch
- TTPs
 - Accesso iniziale
 - Esecuzione
 - Persistenza
 - Escalation dei privilegi
 - Defense Evasion
 - Accessi a credenziali
 - Individuazione
 - Movimento laterale
 - Raccolta
 - Comando e controllo
- Effetti
 - Esposizione di dati
 - **Esfiltrazione di dati**

- Denial of Service
- Consumo di risorse
- Comportamenti insoliti
 - Applicazione
 - Flusso di rete
 - Indirizzo IP
 - Utente
 - VM
 - Container
 - Serverless
 - Processo
 - Database
 - Dati
- Identificazioni dati sensibili
 - Informazioni che consentono l'identificazione personale degli utenti
 - Password
 - Note legali
 - Servizi finanziari
 - Sicurezza
 - Business

Esempio

```
"Types": [  
  "Software and Configuration Checks/Vulnerabilities/CVE"  
]
```

UpdatedAt

Indica quando il provider di ricerca ha aggiornato l'ultima volta il record dei risultati.

Questo timestamp indica l'ora in cui il record di ricerca è stato aggiornato l'ultima volta o l'ultimo aggiornamento. Di conseguenza, può differire dal `LastObservedAt` timestamp, che indica quando l'evento o la vulnerabilità sono stati osservati l'ultima volta o l'ultima volta.

Quando si aggiorna il record di risultato, è necessario aggiornare il timestamp al timestamp corrente. Al momento della creazione di un record di ricerca, i timestamp `CreatedAt` e `UpdatedAt` timestamp devono essere gli stessi. Dopo un aggiornamento del record di ricerca, il valore di questo campo deve essere più recente di tutti i valori precedenti in esso contenuti.

Tieni presente che `UpdatedAt` non può essere aggiornato utilizzando l'operazione [BatchUpdateFindings](#) API. Puoi aggiornarlo solo utilizzando [BatchImportFindings](#).

Esempio

```
"UpdatedAt": "2017-04-22T13:22:13.933Z"
```

Note

Security Hub elimina i risultati 90 giorni dopo l'aggiornamento più recente o 90 giorni dopo la data di creazione se non si verifica alcun aggiornamento. Per archiviare i risultati per più di 90 giorni, puoi configurare una regola in Amazon EventBridge che indirizza i risultati al tuo bucket S3.

Attributi opzionali di primo livello

Questi attributi di primo livello sono opzionali nel AWS Security Finding Format (ASFF). Per ulteriori informazioni su questi attributi, consulta l'AWS Security Hub API [AwsSecurityFindingReference](#).

Azione

L'[Action](#) oggetto fornisce dettagli su un'azione che influisce o che è stata intrapresa su una risorsa.

Esempio

```
"Action": {
  "ActionType": "PORT_PROBE",
  "PortProbeAction": {
    "PortProbeDetails": [
      {
        "LocalPortDetails": {
          "Port": 80,
          "PortName": "HTTP"
        },
        "LocalIpDetails": {
```

```
        "IpAddressV4": "192.0.2.0"
      },
      "RemoteIpDetails": {
        "Country": {
          "CountryName": "Example Country"
        },
        "City": {
          "CityName": "Example City"
        },
        "GeoLocation": {
          "Lon": 0,
          "Lat": 0
        },
        "Organization": {
          "AsnOrg": "ExampleASO",
          "Org": "ExampleOrg",
          "Isp": "ExampleISP",
          "Asn": 64496
        }
      }
    },
    "Blocked": false
  }
}
```

AwsAccountName

Il Account AWS nome a cui si applica il risultato.

Esempio

```
"AwsAccountName": "jane-doe-testaccount"
```

CompanyName

Il nome dell'azienda del prodotto che ha generato il risultato. Per i risultati basati sul controllo, la società è. AWS

Security Hub compila automaticamente questo attributo per ogni risultato. Non è possibile aggiornarlo utilizzando [BatchImportFindings](#) o [BatchUpdateFindings](#). L'eccezione è quando si utilizza un'integrazione personalizzata. Per informazioni, consulta [the section called "Utilizzo di integrazioni di prodotti personalizzate"](#).

Quando si utilizza la console Security Hub per filtrare i risultati in base al nome dell'azienda, si utilizza questo attributo. Quando si utilizza l'API Security Hub per filtrare i risultati in base al nome dell'azienda, si utilizza l'`aws/securityhub/CompanyName` attributo sotto `ProductFields`. Security Hub non sincronizza questi due attributi.

Esempio

```
"CompanyName": "AWS"
```

Conformità

L'[Compliance](#) oggetto fornisce dettagli di ricerca relativi a un controllo. Questo attributo viene restituito per i risultati generati da un controllo Security Hub e per i risultati AWS Config inviati a Security Hub.

Esempio

```
"Compliance": {
  "AssociatedStandards": [
    {"StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
    {"StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
    {"StandardsId": "standards/nist-800-53/v/5.0.0"}
  ],
  "RelatedRequirements": [
    "NIST.800-53.r5 AC-4",
    "NIST.800-53.r5 AC-4(21)",
    "NIST.800-53.r5 SC-7",
    "NIST.800-53.r5 SC-7(11)",
    "NIST.800-53.r5 SC-7(16)",
    "NIST.800-53.r5 SC-7(21)",
    "NIST.800-53.r5 SC-7(4)",
    "NIST.800-53.r5 SC-7(5)"
  ],
  "SecurityControlId": "EC2.18",
  "SecurityControlParameters": [
    {
      "Name": "authorizedTcpPorts",
      "Value": ["80", "443"]
    },
    {
      "Name": "authorizedUdpPorts",
      "Value": ["427"]
    }
  ]
}
```

```
    }
  ],
  "Status": "NOT_AVAILABLE",
  "StatusReasons": [
    {
      "ReasonCode": "CONFIG_RETURNS_NOT_APPLICABLE",
      "Description": "This finding has a compliance status of NOT AVAILABLE because AWS Config sent Security Hub a finding with a compliance state of Not Applicable. The potential reasons for a Not Applicable finding from Config are that (1) a resource has been moved out of scope of the Config rule; (2) the Config rule has been deleted; (3) the resource has been deleted; or (4) the logic of the Config rule itself includes scenarios where Not Applicable is returned. The specific reason why Not Applicable is returned is not available in the Config rule evaluation."
    }
  ]
}
```

Confidence

La probabilità che un risultato identifichi accuratamente il comportamento o il problema che intendeva identificare.

Confidence deve essere aggiornato solo utilizzando [BatchUpdateFindings](#).

La ricerca di fornitori che desiderano fornire un valore per Confidence dovrebbe utilizzare l'attribute Confidence sotto FindingProviderFields. Per informazioni, consulta [the section called "Uso di FindingProviderFields"](#).

Confidence viene assegnato un punteggio da 0 a 100 utilizzando una scala di rapporti. 0 significa confidenza dello 0% e 100 indica una confidenza del 100 percento. Ad esempio, un rilevamento di un'esfiltrazione di dati basato su una deviazione statistica del traffico di rete ha una bassa affidabilità perché non è stata verificata un'effettiva esfiltrazione.

Esempio

```
"Confidence": 42
```

Criticità

Il livello di importanza assegnato alle risorse associate a un risultato.

Criticality deve essere aggiornato solo chiamando l'operazione [BatchUpdateFindingsAPI](#). Non aggiornare questo oggetto con [BatchImportFindings](#).

La ricerca di fornitori che desiderano fornire un valore per `Criticality` deve utilizzare l'`Criticality` attributo sotto `FindingProviderFields`. Per informazioni, consulta [the section called "Uso di FindingProviderFields"](#).

`Criticality` viene assegnato un punteggio da 0 a 100, utilizzando una scala di rapporti che supporta solo numeri interi completi. Un punteggio 0 indica che le risorse sottostanti non presentano criticità, mentre un punteggio 100 è riservato per la maggior parte delle risorse critiche.

Per ogni risorsa, al momento dell'assegnazione, tenete presente quanto segue: `Criticality`

- La risorsa interessata contiene dati sensibili (ad esempio, un bucket S3 con PII)?
- La risorsa interessata consente a un avversario di approfondire il proprio accesso o di estendere le proprie capacità per svolgere attività dannose aggiuntive (ad esempio, un account sysadmin compromesso)?
- La risorsa è un asset critico per l'azienda (ad esempio, un sistema aziendale chiave che se compromesso potrebbe avere un impatto notevole sui profitti)?

Puoi utilizzare le linee guida seguenti:

- Una risorsa che alimenta sistemi mission-critical o che contiene dati altamente sensibili può essere valutata nell'intervallo 75-100.
- Una risorsa che alimenta sistemi importanti (ma non critici) o che contiene dati moderatamente importanti può essere valutata nell'intervallo 25-74.
- Una risorsa che alimenta sistemi non importanti o che contiene dati non sensibili dovrebbe avere un punteggio compreso tra 0 e 24.

Esempio

```
"Criticality": 99
```

`FindingProviderFields`

`FindingProviderFields` include i seguenti attributi:

- `Confidence`
- `Criticality`

- RelatedFindings
- Severity
- Types

È possibile eseguire l'aggiornamento FindingProviderFields utilizzando l'operazione [BatchImportFindings](#) API. Non è possibile aggiornarlo con [BatchUpdateFindings](#).

Per i dettagli su come Security Hub gestisce gli aggiornamenti da FindingProviderFields e [BatchImportFindings](#) verso gli attributi di primo livello corrispondenti, vedere [the section called "Usando di FindingProviderFields"](#).

Esempio

```
"FindingProviderFields": {
  "Confidence": 42,
  "Criticality": 99,
  "RelatedFindings": [
    {
      "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",
      "Id": "123e4567-e89b-12d3-a456-426655440000"
    }
  ],
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [ "Software and Configuration Checks/Vulnerabilities/CVE" ]
}
```

FirstObservedAt

Indica quando il potenziale problema di sicurezza rilevato da un risultato è stato osservato per la prima volta.

Questo timestamp indica l'ora in cui l'evento o la vulnerabilità sono stati osservati per la prima volta. Di conseguenza, può differire dal CreatedAt timestamp, che riflette l'ora in cui è stato creato questo record di risultati.

Questo timestamp dovrebbe essere immutabile tra un aggiornamento e l'altro del record di ricerca, ma può essere aggiornato se viene determinato un timestamp più preciso.

Esempio

```
"FirstObservedAt": "2017-03-22T13:22:13.933Z"
```

LastObservedAt

Indica quando il potenziale problema di sicurezza rilevato da un risultato è stato rilevato più di recente dal prodotto Security Finds.

Questo timestamp indica l'ora in cui l'evento o la vulnerabilità sono stati osservati l'ultima volta o l'ultima volta. Di conseguenza, può differire dal `UpdatedAt` timestamp, che indica quando questo record di risultati è stato aggiornato l'ultima volta o l'ultimo aggiornamento.

È possibile fornire questo timestamp, ma non è richiesto alla prima osservazione. Se fornisci questo campo alla prima osservazione, il timestamp dovrebbe essere lo stesso del timestamp. `FirstObservedAt` Aggiornare questo campo per riflettere l'ultimo timestamp o il timestamp osservato più di recente ogni volta che un risultato viene osservato.

Esempio

```
"LastObservedAt": "2017-03-23T13:22:13.933Z"
```

Malware

L'oggetto [Malware](#) fornisce un elenco di malware relativo a una ricerca.

Esempio

```
"Malware": [  
  {  
    "Name": "Stringler",  
    "Type": "COIN_MINER",  
    "Path": "/usr/sbin/stringler",  
    "State": "OBSERVED"  
  }  
]
```

Rete (ritirata)

L'[Network](#) oggetto fornisce informazioni relative alla rete su un risultato.

Questo oggetto è stato ritirato. Per fornire questi dati, è possibile mappare i dati a una risorsa in `Resources` o utilizzare l'`Action` oggetto.

Esempio

```
"Network": {
  "Direction": "IN",
  "OpenPortRange": {
    "Begin": 443,
    "End": 443
  },
  "Protocol": "TCP",
  "SourceIPv4": "1.2.3.4",
  "SourceIPv6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
  "SourcePort": "42",
  "SourceDomain": "example1.com",
  "SourceMac": "00:0d:83:b1:c0:8e",
  "DestinationIPv4": "2.3.4.5",
  "DestinationIPv6": "FE80:CD00:0000:0CDE:1257:0000:211E:729C",
  "DestinationPort": "80",
  "DestinationDomain": "example2.com"
}
```

NetworkPath

L'[NetworkPath](#) oggetto fornisce informazioni su un percorso di rete correlato a un risultato. Ogni voce in `NetworkPath` rappresenta un componente del percorso.

Esempio

```
"NetworkPath" : [
  {
    "ComponentId": "abc-01a234bc56d8901ee",
    "ComponentType": "AWS::EC2::InternetGateway",
    "Egress": {
      "Destination": {
        "Address": [ "192.0.2.0/24" ],
        "PortRanges": [
          {
            "Begin": 443,
            "End": 443
          }
        ]
      }
    }
  }
]
```

```

    },
    "Protocol": "TCP",
    "Source": {
      "Address": ["203.0.113.0/24"]
    }
  },
  "Ingress": {
    "Destination": {
      "Address": [ "198.51.100.0/24" ],
      "PortRanges": [
        {
          "Begin": 443,
          "End": 443
        }
      ]
    },
    "Protocol": "TCP",
    "Source": {
      "Address": [ "203.0.113.0/24" ]
    }
  }
}
]

```

Nota

L'[Note](#) oggetto specifica una nota definita dall'utente che è possibile aggiungere a un risultato.

Un provider di risultati può fornire una nota iniziale per una ricerca, ma non può aggiungere note successivamente. È possibile aggiornare una nota solo utilizzando [BatchUpdateFindings](#)

Esempio

```

"Note": {
  "Text": "Don't forget to check under the mat.",
  "UpdatedBy": "jsmith",
  "UpdatedAt": "2018-08-31T00:15:09Z"
}

```

PatchSummary

L'[PatchSummary](#) oggetto fornisce un riepilogo dello stato di conformità della patch per un'istanza rispetto a uno standard di conformità selezionato.

Esempio

```
"PatchSummary" : {
  "FailedCount" : 0,
  "Id" : "pb-123456789098",
  "InstalledCount" : 100,
  "InstalledOtherCount" : 1023,
  "InstalledPendingReboot" : 0,
  "InstalledRejectedCount" : 0,
  "MissingCount" : 100,
  "Operation" : "Install",
  "OperationEndTime" : "2018-09-27T23:39:31Z",
  "OperationStartTime" : "2018-09-27T23:37:31Z",
  "RebootOption" : "RebootIfNeeded"
}
```

Processo

L'[Process](#) oggetto fornisce dettagli relativi al processo relativi a un risultato.

Esempio:

```
"Process": {
  "LaunchedAt": "2018-09-27T22:37:31Z",
  "Name": "syslogd",
  "ParentPid": 56789,
  "Path": "/usr/sbin/syslogd",
  "Pid": 12345,
  "TerminatedAt": "2018-09-27T23:37:31Z"
}
```

ProcessedAt

Indica quando Security Hub ha ricevuto un risultato e inizia a elaborarlo.

Ciò differisce da `CreatedAt` e `UpdatedAt`, che sono timestamp obbligatori che si riferiscono all'interazione del fornitore del servizio di ricerca con il problema di sicurezza e la scoperta. Il `ProcessedAt` timestamp indica quando Security Hub inizia a elaborare un risultato. Una volta completata l'elaborazione, viene visualizzato un risultato nell'account di un utente.

```
"ProcessedAt": "2023-03-23T13:22:13.933Z"
```

ProductFields

Un tipo di dati in cui i prodotti per i risultati della sicurezza possono includere dettagli aggiuntivi specifici della soluzione che non fanno parte del AWS Security Finding Format definito.

Per i risultati generati dai controlli del Security Hub, ProductFields include informazioni sul controllo. Per informazioni, consulta [the section called “Generazione e aggiornamento dei risultati del controllo”](#).

Questo campo non deve contenere dati ridondanti e non deve contenere dati in conflitto con i campi del AWS Security Finding Format.

Il prefisso `aws/` rappresenta uno spazio dei nomi riservato solo a AWS prodotti e servizi e non deve essere associato ai risultati di integrazioni di terze parti.

Anche se non richiesto, i nomi di campo dei prodotti devono avere il formato `company-id/product-id/field-name`, in cui `company-id` e `product-id` corrispondono a quelli forniti nella `ProductArn` del risultato.

I campi a cui si fa riferimento `Archival` vengono utilizzati quando Security Hub archivia un risultato esistente. Ad esempio, Security Hub archivia i risultati esistenti quando si disattiva un controllo o uno standard e quando si attivano o disattivano [i risultati del controllo consolidato](#).

Questo campo può includere anche informazioni sullo standard che include il controllo che ha prodotto il risultato.

Esempio

```
"ProductFields": {
  "API", "DeleteTrail",
  "ArchivalReasons:0/Description": "The finding is in an ARCHIVED state because
consolidated control findings has been turned on or off. This causes findings in the
previous state to be archived when new findings are being generated.",
  "ArchivalReasons:0/ReasonCode": "CONSOLIDATED_CONTROL_FINDINGS_UPDATE",
  "aws/inspector/AssessmentTargetName": "My prod env",
  "aws/inspector/AssessmentTemplateName": "My daily CVE assessment",
  "aws/inspector/RulesPackageName": "Common Vulnerabilities and Exposures",
  "generico/secure-pro/Action.Type", "AWS_API_CALL",
  "generico/secure-pro/Count": "6",
  "Service_Name": "cloudtrail.amazonaws.com"
}
```

ProductName

Fornisce il nome del prodotto che ha generato il risultato. Per i risultati basati sul controllo, il nome del prodotto è Security Hub.

Security Hub compila automaticamente questo attributo per ogni risultato. Non è possibile aggiornarlo utilizzando [BatchImportFindings](#) o [BatchUpdateFindings](#). L'eccezione è quando si utilizza un'integrazione personalizzata. Per informazioni, consulta [the section called "Utilizzo di integrazioni di prodotti personalizzate"](#).

Quando si utilizza la console Security Hub per filtrare i risultati in base al nome del prodotto, si utilizza questo attributo.

Quando si utilizza l'API Security Hub per filtrare i risultati in base al nome del prodotto, si utilizza l'aws/securityhub/ProductNameattributo sottoProductFields.

Security Hub non sincronizza questi due attributi.

RecordState

Fornisce lo stato di registrazione di un risultato.

Per impostazione predefinita, i risultati inizialmente generati da un servizio sono considerati ACTIVE.

Lo stato ARCHIVED indica che un risultato deve essere nascosto dalla vista. I risultati archiviati non vengono eliminati immediatamente. È possibile cercarli, esaminarli e riferirli. Security Hub archivia automaticamente i risultati basati sul controllo se la risorsa associata viene eliminata, la risorsa non esiste o il controllo è disabilitato.

RecordState è destinato alla ricerca di fornitori e può essere aggiornato solo da [BatchImportFindings](#). Non è possibile aggiornarlo utilizzando [BatchUpdateFindings](#).

Per tenere traccia dello stato della tua indagine su un risultato, usa [Workflow](#) invece di RecordState.

Se lo stato del record cambia da ARCHIVED a ACTIVE e lo stato del flusso di lavoro del risultato è NOTIFIED o RESOLVED, Security Hub imposta automaticamente lo stato del flusso di lavoro su NEW.

Esempio

```
"RecordState": "ACTIVE"
```

Regione

Specifica il risultato Regione AWS da cui è stato generato il risultato.

Security Hub compila automaticamente questo attributo per ogni risultato. Non è possibile aggiornarlo utilizzando [BatchImportFindings](#) o [BatchUpdateFindings](#).

Esempio

```
"Region": "us-west-2"
```

RelatedFindings

Fornisce un elenco di risultati correlati al risultato corrente.

RelatedFindings deve essere aggiornato solo con l'operazione [BatchUpdateFindings](#) API. Non dovresti aggiornare questo oggetto con [BatchImportFindings](#).

Per [BatchImportFindings](#) le richieste, i provider di ricerca devono utilizzare l'RelatedFindings oggetto sotto [FindingProviderFields](#).

Per visualizzare le descrizioni degli RelatedFindings attributi, [RelatedFinding](#) consulta l'AWS Security Hub API Reference.

Esempio

```
"RelatedFindings": [  
  { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",  
    "Id": "123e4567-e89b-12d3-a456-426655440000" },  
  { "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/guardduty",  
    "Id": "AcmeNerfHerder-111111111111-x189dx7824" }  
]
```

Correzione

L'oggetto [Remediation](#) fornisce informazioni sulle procedure di correzione consigliate per risolvere la ricerca.

Esempio

```
"Remediation": {  
  "Recommendation": {
```

```
    "Text": "For instructions on how to fix this issue, see the AWS Security Hub  
documentation for EC2.2.",  
    "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.2/remediation"  
  }  
}
```

Project N.E.M.O.

Specifica se il risultato è un risultato di esempio.

```
"Sample": true
```

SourceUrl

L'`SourceUrl` oggetto fornisce un URL che rimanda a una pagina relativa alla scoperta corrente del prodotto oggetto della ricerca.

```
"SourceUrl": "http://sourceurl.com"
```

ThreatIntelIndicators

L'[ThreatIntelIndicator](#) oggetto fornisce dettagli di intelligence sulle minacce correlati a una scoperta.

Esempio

```
"ThreatIntelIndicators": [  
  {  
    "Category": "BACKDOOR",  
    "LastObservedAt": "2018-09-27T23:37:31Z",  
    "Source": "Threat Intel Weekly",  
    "SourceUrl": "http://threatintelweekly.org/backdoors/8888",  
    "Type": "IPV4_ADDRESS",  
    "Value": "8.8.8.8",  
  }  
]
```

Minacce

L'[Threats](#) oggetto fornisce dettagli sulla minaccia rilevata da un risultato.

Esempio


```
"Threats": [{
  "FilePaths": [{
    "FileName": "b.txt",
    "FilePath": "/tmp/b.txt",
    "Hash": "sha256",
    "ResourceId": "arn:aws:ec2:us-west-2:123456789012:volume/vol-032f3bdd89aee112f"
  }],
  "ItemCount": 3,
  "Name": "Iot.linux.mirai.vwisi",
  "Severity": "HIGH"
}]
```

UserDefinedFields

Fornisce un elenco di coppie di stringhe nome-valore associate al risultato. Si tratta di campi personalizzati, definiti dall'utente che vengono aggiunti a un risultato. Questi campi possono essere generati automaticamente tramite una configurazione specifica.

I fornitori di servizi di ricerca non devono utilizzare questo campo per i dati generati dal prodotto. Invece, i provider di ricerca possono utilizzare il `ProductFields` campo per i dati che non sono mappati a nessun campo standard del AWS Security Finding Format.

Questi campi possono essere aggiornati solo utilizzando [BatchUpdateFindings](#).

Esempio

```
"UserDefinedFields": {
  "reviewedByCio": "true",
  "comeBackToLater": "Check this again on Monday"
}
```

VerificationState

Fornisce la veridicità di un risultato. I prodotti Findings possono fornire un valore di UNKNOWN per questo campo. Un prodotto dei risultati dovrebbe fornire un valore per questo campo se esiste un analogo significativo nel sistema del prodotto dei risultati. Questo campo viene in genere compilato in base alla determinazione o all'azione dell'utente dopo l'analisi di un risultato.

Un provider di risultati può fornire un valore iniziale per questo attributo, ma non può aggiornarlo successivamente. È possibile aggiornare questo attributo solo utilizzando [BatchUpdateFindings](#)

```
"VerificationState": "Confirmed"
```

Vulnerabilità

L'[Vulnerabilities](#) oggetto fornisce un elenco di vulnerabilità associate a un risultato.

Esempio

```
"Vulnerabilities" : [
  {
    "CodeVulnerabilities": [{
      "Cwes": [
        "CWE-798",
        "CWE-799"
      ],
      "FilePath": {
        "EndLine": 421,
        "FileName": "package-lock.json",
        "FilePath": "package-lock.json",
        "StartLine": 420
      },
      "SourceArn": "arn:aws:lambda:us-east-1:123456789012:layer:AWS-AppConfig-
Extension:114"
    }],
    "Cvss": [
      {
        "BaseScore": 4.7,
        "BaseVector": "AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N",
        "Version": "V3"
      },
      {
        "BaseScore": 4.7,
        "BaseVector": "AV:L/AC:M/Au:N/C:C/I:N/A:N",
        "Version": "V2"
      }
    ],
    "EpssScore": 0.015,
    "ExploitAvailable": "YES",
    "FixAvailable": "YES",
    "Id": "CVE-2020-12345",
    "LastKnownExploitAt": "2020-01-16T00:01:35Z",
    "ReferenceUrls": [
      "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-12418",

```

```

    "http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17563"
  ],
  "RelatedVulnerabilities": ["CVE-2020-12345"],
  "Vendor": {
    "Name": "Alas",
    "Url": "https://alas.aws.amazon.com/ALAS-2020-1337.html",
    "VendorCreatedAt": "2020-01-16T00:01:43Z",
    "VendorSeverity": "Medium",
    "VendorUpdatedAt": "2020-01-16T00:01:43Z"
  },
  "VulnerablePackages": [
    {
      "Architecture": "x86_64",
      "Epoch": "1",
      "FilePath": "/tmp",
      "FixedInVersion": "0.14.0",
      "Name": "openssl",
      "PackageManager": "OS",
      "Release": "16.amzn2.0.3",
      "Remediation": "Update aws-crt to 0.14.0",
      "SourceLayerArn": "arn:aws:lambda:us-west-2:123456789012:layer:id",
      "SourceLayerHash":
"sha256:c1962c35b63a6ff6ce7df6e042ee82371a605ca9515569edec46ff14f926f001",
      "Version": "1.0.2k"
    }
  ]
}
]

```

Flusso di lavoro

L'oggetto [Workflow](#) fornisce informazioni sullo stato dell'indagine su un risultato.

Questo campo è destinato ai clienti da utilizzare con strumenti di correzione, orchestrazione e ticketing. Non è destinato per provider di risultati.

Puoi aggiornare il campo solo con Workflow [BatchUpdateFindings](#). I clienti possono anche aggiornarlo dalla console. Per informazioni, consulta [the section called "Impostazione dello stato dei risultati del flusso di lavoro"](#).

Esempio

```
"Workflow": {
```

```
"Status": "NEW"  
}
```

WorkflowState (Ritirato)

Questo oggetto è stato ritirato ed è stato sostituito dal Status campo dell'Workflowoggetto.

Questo campo fornisce lo stato del flusso di lavoro di un risultato. I prodotti dei risultati sono in grado di fornire il valore di NEW per questo campo. Un prodotto dei risultati è in grado di fornire un valore per questo campo se esiste un analogo significativo nel sistema del prodotto dei risultati.

Esempio

```
"WorkflowState": "NEW"
```

Resources

L'oggetto Resources fornisce informazioni sulle risorse coinvolte in una ricerca.

Contiene una matrice di un massimo di 32 oggetti risorsa.

Per determinare come vengono formattati i nomi delle risorse, vedere [AWS Sintassi del Security Finding Format \(ASFF\)](#).

Per alcuni esempi di ogni oggetto risorsa, selezionatelo dall'elenco seguente.

Argomenti

- [Attributi delle risorse](#)
- [AwsAmazonMQ](#)
- [AwsApiGateway](#)
- [AwsAppSync](#)
- [AwsAthena](#)
- [AwsAutoScaling](#)
- [AwsBackup](#)
- [AwsCertificateManager](#)
- [AwsCloudFormation](#)
- [AwsCloudFront](#)
- [AwsCloudTrail](#)

- [AwsCloudWatch](#)
- [AwsCodeBuild](#)
- [AwsDms](#)
- [AwsDynamoDB](#)
- [AwsEc2](#)
- [AwsEcr](#)
- [AwsEcs](#)
- [AwsEfs](#)
- [AwsEks](#)
- [AwsElasticBeanstalk](#)
- [AwsElasticSearch](#)
- [AwsElb](#)
- [AwsEventBridge](#)
- [AwsGuardDuty](#)
- [AwsIam](#)
- [AwsKinesis](#)
- [AwsKms](#)
- [AwsLambda](#)
- [AwsMsk](#)
- [AwsNetworkFirewall](#)
- [AwsOpenSearchService](#)
- [AwsRds](#)
- [AwsRedshift](#)
- [AwsRoute53](#)
- [AwsS3](#)
- [AwsSageMaker](#)
- [AwsSecretsManager](#)
- [AwsSns](#)
- [AwsSqs](#)
- [AwsSsm](#)

- [AwsStepFunctions](#)
- [AwsWaf](#)
- [AwsXray](#)
- [Container](#)
- [Other](#)

Attributi delle risorse

Di seguito sono riportate le descrizioni e gli esempi dell'Resource soggetto nel AWS Security Finding Format (ASFF). Per ulteriori informazioni sui campi, consulta [Risorse](#).

ApplicationArn

Identifica l'Amazon Resource Name (ARN) dell'applicazione coinvolta nella scoperta.

Esempio

```
"ApplicationArn": "arn:aws:resource-groups:us-west-2:123456789012:group/SampleApp/1234567890abcdef0"
```

ApplicationName

Identifica il nome dell'applicazione coinvolta nella scoperta.

Esempio

```
"ApplicationName": "SampleApp"
```

DataClassification

Il [DataClassification](#) campo fornisce informazioni sui dati sensibili rilevati sulla risorsa.

Esempio

```
"DataClassification": {  
  "DetailedResultsLocation": "Path_to_Folder_Or_File",  
  "Result": {  
    "MimeType": "text/plain",  
    "SizeClassified": 2966026,  
    "AdditionalOccurrences": false,  
    "Status": {
```

```

    "Code": "COMPLETE",
    "Reason": "Unsupportedfield"
  },
  "SensitiveData": [
    {
      "Category": "PERSONAL_INFORMATION",
      "Detections": [
        {
          "Count": 34,
          "Type": "GE_PERSONAL_ID",
          "Occurrences": {
            "LineRanges": [
              {
                "Start": 1,
                "End": 10,
                "StartColumn": 20
              }
            ],
            "Pages": [],
            "Records": [],
            "Cells": []
          }
        },
        {
          "Count": 59,
          "Type": "EMAIL_ADDRESS",
          "Occurrences": {
            "Pages": [
              {
                "PageNumber": 1,
                "OffsetRange": {
                  "Start": 1,
                  "End": 100,
                  "StartColumn": 10
                },
                "LineRange": {
                  "Start": 1,
                  "End": 100,
                  "StartColumn": 10
                }
              }
            ]
          }
        }
      ]
    }
  ],

```

```
    {
      "Count": 2229,
      "Type": "URL",
      "Occurrences": {
        "LineRanges": [
          {
            "Start": 1,
            "End": 13
          }
        ]
      }
    },
    {
      "Count": 13826,
      "Type": "NameDetection",
      "Occurrences": {
        "Records": [
          {
            "RecordIndex": 1,
            "JsonPath": "$.ssn.value"
          }
        ]
      }
    },
    {
      "Count": 32,
      "Type": "AddressDetection"
    }
  ],
  "TotalCount": 32
},
"CustomDataIdentifiers": {
  "Detections": [
    {
      "Arn": "1712be25e7c7f53c731fe464f1c869b8",
      "Name": "1712be25e7c7f53c731fe464f1c869b8",
      "Count": 2,
    }
  ],
  "TotalCount": 2
}
}
```



```
}
```

Informazioni

Il [Details](#) campo fornisce informazioni aggiuntive su una singola risorsa utilizzando gli oggetti appropriati. Ogni risorsa deve essere fornita in un oggetto risorsa separato nell'`Resources` oggetto.

Si noti che se la dimensione del risultato supera il massimo di 240 KB, l'`Details` oggetto viene rimosso dal risultato. Per i risultati del controllo che utilizzano AWS Config regole, è possibile visualizzare i dettagli delle risorse sulla AWS Config console.

Security Hub fornisce una serie di dettagli sulle risorse disponibili per i tipi di risorse supportati. Questi dettagli corrispondono ai valori dell'`Type` oggetto. Usa i tipi forniti quando possibile.

Ad esempio, se la risorsa è un bucket S3, imposta la risorsa `Type` su `AwsS3Bucket` e fornisci i dettagli della risorsa nell'[AwsS3Bucket](#) oggetto.

L'[Other](#) oggetto consente di fornire campi e valori personalizzati. L'`Other` oggetto viene utilizzato nei seguenti casi:

- Il tipo di risorsa (il valore della `resourceType`) non ha un oggetto di dettaglio corrispondente. Per fornire dettagli sulla risorsa, si utilizza l'[Other](#) oggetto.
- L'oggetto per il tipo di risorsa non include tutti i campi che si desidera compilare. In questo caso, utilizzate l'oggetto di dettaglio relativo al tipo di risorsa per compilare i campi disponibili. Utilizzate l'`Other` oggetto per compilare i campi che non si trovano nell'oggetto specifico del tipo.
- Il tipo di risorsa non è uno dei tipi forniti. In questo caso, `Resource.Type` impostate `Other` e utilizzate l'`Other` oggetto per compilare i dettagli.

Esempio

```
"Details": {
  "AwsEc2Instance": {
    "IamInstanceProfileArn": "arn:aws:iam::123456789012:role/IamInstanceProfileArn",
    "ImageId": "ami-79fd7eee",
    "IpV4Addresses": ["1.1.1.1"],
    "IpV6Addresses": ["2001:db8:1234:1a2b::123"],
    "KeyName": "testkey",
    "LaunchedAt": "2018-09-29T01:25:54Z",
    "MetadataOptions": {
      "HttpEndpoint": "enabled",
```

```
    "HttpProtocolIpv6": "enabled",
    "HttpPutResponseHopLimit": 1,
    "HttpTokens": "optional",
    "InstanceMetadataTags": "disabled"
  },
  "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
  ],
  "SubnetId": "PublicSubnet",
  "Type": "i3.xlarge",
  "VirtualizationType": "hvm",
  "VpcId": "TestVPCIPv6"
},
"AwsS3Bucket": {
  "OwnerId": "da4d66eac431652a4d44d490a00500bded52c97d235b7b4752f9f688566fe6de",
  "OwnerName": "acmes3bucketowner"
},
"Other": { "LightPen": "blinky", "SerialNo": "1234abcd"}
}
```

Id

L'identificatore per il tipo di risorsa specificato.

Per AWS le risorse identificate da Amazon Resource Names (ARN), questo è l'ARN.

Per AWS le risorse prive di ARN, questo è l'identificatore definito dal AWS servizio che ha creato la risorsa.

Per le non AWS risorse, si tratta di un identificatore univoco associato alla risorsa.

Esempio

```
"Id": "arn:aws:s3:::example-bucket"
```

Partizione

La partizione in cui si trova la risorsa. Una partizione è un gruppo di Regioni AWS. Ciascuno Account AWS è limitato a una partizione.

Sono supportate le seguenti partizioni:

- aws – Regioni AWS
- aws-cn - Regioni Cina
- aws-us-gov – AWS GovCloud (US) Region

Esempio

```
"Partition": "aws"
```

Regione

Il codice del Regione AWS luogo in cui si trova questa risorsa. Per un elenco dei codici regionali, consulta [Endpoint regionali](#).

Esempio

```
"Region": "us-west-2"
```

ResourceRole

Identifica il ruolo della risorsa nella scoperta. Una risorsa è l'obiettivo dell'attività di ricerca o l'attore che ha eseguito l'attività.

Esempio

```
"ResourceRole": "target"
```

Tag

È possibile aggiungere tag di risorse ai risultati che vengono inseriti in Security Hub, compresi i risultati di prodotti integrati Servizi AWS e di terze parti. È possibile etichettare le risorse supportate dal GetResources funzionamento dell'API AWS Resource Groups Tagging. Per un elenco delle risorse supportate, consulta [Servizi che supportano l'API Resource Groups Tagging](#).

L'aggiunta di tag indica i tag associati a una risorsa al momento dell'elaborazione del risultato. È possibile includere l'Tagsattributo solo per le risorse a cui è associato un tag. Se a una risorsa non è associato un tag, non includere un attributo Tags nel risultato.

L'inclusione dei tag delle risorse nei risultati elimina la necessità di creare pipeline di arricchimento dei dati o di arricchire manualmente i metadati dei risultati di sicurezza. [Puoi anche utilizzare i tag per cercare o filtrare risultati e approfondimenti e creare regole di automazione.](#)

Per informazioni sulle restrizioni che si applicano ai tag, consulta [Limiti e requisiti di denominazione dei tag](#).

In questo campo puoi fornire solo i tag che esistono su una AWS risorsa. Per fornire dati che non sono definiti nel AWS Security Finding Format, utilizza il sottocampo dei `Other` dettagli.

Esempio

```
"Tags": {
  "billingCode": "Lotus-1-2-3",
  "needsPatching": "true"
}
```

Type

Il tipo di risorsa per cui stai fornendo i dettagli.

Quando possibile, utilizza uno dei tipi di risorse forniti, ad esempio `AwsEc2Instance` o `AwsS3Bucket`.

Se il tipo di risorsa non corrisponde a nessuno dei tipi di risorsa forniti, imposta la risorsa `Type` su e utilizza il sottocampo dei `Other` dettagli per compilare i dettagli. `Other`

[I valori supportati sono elencati in Risorse.](#)

Esempio

```
"Type": "AwsS3Bucket"
```

AwsAmazonMQ

Di seguito sono riportati alcuni esempi del AWS Security Finding Format (ASFF) per le `AwsAmazonMQ` risorse.

AwsAmazonMQBroker

`AwsAmazonMQBroker` fornisce informazioni su un broker Amazon MQ, che è un ambiente di broker di messaggi in esecuzione su Amazon MQ.

L'esempio seguente mostra l'ASFF per l'`AwsAmazonMQBroker` oggetto. Per visualizzare le descrizioni degli `AwsAmazonMQBroker` attributi, consulta [AwsAmazonMQBroker](#) nel riferimento AWS Security Hub API.

Esempio

```
"AwsAmazonMQBroker": {
  "AutoMinorVersionUpgrade": true,
  "BrokerArn": "arn:aws:mq:us-east-1:123456789012:broker:TestBroker:b-
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "BrokerId": "b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "BrokerName": "TestBroker",
  "Configuration": {
    "Id": "c-a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "Revision": 1
  },
  "DeploymentMode": "ACTIVE_STANDBY_MULTI_AZ",
  "EncryptionOptions": {
    "UseAwsOwnedKey": true
  },
  "EngineType": "ActiveMQ",
  "EngineVersion": "5.17.2",
  "HostInstanceType": "mq.t2.micro",
  "Logs": {
    "Audit": false,
    "AuditLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-EXAMPLE11111/
audit",
    "General": false,
    "GeneralLogGroup": "/aws/amazonmq/broker/b-a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111/general"
  },
  "MaintenanceWindowStartTime": {
    "DayOfWeek": "MONDAY",
    "TimeOfDay": "22:00",
    "TimeZone": "UTC"
  },
  "PubliclyAccessible": true,
  "SecurityGroups": [
    "sg-021345abcdef6789"
  ],
  "StorageType": "efs",
  "SubnetIds": [
    "subnet-1234567890abcdef0",
    "subnet-abcdef01234567890"
  ],
  "Users": [
    {
      "Username": "admin"
    }
  ]
}
```

```
    }  
  ]  
}
```

AwsApiGateway

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsApiGateway` risorse.

AwsApiGatewayRestApi

L'`AwsApiGatewayRestApi` oggetto contiene informazioni su un'API REST nella versione 1 di Amazon API Gateway.

Di seguito è riportato un esempio di `AwsApiGatewayRestApi` ricerca nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayRestApi` attributi, consulta [AwsApiGatewayRestApiDetails](#) l'AWS Security Hub API Reference.

Esempio

```
AwsApiGatewayRestApi: {  
  "Id": "exampleapi",  
  "Name": "Security Hub",  
  "Description": "AWS Security Hub",  
  "CreatedDate": "2018-11-18T10:20:05-08:00",  
  "Version": "2018-10-26",  
  "BinaryMediaTypes" : ["-'*~1*"],  
  "MinimumCompressionSize": 1024,  
  "ApiKeySource": "AWS_ACCOUNT_ID",  
  "EndpointConfiguration": {  
    "Types": [  
      "REGIONAL"  
    ]  
  }  
}
```

AwsApiGatewayStage

L'`AwsApiGatewayStage` oggetto fornisce informazioni su una fase di Amazon API Gateway versione 1.

Di seguito è riportato un esempio di `AwsApiGatewayStage` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayStage` attributi, consulta [AwsApiGatewayStageDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsApiGatewayStage": {
  "DeploymentId": "n7h1mf",
  "ClientCertificateId": "a1b2c3",
  "StageName": "Prod",
  "Description": "Stage Description",
  "CacheClusterEnabled": false,
  "CacheClusterSize": "1.6",
  "CacheClusterStatus": "NOT_AVAILABLE",
  "MethodSettings": [
    {
      "MetricsEnabled": true,
      "LoggingLevel": "INFO",
      "DataTraceEnabled": false,
      "ThrottlingBurstLimit": 100,
      "ThrottlingRateLimit": 5.0,
      "CachingEnabled": false,
      "CacheTtlInSeconds": 300,
      "CacheDataEncrypted": false,
      "RequireAuthorizationForCacheControl": true,
      "UnauthorizedCacheControlHeaderStrategy": "SUCCEED_WITH_RESPONSE_HEADER",
      "HttpMethod": "POST",
      "ResourcePath": "/echo"
    }
  ],
  "Variables": {"test": "value"},
  "DocumentationVersion": "2.0",
  "AccessLogSettings": {
    "Format": "{\"requestId\": \"${context.requestId}\", \"extendedRequestId\": \"${context.extendedRequestId}\", \"ownerAccountId\": \"${context.accountId}\", \"requestAccountId\": \"${context.identity.accountId}\", \"callerPrincipal\": \"${context.identity.caller}\", \"httpMethod\": \"${context.httpMethod}\", \"resourcePath\": \"${context.resourcePath}\", \"status\": \"${context.status}\", \"requestTime\": \"${context.requestTime}\", \"responseLatencyMs\": \"${context.responseLatency}\", \"errorMessage\": \"${context.error.message}\", \"errorResponseType\": \"${context.error.responseType}\", \"apiId\": \"${context.apiId}\", \"awsEndpointRequestId\": \"${context.awsEndpointRequestId}\", \"domainName\": \"${context.domainName}\", \"stage\": \"${context.stage}\", \"xrayTraceId\": \"${context.xrayTraceId}\", \"sourceIp\": \"
```

```

  \"\$context.identity.sourceIp\", \"user\": \"\$context.identity.user\", \"userAgent
\": \"\$context.identity.userAgent\", \"userArn\": \"\$context.identity.userArn\",
  \"integrationLatency\": \"\$context.integrationLatency\", \"integrationStatus
\": \"\$context.integrationStatus\", \"authorizerIntegrationLatency\":
  \"\$context.authorizer.integrationLatency\" }\",
    \"DestinationArn\": \"arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod\"
  },
  \"CanarySettings\": {
    \"PercentTraffic\": 0.0,
    \"DeploymentId\": \"ul73s8\",
    \"StageVariable0verrides\" : [
      \"String\" : \"String\"
    ],
    \"UseStageCache\": false
  },
  \"TracingEnabled\": false,
  \"CreatedDate\": \"2018-07-11T10:55:18-07:00\",
  \"LastUpdatedDate\": \"2020-08-26T11:51:04-07:00\",
  \"WebAclArn\" : \"arn:aws:waf-regional:us-west-2:111122223333:webacl/
cb606bd8-5b0b-4f0b-830a-dd304e48a822\"
}

```

AwsApiGatewayV2Api

L'AwsApiGatewayV2Api oggetto contiene informazioni su un'API versione 2 in Amazon API Gateway.

Di seguito è riportato un esempio di AwsApiGatewayV2Api ricerca nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli AwsApiGatewayV2Api attributi, vedere [AwsApiGatewayV2 ApiDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

\"AwsApiGatewayV2Api\": {
  \"ApiEndpoint\": \"https://example.us-west-2.amazonaws.com\",
  \"ApiId\": \"a1b2c3d4\",
  \"ApiKeySelectionExpression\": \"\$request.header.x-api-key\",
  \"CreatedDate\": \"2020-03-28T00:32:37Z\",
  \"Description\": \"ApiGatewayV2 Api\",
  \"Version\": \"string\",
  \"Name\": \"my-api\",
  \"ProtocolType\": \"HTTP\",

```



```

    "RouteSelectionExpression": "$request.method $request.path",
  "CorsConfiguration": {
    "AllowOrigins": [ "*" ],
    "AllowCredentials": true,
    "ExposeHeaders": [ "string" ],
    "MaxAge": 3000,
    "AllowMethods": [
      "GET",
      "PUT",
      "POST",
      "DELETE",
      "HEAD"
    ],
    "AllowHeaders": [ "*" ]
  }
}

```

AwsApiGatewayV2 Stage

`AwsApiGatewayV2Stage` contiene informazioni sulla versione 2 (fase) per Amazon API Gateway.

Di seguito è riportato un esempio di `AwsApiGatewayV2Stage` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayV2Stage` attributi, vedere [AwsApiGatewayV2 StageDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

"AwsApiGatewayV2Stage": {
  "CreateDate": "2020-04-08T00:36:05Z",
  "Description": "ApiGatewayV2",
  "DefaultRouteSettings": {
    "DetailedMetricsEnabled": false,
    "LoggingLevel": "INFO",
    "DataTraceEnabled": true,
    "ThrottlingBurstLimit": 100,
    "ThrottlingRateLimit": 50
  },
  "DeploymentId": "x1zwyv",
  "LastUpdatedDate": "2020-04-08T00:36:13Z",
  "RouteSettings": {
    "DetailedMetricsEnabled": false,
    "LoggingLevel": "INFO",
    "DataTraceEnabled": true,

```

```

    "ThrottlingBurstLimit": 100,
    "ThrottlingRateLimit": 50
  },
  "StageName": "prod",
  "StageVariables": [
    "function": "my-prod-function"
  ],
  "AccessLogSettings": {
    "Format": "{\"requestId\": \"${context.requestId}\", \"extendedRequestId
\": \"${context.extendedRequestId}\", \"ownerAccountId\": \"${context.accountId}\",
  \"requestAccountId\": \"${context.identity.accountId}\", \"callerPrincipal\":
  \"${context.identity.caller}\", \"httpMethod\": \"${context.httpMethod}\", \"resourcePath
\": \"${context.resourcePath}\", \"status\": \"${context.status}\", \"requestTime
\": \"${context.requestTime}\", \"responseLatencyMs\": \"${context.responseLatency
}\", \"errorMessage\": \"${context.error.message}\", \"errorResponseType\":
  \"${context.error.responseType}\", \"apiId\": \"${context.apiId}\", \"awsEndpointRequestId
\": \"${context.awsEndpointRequestId}\", \"domainName\": \"${context.domainName}\", \"stage
\": \"${context.stage}\", \"xrayTraceId\": \"${context.xrayTraceId}\", \"sourceIp\":
  \"${context.identity.sourceIp}\", \"user\": \"${context.identity.user}\", \"userAgent
\": \"${context.identity.userAgent}\", \"userArn\": \"${context.identity.userArn}\",
  \"integrationLatency\": \"${context.integrationLatency}\", \"integrationStatus
\": \"${context.integrationStatus}\", \"authorizerIntegrationLatency\":
  \"${context.authorizer.integrationLatency}\" }",
    "DestinationArn": "arn:aws:logs:us-west-2:111122223333:log-
group:SecurityHubAPIAccessLog/Prod"
  },
  "AutoDeploy": false,
  "LastDeploymentStatusMessage": "Message",
  "ApiGatewayManaged": true,
}

```

AwsAppSync

Di seguito sono riportati alcuni esempi del AWS Security Finding Format (ASFF) per le AwsAppSync risorse.

AwsAppSyncGraphQLApi

AwsAppSyncGraphQLApi fornisce informazioni su un'API AWS AppSync GraphQL, che è un costruito di primo livello per l'applicazione.

L'esempio seguente mostra l'ASFF per l'oggetto. `AwsAppSyncGraphQLApi`. Per visualizzare le descrizioni degli `AwsAppSyncGraphQLApi` attributi, vedere [AwsAppSyncGraphQLApi nell'API Reference](#). AWS Security Hub

Esempio

```
"AwsAppSyncGraphQLApi": {
  "AdditionalAuthenticationProviders": [
    {
      "AuthenticationType": "AWS_LAMBDA",
      "LambdaAuthorizerConfig": {
        "AuthorizerResultTtlInSeconds": 300,
        "AuthorizerUri": "arn:aws:lambda:us-east-1:123456789012:function:mylambdafunc"
      }
    },
    {
      "AuthenticationType": "AWS_IAM"
    }
  ],
  "ApiId": "021345abcdef6789",
  "Arn": "arn:aws:appsync:eu-central-1:123456789012:apis/021345abcdef6789",
  "AuthenticationType": "API_KEY",
  "Id": "021345abcdef6789",
  "LogConfig": {
    "CloudWatchLogsRoleArn": "arn:aws:iam::123456789012:role/service-role/appsync-graphqlapi-logs-eu-central-1",
    "ExcludeVerboseContent": true,
    "FieldLogLevel": "ALL"
  },
  "Name": "My AppSync App",
  "XrayEnabled": true,
}
```

AwsAthena

Di seguito sono riportati alcuni esempi del AWS Security Finding Format (ASFF) per le `AwsAthena` risorse.

AwsAthenaWorkGroup

`AwsAthenaWorkGroup` fornisce informazioni su un gruppo di lavoro Amazon Athena. Un gruppo di lavoro ti aiuta a separare utenti, team, applicazioni o carichi di lavoro. Inoltre, consente di impostare limiti all'elaborazione dei dati e tenere traccia dei costi.

L'esempio seguente mostra l'ASFF per l'`AwsAthenaWorkGroup` oggetto. Per visualizzare le descrizioni degli `AwsAthenaWorkGroup` attributi, consulta [AwsAthenaWorkGroup](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsAthenaWorkGroup": {
  "Description": "My workgroup for prod workloads",
  "Name": "MyWorkgroup",
  "WorkgroupConfiguration" {
    "ResultConfiguration": {
      "EncryptionConfiguration": {
        "EncryptionOption": "SSE_KMS",
        "KmsKey": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-
cdef-EXAMPLE11111"
      }
    }
  },
  "State": "ENABLED"
}
```

AwsAutoScaling

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsAutoScaling` risorse.

AwsAutoScalingAutoScalingGroup

L'`AwsAutoScalingAutoScalingGroup` oggetto fornisce dettagli su un gruppo di ridimensionamento automatico.

Di seguito è riportato un esempio di `AwsAutoScalingAutoScalingGroup` ricerca nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsAutoScalingAutoScalingGroup` attributi, consulta [AwsAutoScalingAutoScalingGroupDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsAutoScalingAutoScalingGroup": {
  "CreatedTime": "2017-10-17T14:47:11Z",
  "HealthCheckGracePeriod": 300,
  "HealthCheckType": "EC2",
```

```

    "LaunchConfigurationName": "mylaunchconf",
    "LoadBalancerNames": [],
    "LaunchTemplate": {
      "LaunchTemplateId": "string",
      "LaunchTemplateName": "string",
      "Version": "string"
    },
    "MixedInstancesPolicy": {
      "InstancesDistribution": {
        "OnDemandAllocationStrategy": "prioritized",
        "OnDemandBaseCapacity": number,
        "OnDemandPercentageAboveBaseCapacity": number,
        "SpotAllocationStrategy": "lowest-price",
        "SpotInstancePools": number,
        "SpotMaxPrice": "string"
      },
      "LaunchTemplate": {
        "LaunchTemplateSpecification": {
          "LaunchTemplateId": "string",
          "LaunchTemplateName": "string",
          "Version": "string"
        },
        "CapacityRebalance": true,
        "Overrides": [
          {
            "InstanceType": "string",
            "WeightedCapacity": "string"
          }
        ]
      }
    }
  }
}

```

AwsAutoScalingLaunchConfiguration

L'AwsAutoScalingLaunchConfiguration oggetto fornisce dettagli sulla configurazione di avvio.

Di seguito è riportato un esempio di AwsAutoScalingLaunchConfiguration ricerca nel AWS Security Finding Format (ASFF).

Per visualizzare le descrizioni degli AwsAutoScalingLaunchConfiguration attributi, consulta [AwsAutoScalingLaunchConfigurationDetails](#) l'AWS Security Hub API Reference.

Esempio

```
AwsAutoScalingLaunchConfiguration: {
  "LaunchConfigurationName": "newtest",
  "ImageId": "ami-058a3739b02263842",
  "KeyName": "55hundredinstance",
  "SecurityGroups": [ "sg-01fce87ad6e019725" ],
  "ClassicLinkVpcSecurityGroups": [],
  "UserData": "...Base64-Encoded user data..."
  "InstanceType": "a1.metal",
  "KernelId": "",
  "RamdiskId": "ari-a51cf9cc",
  "BlockDeviceMappings": [
    {
      "DeviceName": "/dev/sdh",
      "Ebs": {
        "VolumeSize": 30,
        "VolumeType": "gp2",
        "DeleteOnTermination": false,
        "Encrypted": true,
        "SnapshotId": "snap-ffaa1e69",
        "VirtualName": "ephemeral1"
      }
    },
    {
      "DeviceName": "/dev/sdb",
      "NoDevice": true
    },
    {
      "DeviceName": "/dev/sda1",
      "Ebs": {
        "SnapshotId": "snap-02420cd3d2dea1bc0",
        "VolumeSize": 8,
        "VolumeType": "gp2",
        "DeleteOnTermination": true,
        "Encrypted": false
      }
    },
    {
      "DeviceName": "/dev/sdi",
      "Ebs": {
        "VolumeSize": 20,
        "VolumeType": "gp2",
        "DeleteOnTermination": false,
```

```

        "Encrypted": true
      }
    },
    {
      "DeviceName": "/dev/sdc",
      "NoDevice": true
    }
  ],
  "InstanceMonitoring": {
    "Enabled": false
  },
  "CreatedTime": 1620842933453,
  "EbsOptimized": false,
  "AssociatePublicIpAddress": true,
  "SpotPrice": "0.045"
}

```

AwsBackup

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsBackup risorse.

AwsBackupBackupPlan

L'AwsBackupBackupPlanoggetto fornisce informazioni su un piano AWS Backup di backup. Un piano di AWS Backup backup è un'espressione politica che definisce quando e come si desidera eseguire il backup AWS delle risorse.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsBackupBackupPlanoggetto. Per visualizzare le descrizioni degli AwsBackupBackupPlan attributi, consulta [AwsBackupBackupPlan](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsBackupBackupPlan": {
  "BackupPlan": {
    "AdvancedBackupSettings": [{
      "BackupOptions": {
        "WindowsVSS": "enabled"
      },
      "ResourceType": "EC2"
    }],
    "BackupPlanName": "test",
    "BackupPlanRule": [{

```

```

    "CompletionWindowMinutes": 10080,
    "CopyActions": [{
      "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
      "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
      }
    }],
    "Lifecycle": {
      "DeleteAfterDays": 35
    },
    "RuleName": "DailyBackups",
    "ScheduleExpression": "cron(0 5 ? * * *)",
    "StartWindowMinutes": 480,
    "TargetBackupVault": "Default"
  },
  {
    "CompletionWindowMinutes": 10080,
    "CopyActions": [{
      "DestinationBackupVaultArn": "arn:aws:backup:us-east-1:858726136373:backup-
vault:aws/efs/automatic-backup-vault",
      "Lifecycle": {
        "DeleteAfterDays": 365,
        "MoveToColdStorageAfterDays": 30
      }
    }],
    "Lifecycle": {
      "DeleteAfterDays": 35
    },
    "RuleName": "Monthly",
    "ScheduleExpression": "cron(0 5 1 * ? *)",
    "StartWindowMinutes": 480,
    "TargetBackupVault": "Default"
  }
],
"BackupPlanArn": "arn:aws:backup:us-east-1:858726136373:backup-
plan:b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
"BackupPlanId": "b6d6b896-590d-4ee1-bf29-c5ccae63f4e7",
"VersionId": "ZDVjNDIzMjItYTZiNS00NzgzLTg4YzctNmExMWM2NjZhY2E1"
}

```


AwsBackupBackupVault

L'AwsBackupBackupVault oggetto fornisce informazioni su un archivio AWS Backup di backup. Un archivio AWS Backup di backup è un contenitore che archivia e organizza i backup.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

AwsBackupBackupVault Per visualizzare le descrizioni degli AwsBackupBackupVault attributi, consulta [AwsBackupBackupVault](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsBackupBackupVault": {
  "AccessPolicy": {
    "Statement": [{
      "Action": [
        "backup:DeleteBackupVault",
        "backup:DeleteBackupVaultAccessPolicy",
        "backup:DeleteRecoveryPoint",
        "backup:StartCopyJob",
        "backup:StartRestoreJob",
        "backup:UpdateRecoveryPointLifecycle"
      ],
      "Effect": "Deny",
      "Principal": {
        "AWS": "*"
      },
      "Resource": "*"
    }],
    "Version": "2012-10-17"
  },
  "BackupVaultArn": "arn:aws:backup:us-east-1:123456789012:backup-vault:aws/efs/automatic-backup-vault",
  "BackupVaultName": "aws/efs/automatic-backup-vault",
  "EncryptionKeyArn": "arn:aws:kms:us-east-1:444455556666:key/72ba68d4-5e43-40b0-ba38-838bf8d06ca0",
  "Notifications": {
    "BackupVaultEvents": ["BACKUP_JOB_STARTED", "BACKUP_JOB_COMPLETED", "COPY_JOB_STARTED"],
    "SNSTopicArn": "arn:aws:sns:us-west-2:111122223333:MyVaultTopic"
  }
}
```

AwsBackupRecoveryPoint

L'AwsBackupRecoveryPointoggetto fornisce informazioni su un AWS Backup backup, noto anche come punto di ripristino. Un punto di AWS Backup ripristino rappresenta il contenuto di una risorsa in un momento specifico.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsBackupRecoveryPointoggetto. Per visualizzare le descrizioni degli AwsBackupBackupVault attributi, consulta [AwsBackupRecoveryPoint](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsBackupRecoveryPoint": {
  "BackupSizeInBytes": 0,
  "BackupVaultName": "aws/efs/automatic-backup-vault",
  "BackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/efs/automatic-backup-vault",
  "CalculatedLifecycle": {
    "DeleteAt": "2021-08-30T06:51:58.271Z",
    "MoveToColdStorageAt": "2020-08-10T06:51:58.271Z"
  },
  "CompletionDate": "2021-07-26T07:21:40.361Z",
  "CreatedBy": {
    "BackupPlanArn": "arn:aws:backup:us-east-1:111122223333:backup-plan:aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
    "BackupPlanId": "aws/efs/73d922fb-9312-3a70-99c3-e69367f9fdad",
    "BackupPlanVersion": "ZGM4YzY5YjktMWYxNC00ZTBmLWE5MjYtZmU5OWNiZmM5ZjIz",
    "BackupRuleId": "2a600c2-42ad-4196-808e-084923ebfd25"
  },
  "CreationDate": "2021-07-26T06:51:58.271Z",
  "EncryptionKeyArn": "arn:aws:kms:us-east-1:111122223333:key/72ba68d4-5e43-40b0-ba38-838bf8d06ca0",
  "IamRoleArn": "arn:aws:iam::111122223333:role/aws-service-role/backup.amazonaws.com/AWSServiceRoleForBackup",
  "IsEncrypted": true,
  "LastRestoreTime": "2021-07-26T06:51:58.271Z",
  "Lifecycle": {
    "DeleteAfterDays": 35,
    "MoveToColdStorageAfterDays": 15
  },
  "RecoveryPointArn": "arn:aws:backup:us-east-1:111122223333:recovery-point:151a59e4-f1d5-4587-a7fd-0774c6e91268",
```

```

    "ResourceArn": "arn:aws:elasticfilesystem:us-east-1:858726136373:file-system/
fs-15bd31a1",
    "ResourceType": "EFS",
    "SourceBackupVaultArn": "arn:aws:backup:us-east-1:111122223333:backup-vault:aws/
efs/automatic-backup-vault",
    "Status": "COMPLETED",
    "StatusMessage": "Failure message",
    "StorageClass": "WARM"
}

```

AwsCertificateManager

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsCertificateManager` risorse.

AwsCertificateManagerCertificate

L'`AwsCertificateManagerCertificate` oggetto fornisce dettagli su un certificato AWS Certificate Manager (ACM).

Di seguito è riportato un esempio di `AwsCertificateManagerCertificate` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsCertificateManagerCertificate` attributi, consulta [AwsCertificateManagerCertificateDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsCertificateManagerCertificate": {
  "CertificateAuthorityArn": "arn:aws:acm:us-west-2:444455556666:certificate-
authority/example",
  "CreatedAt": "2019-05-24T18:12:02.000Z",
  "DomainName": "example.amazondomains.com",
  "DomainValidationOptions": [
    {
      "DomainName": "example.amazondomains.com",
      "ResourceRecord": {
        "Name": "_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
        "Type": "CNAME",
        "Value": "_example.acm-validations.aws."
      },
      "ValidationDomain": "example.amazondomains.com",
      "ValidationEmails": [sample_email@sample.com],
      "ValidationMethod": "DNS",

```

```

        "ValidationStatus": "SUCCESS"
    }
],
"ExtendedKeyUsages": [
    {
        "Name": "TLS_WEB_SERVER_AUTHENTICATION",
        "Oid": "1.3.6.1.5.5.7.3.1"
    },
    {
        "Name": "TLS_WEB_CLIENT_AUTHENTICATION",
        "Oid": "1.3.6.1.5.5.7.3.2"
    }
],
"FailureReason": "",
"ImportedAt": "2018-08-17T00:13:00.000Z",
"InUseBy": ["arn:aws:amazondomains:us-west-2:444455556666:loadbalancer/example"],
"IssuedAt": "2020-04-26T00:41:17.000Z",
"Issuer": "Amazon",
"KeyAlgorithm": "RSA-1024",
"KeyUsages": [
    {
        "Name": "DIGITAL_SIGNATURE",
    },
    {
        "Name": "KEY_ENCIPHERMENT",
    }
],
"NotAfter": "2021-05-26T12:00:00.000Z",
"NotBefore": "2020-04-26T00:00:00.000Z",
"Options": {
    "CertificateTransparencyLoggingPreference": "ENABLED",
}
"RenewalEligibility": "ELIGIBLE",
"RenewalSummary": {
    "DomainValidationOptions": [
        {
            "DomainName": "example.amazondomains.com",
            "ResourceRecord": {
                "Name":
"_1bacb61828d3a1020c40a560ceed08f7.example.amazondomains.com",
                "Type": "CNAME",
                "Value": "_example.acm-validations.aws.com",
            },
            "ValidationDomain": "example.amazondomains.com",
        }
    ]
}

```

```

        "ValidationEmails": ["sample_email@sample.com"],
        "ValidationMethod": "DNS",
        "ValidationStatus": "SUCCESS"
    }
],
"RenewalStatus": "SUCCESS",
"RenewalStatusReason": "",
"UpdatedAt": "2020-04-26T00:41:35.000Z",
},
"Serial": "02:ac:86:b6:07:2f:0a:61:0e:3a:ac:fd:d9:ab:17:1a",
"SignatureAlgorithm": "SHA256WITHRSA",
>Status": "ISSUED",
"Subject": "CN=example.amazondomains.com",
"SubjectAlternativeNames": ["example.amazondomains.com"],
>Type": "AMAZON_ISSUED"
}

```

AwsCloudFormation

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsCloudFormation risorse.

AwsCloudFormationStack

L'AwsCloudFormationStackoggetto fornisce dettagli su uno AWS CloudFormation stack annidato come risorsa in un modello di primo livello.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

AwsCloudFormationStack Per visualizzare le descrizioni degli AwsCloudFormationStack attributi, consulta [AwsCloudFormationStackDetails](#)!AWS Security Hub API Reference.

Esempio

```

"AwsCloudFormationStack": {
  "Capabilities": [
    "CAPABILITY_IAM",
    "CAPABILITY_NAMED_IAM"
  ],
  "CreationTime": "2022-02-18T15:31:53.161Z",
  "Description": "AWS CloudFormation Sample",
  "DisableRollback": true,
  "DriftInformation": {
    "StackDriftStatus": "DRIFTED"
  }
}

```

```

},
"EnableTerminationProtection": false,
"LastUpdatedTime": "2022-02-18T15:31:53.161Z",
"NotificationArns": [
  "arn:aws:sns:us-east-1:978084797471:sample-sns-cfn"
],
"Outputs": [{
  "Description": "URL for newly created LAMP stack",
  "OutputKey": "WebsiteUrl",
  "OutputValue": "http://ec2-44-193-18-241.compute-1.amazonaws.com"
}],
"RoleArn": "arn:aws:iam::012345678910:role/exampleRole",
"StackId": "arn:aws:cloudformation:us-east-1:978084797471:stack/sample-stack/
e5d9f7e0-90cf-11ec-88c6-12ac1f91724b",
"StackName": "sample-stack",
"StackStatus": "CREATE_COMPLETE",
"StackStatusReason": "Success",
"TimeoutInMinutes": 1
}

```

AwsCloudFront

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsCloudFront risorse.

AwsCloudFrontDistribution

L'AwsCloudFrontDistribution oggetto fornisce dettagli su una configurazione di CloudFront distribuzione Amazon.

Di seguito è riportato un esempio di AwsCloudFrontDistribution ricerca nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli AwsCloudFrontDistribution attributi, consulta [AwsCloudFrontDistributionDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsCloudFrontDistribution": {
  "CacheBehaviors": {
    "Items": [
      {
        "ViewerProtocolPolicy": "https-only"
      }
    ]
  }
}

```

```
},
"DefaultCacheBehavior": {
  "ViewerProtocolPolicy": "https-only"
},
"DefaultRootObject": "index.html",
"DomainName": "d2wkuj2w9l34gt.cloudfront.net",
"Etag": "E37HOT42DHPVYH",
"LastModifiedTime": "2015-08-31T21:11:29.093Z",
"Logging": {
  "Bucket": "myawslogbucket.s3.amazonaws.com",
  "Enabled": false,
  "IncludeCookies": false,
  "Prefix": "myawslog/"
},
"OriginGroups": {
  "Items": [
    {
      "FailoverCriteria": {
        "StatusCodes": {
          "Items": [
            200,
            301,
            404
          ]
        }
      }
    }
  ]
},
"Origins": {
  "Items": [
    {
      "CustomOriginConfig": {
        "HttpPort": 80,
        "HttpsPort": 443,
        "OriginKeepaliveTimeout": 60,
        "OriginProtocolPolicy": "match-viewer",
        "OriginReadTimeout": 30,
        "OriginSslProtocols": {
          "Items": ["SSLv3", "TLSv1"],
          "Quantity": 2
        }
      }
    }
  ]
}
```

```

    },
  ],
},
  "DomainName": "my-bucket.s3.amazonaws.com",
  "Id": "my-origin",
  "OriginPath": "/production",
  "S3OriginConfig": {
    "OriginAccessIdentity": "origin-access-identity/cloudfront/
E2YFS67H6VB6E4"
  }
],
},
"Status": "Deployed",
"ViewerCertificate": {
  "AcmCertificateArn": "arn:aws:acm::123456789012:AcmCertificateArn",
  "Certificate": "ASCAJRRE5XYF52TKRY5M4",
  "CertificateSource": "iam",
  "CloudFrontDefaultCertificate": true,
  "IamCertificateId": "ASCAJRRE5XYF52TKRY5M4",
  "MinimumProtocolVersion": "TLSv1.2_2021",
  "SslSupportMethod": "sni-only"
},
"WebAclId": "waf-1234567890"
}

```

AwsCloudTrail

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsCloudTrail` risorse.

AwsCloudTrailTrail

L'`AwsCloudTrailTrail` oggetto fornisce dettagli su un AWS CloudTrail percorso.

Di seguito è riportato un esempio di `AwsCloudTrailTrail` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsCloudTrailTrail` attributi, consulta [AwsCloudTrailTrailDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsCloudTrailTrail": {
  "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-west-2:123456789012:log-
group:CloudTrail/regression:*",

```



```

    "CloudWatchLogsRoleArn": "arn:aws:iam::866482105055:role/
CloudTrail_CloudWatchLogs",
    "HasCustomEventSelectors": true,
    "HomeRegion": "us-west-2",
    "IncludeGlobalServiceEvents": true,
    "IsMultiRegionTrail": true,
    "IsOrganizationTrail": false,
    "KmsKeyId": "kmsKeyId",
    "LogFileValidationEnabled": true,
    "Name": "regression-trail",
    "S3BucketName": "cloudtrail-bucket",
    "S3KeyPrefix": "s3KeyPrefix",
    "SnsTopicArn": "arn:aws:sns:us-east-2:123456789012:MyTopic",
    "SnsTopicName": "snsTopicName",
    "TrailArn": "arn:aws:cloudtrail:us-west-2:123456789012:trail"
}

```

AwsCloudWatch

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsCloudWatch` risorse.

AwsCloudWatchAlarm

L'`AwsCloudWatchAlarm` oggetto fornisce dettagli sugli `CloudWatch` allarmi Amazon che controllano una metrica o eseguono un'azione quando un allarme cambia stato.

L'esempio seguente mostra il `AWS Security Finding Format (ASFF)` per l'oggetto.

`AwsCloudWatchAlarm` Per visualizzare le descrizioni degli `AwsCloudWatchAlarm` attributi, consulta [AwsCloudWatchAlarmDetails](#) l'`AWS Security Hub API Reference`.

Esempio

```

"AwsCloudWatchAlarm": {
  "ActonsEnabled": true,
  "AlarmActions": [
    "arn:aws:automate:region:ec2:stop",
    "arn:aws:automate:region:ec2:terminate"
  ],
  "AlarmArn": "arn:aws:cloudwatch:us-west-2:012345678910:alarm:sampleAlarm",
  "AlarmConfigurationUpdatedTimestamp": "2022-02-18T15:31:53.161Z",
  "AlarmDescription": "Alarm Example",
  "AlarmName": "Example",

```

```

"ComparisonOperator": "GreaterThanOrEqualToThreshold",
"DatapointsToAlarm": 1,
"Dimensions": [{
  "Name": "InstanceId",
  "Value": "i-1234567890abcdef0"
}],
"EvaluateLowSampleCountPercentile": "evaluate",
"EvaluationPeriods": 1,
"ExtendedStatistic": "p99.9",
"InsufficientDataActions": [
  "arn:aws:automate:region:ec2:stop"
],
"MetricName": "Sample Metric",
"Namespace": "YourNamespace",
"OkActions": [
  "arn:aws:swf:region:account-id:action/actions/AWS_EC2.InstanceId.Stop/1.0"
],
"Period": 1,
"Statistic": "SampleCount",
"Threshold": 12.3,
"ThresholdMetricId": "t1",
"TreatMissingData": "notBreaching",
"Unit": "Kilobytes/Second"
}

```

AwsCodeBuild

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsCodeBuild risorse.

AwsCodeBuildProject

L'oggetto `AwsCodeBuildProject` fornisce informazioni su un progetto AWS CodeBuild .

Di seguito è riportato un esempio di `AwsCodeBuildProject` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsCodeBuildProject` attributi, consulta [AwsCodeBuildProjectDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsCodeBuildProject": {
  "Artifacts": [
    {
      "ArtifactIdentifier": "string",

```

```
    "EncryptionDisabled": boolean,
    "Location": "string",
    "Name": "string",
    "NamespaceType": "string",
    "OverrideArtifactName": boolean,
    "Packaging": "string",
    "Path": "string",
    "Type": "string"
  }
],
"SecondaryArtifacts": [
  {
    "ArtifactIdentifier": "string",
    "EncryptionDisabled": boolean,
    "Location": "string",
    "Name": "string",
    "NamespaceType": "string",
    "OverrideArtifactName": boolean,
    "Packaging": "string",
    "Path": "string",
    "Type": "string"
  }
],
"EncryptionKey": "string",
"Certificate": "string",
"Environment": {
  "Certificate": "string",
  "EnvironmentVariables": [
    {
      "Name": "string",
      "Type": "string",
      "Value": "string"
    }
  ]
},
"ImagePullCredentialsType": "string",
"PrivilegedMode": boolean,
"RegistryCredential": {
  "Credential": "string",
  "CredentialProvider": "string"
},
"Type": "string"
},
"LogsConfig": {
  "CloudWatchLogs": {
```

```

        "GroupName": "string",
        "Status": "string",
        "StreamName": "string"
    },
    "S3Logs": {
        "EncryptionDisabled": boolean,
        "Location": "string",
        "Status": "string"
    }
},
"Name": "string",
"ServiceRole": "string",
"Source": {
    "Type": "string",
    "Location": "string",
    "GitCloneDepth": integer
},
"VpcConfig": {
    "VpcId": "string",
    "Subnets": ["string"],
    "SecurityGroupIds": ["string"]
}
}

```

AwsDms

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsDms risorse.

AwsDmsEndpoint

L'AwsDmsEndpoint oggetto fornisce informazioni su un endpoint AWS Database Migration Service (AWS DMS). Un endpoint fornisce informazioni sulla connessione, sul tipo di data store e sulla posizione del data store.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsDmsEndpoint oggetto. Per visualizzare le descrizioni degli AwsDmsEndpoint attributi, consulta [AwsDmsEndpointDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsDmsEndpoint": {
    "CertificateArn": "arn:aws:dms:us-
east-1:123456789012:cert:EXAMPLEIGDURVZGVJQZDPWJ5A7F2YDJVSMTBWF1",

```

```

    "DatabaseName": "Test",
    "EndpointArn": "arn:aws:dms:us-east-1:123456789012:endpoint:EXAMPLEQB3CZY33F7XV253NAJVBNPK6MJQVQVQA",
    "EndpointIdentifier": "target-db",
    "EndpointType": "TARGET",
    "EngineName": "mariadb",
    "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "Port": 3306,
    "ServerName": "target-db.exampletafyu.us-east-1.rds.amazonaws.com",
    "SslMode": "verify-ca",
    "Username": "admin"
}

```

AwsDmsReplicationInstance

L'AwsDmsReplicationInstance oggetto fornisce informazioni su un'istanza di replica AWS Database Migration Service (AWS DMS). DMS utilizza un'istanza di replica per connettersi al data store di origine, leggere i dati di origine e formattare i dati per l'utilizzo da parte del data store di destinazione.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. AwsDmsReplicationInstance Per visualizzare le descrizioni degli AwsDmsReplicationInstance attributi, consulta [AwsDmsReplicationInstanceDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsDmsReplicationInstance": {
  "AllocatedStorage": 50,
  "AutoMinorVersionUpgrade": true,
  "AvailabilityZone": "us-east-1b",
  "EngineVersion": "3.5.1",
  "KmsKeyId": "arn:aws:kms:us-east-1:123456789012:key/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "MultiAZ": false,
  "PreferredMaintenanceWindow": "wed:08:08-wed:08:38",
  "PubliclyAccessible": true,
  "ReplicationInstanceClass": "dms.c5.xlarge",
  "ReplicationInstanceIdentifier": "second-replication-instance",
  "ReplicationSubnetGroup": {
    "ReplicationSubnetGroupIdentifier": "default-vpc-2344f44f"
  },
}

```

```

    "VpcSecurityGroups": [
      {
        "VpcSecurityGroupId": "sg-003a34e205138138b"
      }
    ]
  }

```

AwsDmsReplicationTask

L'oggetto `AwsDmsReplicationTask` fornisce informazioni su un'attività di replica AWS Database Migration Service (AWS DMS). Un'attività di replica sposta un set di dati dall'endpoint di origine all'endpoint di destinazione.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto `AwsDmsReplicationInstance`. Per visualizzare le descrizioni degli `AwsDmsReplicationInstance` attributi, consulta [AwsDmsReplicationInstance](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsDmsReplicationTask": {
  "CdcStartPosition": "2023-08-28T14:26:22",
  "Id": "arn:aws:dms:us-east-1:123456789012:task:YDYUOHZIXWKQSUCBMUCQCNY44SJW74VJNB5DFWQ",
  "MigrationType": "cdc",
  "ReplicationInstanceArn": "arn:aws:dms:us-east-1:123456789012:rep:T7V6RFDP23PYQWUL26N3PF5REKML4Y0UGIMYJUI",
  "ReplicationTaskIdentifier": "test-task",
  "ReplicationTaskSettings": "{\"Logging\":{\"EnableLogging\":false,
  \"EnableLogContext\":false, \"LogComponents\":[{\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"TRANSFORMATION\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"SOURCE_UNLOAD\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"IO\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"TARGET_LOAD\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"PERFORMANCE\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"SOURCE_CAPTURE\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"SORTER\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"REST_SERVER\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"VALIDATOR_EXT\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"TARGET_APPLY\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"TASK_MANAGER\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"TABLES_MANAGER\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"METADATA_MANAGER\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"FILE_FACTORY\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT\", \"Id\":\"COMMON\"}, {\"Severity\":\"LOGGER_SEVERITY_DEFAULT

```

```

\","Id\":"ADDONS\"}, {"Severity\":"LOGGER_SEVERITY_DEFAULT\","Id\":"DATA_STRUCTURE
\"}, {"Severity\":"LOGGER_SEVERITY_DEFAULT\","Id\":"COMMUNICATION\"}, {"Severity
\":"LOGGER_SEVERITY_DEFAULT\","Id\":"FILE_TRANSFER\"}], "CloudWatchLogGroup
\":"null","CloudWatchLogStream\":"null"}, {"StreamBufferSettings\":{"StreamBufferCount
\":"3","CtrlStreamBufferSizeInMB\":"5","StreamBufferSizeInMB\":"8"}, {"ErrorBehavior
\":{"FailOnNoTablesCaptured\":"true","ApplyErrorUpdatePolicy\":"LOG_ERROR",
"FailOnTransactionConsistencyBreached\":"false","RecoverableErrorThrottlingMax\":"1800,
"DataErrorEscalationPolicy\":"SUSPEND_TABLE","ApplyErrorEscalationCount\":"0,
"RecoverableErrorStopRetryAfterThrottlingMax\":"true","RecoverableErrorThrottling
\":"true","ApplyErrorFailOnTruncationDdl\":"false","DataTruncationErrorPolicy\":"
LOG_ERROR","ApplyErrorInsertPolicy\":"LOG_ERROR","EventErrorPolicy\":"
IGNORE","ApplyErrorEscalationPolicy\":"LOG_ERROR","RecoverableErrorCount
\":"-1","DataErrorEscalationCount\":"0","TableErrorEscalationPolicy\":"STOP_TASK
","RecoverableErrorInterval\":"5","ApplyErrorDeletePolicy\":"IGNORE_RECORD",
"TableErrorEscalationCount\":"0","FullLoadIgnoreConflicts\":"true","DataErrorPolicy
\":"LOG_ERROR","TableErrorPolicy\":"SUSPEND_TABLE"}, {"TTSettings
\":{"TTS3Settings\":"null","TTRRecordSettings\":"null","EnableTT\":"false"},
"FullLoadSettings\":{"CommitRate\":"10000","StopTaskCachedChangesApplied
\":"false","StopTaskCachedChangesNotApplied\":"false","MaxFullLoadSubTasks
\":"8","TransactionConsistencyTimeout\":"600","CreatePkAfterFullLoad\":"false,
"TargetTablePrepMode\":"DO_NOTHING"}, {"TargetMetadata\":{"ParallelApplyBufferSize
\":"0","ParallelApplyQueuesPerThread\":"0","ParallelApplyThreads\":"0","TargetSchema
\":"\","InlineLobMaxSize\":"0","ParallelLoadQueuesPerThread\":"0","SupportLobs
\":"true","LobChunkSize\":"64","TaskRecoveryTableEnabled\":"false","ParallelLoadThreads
\":"0","LobMaxSize\":"0","BatchApplyEnabled\":"false","FullLobMode\":"true,
"LimitedSizeLobMode\":"false","LoadMaxFileSize\":"0","ParallelLoadBufferSize\":"0},
"BeforeImageSettings\":"null","ControlTablesSettings\":{"historyTimeslotInMinutes
\":"5","HistoryTimeslotInMinutes\":"5","StatusTableEnabled\":"false,
"SuspendedTablesTableEnabled\":"false","HistoryTableEnabled\":"false","ControlSchema
\":"\","FullLoadExceptionTableEnabled\":"false"}, {"LoopbackPreventionSettings
\":"null","CharacterSetSettings\":"null","FailTaskWhenCleanTaskResourceFailed
\":"false","ChangeProcessingTuning\":{"StatementCacheSize\":"50","CommitTimeout
\":"1","BatchApplyPreserveTransaction\":"true","BatchApplyTimeoutMin\":"1,
"BatchSplitSize\":"0","BatchApplyTimeoutMax\":"30","MinTransactionSize\":"1000,
"MemoryKeepTime\":"60","BatchApplyMemoryLimit\":"500","MemoryLimitTotal\":"1024},
"ChangeProcessingDdlHandlingPolicy\":{"HandleSourceTableDropped\":"true,
"HandleSourceTableTruncated\":"true","HandleSourceTableAltered\":"true},
"PostProcessingRules\":"null}],
  "SourceEndpointArn": "arn:aws:dms:us-
east-1:123456789012:endpoint:TZPWV2VCXEGHYOKVKRNHAKJ4Q3RUXACNGFGYWRI",
  "TableMappings": [{"rules\":[{"rule-type\":"selection","rule-id\":"
969761702","rule-name\":"969761702","object-locator\":{"schema-name\":"%table
","table-name\":"%example"},"rule-action\":"exclude","filters\":[]}]}],

```

```
"TargetEndpointArn": "arn:aws:dms:us-east-1:123456789012:endpoint:ABR8LB0QB3CZY33F7XV253NAJVBNPK6MJQVQVQA"
}
```

AwsDynamoDB

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsDynamoDB risorse.

AwsDynamoDbTable

L'AwsDynamoDbTable oggetto fornisce dettagli su una tabella Amazon DynamoDB.

Di seguito è riportato un esempio di AwsDynamoDbTable ricerca nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli AwsDynamoDbTable attributi, consulta [AwsDynamoDbTableDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsDynamoDbTable": {
  "AttributeDefinitions": [
    {
      "AttributeName": "attribute1",
      "AttributeType": "value 1"
    },
    {
      "AttributeName": "attribute2",
      "AttributeType": "value 2"
    },
    {
      "AttributeName": "attribute3",
      "AttributeType": "value 3"
    }
  ],
  "BillingModeSummary": {
    "BillingMode": "PAY_PER_REQUEST",
    "LastUpdateToPayPerRequestDateTime": "2019-12-03T15:23:10.323Z"
  },
  "CreationDateTime": "2019-12-03T15:23:10.248Z",
  "DeletionProtectionEnabled": true,
  "GlobalSecondaryIndexes": [
    {
      "Backfilling": false,
```



```
    "IndexArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
index/exampleIndex",
    "IndexName": "standardsControlArnIndex",
    "IndexSizeBytes": 1862513,
    "IndexStatus": "ACTIVE",
    "ItemCount": 20,
    "KeySchema": [
      {
        "AttributeName": "City",
        "KeyType": "HASH"
      },
      {
        "AttributeName": "Date",
        "KeyType": "RANGE"
      }
    ],
    "Projection": {
      "NonKeyAttributes": ["predictorName"],
      "ProjectionType": "ALL"
    },
    "ProvisionedThroughput": {
      "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
      "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
      "NumberOfDecreasesToday": 0,
      "ReadCapacityUnits": 100,
      "WriteCapacityUnits": 50
    },
  },
],
"GlobalTableVersion": "V1",
"ItemCount": 2705,
"KeySchema": [
  {
    "AttributeName": "zipcode",
    "KeyType": "HASH"
  }
],
"LatestStreamArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/
stream/2019-12-03T23:23:10.248",
"LatestStreamLabel": "2019-12-03T23:23:10.248",
"LocalSecondaryIndexes": [
  {
    "IndexArn": "arn:aws:dynamodb:us-east-1:111122223333:table/exampleGroup/
index/exampleId",
```

```

    "IndexName": "CITY_DATE_INDEX_NAME",
    "KeySchema": [
      {
        "AttributeName": "zipcode",
        "KeyType": "HASH"
      }
    ],
    "Projection": {
      "NonKeyAttributes": ["predictorName"],
      "ProjectionType": "ALL"
    },
  }
],
"ProvisionedThroughput": {
  "LastIncreaseDateTime": "2019-03-14T13:21:00.399Z",
  "LastDecreaseDateTime": "2019-03-14T12:47:35.193Z",
  "NumberOfDecreasesToday": 0,
  "ReadCapacityUnits": 100,
  "WriteCapacityUnits": 50
},
"Replicas": [
  {
    "GlobalSecondaryIndexes": [
      {
        "IndexName": "CITY_DATE_INDEX_NAME",
        "ProvisionedThroughputOverride": {
          "ReadCapacityUnits": 10
        }
      }
    ],
    "KmsMasterKeyId" : "KmsKeyId"
    "ProvisionedThroughputOverride": {
      "ReadCapacityUnits": 10
    },
    "RegionName": "regionName",
    "ReplicaStatus": "CREATING",
    "ReplicaStatusDescription": "replicaStatusDescription"
  }
],
"RestoreSummary" : {
  "SourceBackupArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable/backup/backup1",
  "SourceTableArn": "arn:aws:dynamodb:us-west-2:111122223333:table/exampleTable",
  "RestoreDateTime": "2020-06-22T17:40:12.322Z",

```

```

    "RestoreInProgress": true
  },
  "SseDescription": {
    "InaccessibleEncryptionDateTime": "2018-01-26T23:50:05.000Z",
    "Status": "ENABLED",
    "SseType": "KMS",
    "KmsMasterKeyArn": "arn:aws:kms:us-east-1:111122223333:key/key1"
  },
  "StreamSpecification" : {
    "StreamEnabled": true,
    "StreamViewType": "NEW_IMAGE"
  },
  "TableId": "example-table-id-1",
  "TableName": "example-table",
  "TableSizeBytes": 1862513,
  "TableStatus": "ACTIVE"
}

```

AwsEc2

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsEc2 risorse.

AwsEc2ClientVpnEndpoint

L'AwsEc2ClientVpnEndpoint oggetto fornisce informazioni su un AWS Client VPN endpoint. Un endpoint Client VPN è la risorsa che crei e configuri per abilitare e gestire le sessioni VPN client. È il punto di chiusura per tutte le sessioni VPN client.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsEc2ClientVpnEndpoint oggetto. Per visualizzare le descrizioni degli AwsEc2ClientVpnEndpoint attributi, vedere [AwsEc2 ClientVpnEndpointDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

"AwsEc2ClientVpnEndpoint": {
  "AuthenticationOptions": [
    {
      "MutualAuthentication": {
        "ClientRootCertificateChainArn": "arn:aws:acm:us-east-1:123456789012:certificate/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "Type": "certificate-authentication"
    }
  ]
}

```

```

    }
  ],
  "ClientCidrBlock": "10.0.0.0/22",
  "ClientConnectOptions": {
    "Enabled": false
  },
  "ClientLoginBannerOptions": {
    "Enabled": false
  },
  "ClientVpnEndpointId": "cvpn-endpoint-00c5d11fc4729f2a5",
  "ConnectionLogOptions": {
    "Enabled": false
  },
  "Description": "test",
  "DnsServer": ["10.0.0.0"],
  "ServerCertificateArn": "arn:aws:acm:us-east-1:123456789012:certificate/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "SecurityGroupIdSet": [
    "sg-0f7a177b82b443691"
  ],
  "SelfServicePortalUrl": "https://self-service.clientvpn.amazonaws.com/endpoints/
cvpn-endpoint-00c5d11fc4729f2a5",
  "SessionTimeoutHours": 24,
  "SplitTunnel": false,
  "TransportProtocol": "udp",
  "VpcId": "vpc-1a2b3c4d5e6f1a2b3",
  "VpnPort": 443
}

```

AwsEc2Eip

L'AwsEc2Eipoggetto fornisce informazioni su un indirizzo IP elastico.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsEc2Eipoggetto. Per visualizzare le descrizioni degli AwsEc2Eip attributi, vedere [AwsEc2 EipDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

"AwsEc2Eip": {
  "InstanceId": "instance1",
  "PublicIp": "192.0.2.04",
  "AllocationId": "eipalloc-example-id-1",

```

```
"AssociationId": "eipassoc-example-id-1",
"Domain": "vpc",
"PublicIpv4Pool": "anycompany",
"NetworkBorderGroup": "eu-central-1",
"NetworkInterfaceId": "eni-example-id-1",
"NetworkInterfaceOwnerId": "777788889999",
"PrivateIpAddress": "192.0.2.03"
}
```

AwsEc2Instance

L'AwsEc2Instanceoggetto fornisce dettagli su un'istanza Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsEc2Instanceoggetto. Per visualizzare le descrizioni degli AwsEc2Instance attributi, vedere [AwsEc2 InstanceDetails](#) nell'AWS Security Hub API Reference.

Esempio

```
"AwsEc2Instance": {
  "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/AdminRole",
  "ImageId": "ami-1234",
  "IPv4Addresses": [ "1.1.1.1" ],
  "IPv6Addresses": [ "2001:db8:1234:1a2b::123" ],
  "KeyName": "my_keypair",
  "LaunchedAt": "2018-05-08T16:46:19.000Z",
  "MetadataOptions": {
    "HttpEndpoint": "enabled",
    "HttpProtocolIpv6": "enabled",
    "HttpPutResponseHopLimit": 1,
    "HttpTokens": "optional",
    "InstanceMetadataTags": "disabled",
  },
  "Monitoring": {
    "State": "disabled"
  },
  "NetworkInterfaces": [
    {
      "NetworkInterfaceId": "eni-e5aa89a3"
    }
  ],
  "SubnetId": "subnet-123",
  "Type": "i3.xlarge",
}
```

```
"VpcId": "vpc-123"
}
```

AwsEc2LaunchTemplate

L'AwsEc2LaunchTemplate oggetto contiene dettagli su un modello di lancio di Amazon Elastic Compute Cloud che specifica le informazioni di configurazione dell'istanza.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

AwsEc2LaunchTemplate Per visualizzare le descrizioni degli AwsEc2LaunchTemplate attributi, vedere [AwsEc2 LaunchTemplateDetails](#) nell'AWS Security Hub API Reference.

Esempio

```
"AwsEc2LaunchTemplate": {
  "DefaultVersionNumber": "1",
  "ElasticGpuSpecifications": ["string"],
  "ElasticInferenceAccelerators": ["string"],
  "Id": "lt-0a16e9802800bdd85",
  "ImageId": "ami-0d5eff06f840b45e9",
  "LatestVersionNumber": "1",
  "LaunchTemplateData": {
    "BlockDeviceMappings": [{
      "DeviceName": "/dev/xvda",
      "Ebs": {
        "DeleteonTermination": true,
        "Encrypted": true,
        "SnapshotId": "snap-01047646ec075f543",
        "VolumeSize": 8,
        "VolumeType": "gp2"
      }
    }
  ],
  "MetadataOptions": {
    "HttpTokens": "enabled",
    "HttpPutResponseHopLimit" : 1
  },
  "Monitoring": {
    "Enabled": true,
  },
  "NetworkInterfaces": [{
    "AssociatePublicIpAddress" : true,
  }],
  "LaunchTemplateName": "string",
  "LicenseSpecifications": ["string"],
```

```

"SecurityGroupIds": ["sg-01fce87ad6e019725"],
"SecurityGroups": ["string"],
"TagSpecifications": ["string"]
}

```

AwsEc2NetworkAcl

L'AwsEc2NetworkAcl oggetto contiene dettagli su una lista di controllo degli accessi alla rete (ACL) di Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

AwsEc2NetworkAcl Per visualizzare le descrizioni degli AwsEc2NetworkAcl attributi, vedere [AwsEc2 NetworkAclDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

"AwsEc2NetworkAcl": {
  "IsDefault": false,
  "NetworkAclId": "acl-1234567890abcdef0",
  "OwnerId": "123456789012",
  "VpcId": "vpc-1234abcd",
  "Associations": [{
    "NetworkAclAssociationId": "aclassoc-abcd1234",
    "NetworkAclId": "acl-021345abcdef6789",
    "SubnetId": "subnet-abcd1234"
  }],
  "Entries": [{
    "CidrBlock": "10.24.34.0/23",
    "Egress": true,
    "IcmpTypeCode": {
      "Code": 10,
      "Type": 30
    },
    "Ipv6CidrBlock": "2001:DB8::/32",
    "PortRange": {
      "From": 20,
      "To": 40
    },
    "Protocol": "tcp",
    "RuleAction": "allow",
    "RuleNumber": 100
  }
]
}

```

AwsEc2NetworkInterface

L'`AwsEc2NetworkInterface` oggetto fornisce informazioni su un'interfaccia di rete Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEc2NetworkInterface` oggetto. Per visualizzare le descrizioni degli `AwsEc2NetworkInterface` attributi, vedere [AwsEc2 NetworkInterfaceDetails](#) nell'AWS Security Hub API Reference.

Esempio

```
"AwsEc2NetworkInterface": {
  "Attachment": {
    "AttachTime": "2019-01-01T03:03:21Z",
    "AttachmentId": "eni-attach-43348162",
    "DeleteOnTermination": true,
    "DeviceIndex": 123,
    "InstanceId": "i-1234567890abcdef0",
    "InstanceOwnerId": "123456789012",
    "Status": 'ATTACHED'
  },
  "SecurityGroups": [
    {
      "GroupName": "my-security-group",
      "GroupId": "sg-903004f8"
    }
  ],
  "NetworkInterfaceId": 'eni-686ea200',
  "SourceDestCheck": false
}
```

AwsEc2RouteTable

L'`AwsEc2RouteTable` oggetto fornisce informazioni su una tabella di routing di Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEc2RouteTable` oggetto. Per visualizzare le descrizioni degli `AwsEc2RouteTable` attributi, vedere [AwsEc2 RouteTableDetails](#) nell'AWS Security Hub API Reference.

Esempio

```
"AwsEc2RouteTable": {
  "AssociationSet": [{
```



```

    "AssociationSet": {
      "State": "associated"
    },
    "Main": true,
    "RouteTableAssociationId": "rtbassoc-08e706c45de9f7512",
    "RouteTableId": "rtb-0a59bde9cf2548e34",
  ]],
  "PropogatingVgwSet": [],
  "RouteTableId": "rtb-0a59bde9cf2548e34",
  "RouteSet": [
    {
      "DestinationCidrBlock": "10.24.34.0/23",
      "GatewayId": "local",
      "Origin": "CreateRouteTable",
      "State": "active"
    },
    {
      "DestinationCidrBlock": "10.24.34.0/24",
      "GatewayId": "igw-0242c2d7d513fc5d3",
      "Origin": "CreateRoute",
      "State": "active"
    }
  ],
  "VpcId": "vpc-0c250a5c33f51d456"
}

```

AwsEc2SecurityGroup

L'AwsEc2SecurityGroupoggetto descrive un gruppo di sicurezza Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsEc2SecurityGroupoggetto. Per visualizzare le descrizioni degli AwsEc2SecurityGroup attributi, vedere [AwsEc2 SecurityGroupDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

"AwsEc2SecurityGroup": {
  "GroupName": "MySecurityGroup",
  "GroupId": "sg-903004f8",
  "OwnerId": "123456789012",
  "VpcId": "vpc-1a2b3c4d",
  "IpPermissions": [
    {

```

```

    "IpProtocol": "-1",
    "IpRanges": [],
    "UserIdGroupPairs": [
      {
        "UserId": "123456789012",
        "GroupId": "sg-903004f8"
      }
    ],
    "PrefixListIds": [
      {"PrefixListId": "pl-63a5400a"}
    ]
  },
  {
    "PrefixListIds": [],
    "FromPort": 22,
    "IpRanges": [
      {
        "CidrIp": "203.0.113.0/24"
      }
    ],
    "ToPort": 22,
    "IpProtocol": "tcp",
    "UserIdGroupPairs": []
  }
]
}

```

AwsEc2Subnet

L'AwsEc2Subnet oggetto fornisce informazioni su una sottorete in Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. AwsEc2Subnet. Per visualizzare le descrizioni degli AwsEc2Subnet attributi, vedere [AwsEc2 SubnetDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

AwsEc2Subnet: {
  "AssignIpv6AddressOnCreation": false,
  "AvailabilityZone": "us-west-2c",
  "AvailabilityZoneId": "usw2-az3",
  "AvailableIpAddressCount": 8185,
  "CidrBlock": "10.0.0.0/24",

```

```

    "DefaultForAz": false,
    "MapPublicIpOnLaunch": false,
    "OwnerId": "123456789012",
    "State": "available",
    "SubnetArn": "arn:aws:ec2:us-west-2:123456789012:subnet/subnet-d5436c93",
    "SubnetId": "subnet-d5436c93",
    "VpcId": "vpc-153ade70",
    "Ipv6CidrBlockAssociationSet": [{
      "AssociationId": "subnet-cidr-assoc-EXAMPLE",
      "Ipv6CidrBlock": "2001:DB8::/32",
      "CidrBlockState": "associated"
    }]
  }
}

```

AwsEc2TransitGateway

L'AwsEc2TransitGatewayoggetto fornisce dettagli su un gateway di transito Amazon EC2 che interconnette i cloud privati virtuali (VPC) e le reti locali.

Di seguito è riportato un esempio di AwsEc2TransitGateway risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli AwsEc2TransitGateway attributi, vedere [AwsEc2 TransitGatewayDetails](#) nel riferimento AWS Security Hub API.

Esempio

```

"AwsEc2TransitGateway": {
  "AmazonSideAsn": 65000,
  "AssociationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
  "AutoAcceptSharedAttachments": "disable",
  "DefaultRouteTableAssociation": "enable",
  "DefaultRouteTablePropagation": "enable",
  "Description": "sample transit gateway",
  "DnsSupport": "enable",
  "Id": "tgw-042ae6bf7a5c126c3",
  "MulticastSupport": "disable",
  "PropagationDefaultRouteTableId": "tgw-rtb-099ba47cbbea837cc",
  "TransitGatewayCidrBlocks": ["10.0.0.0/16"],
  "VpnEcmpSupport": "enable"
}

```

AwsEc2Volume

L'AwsEc2Volumeoggetto fornisce dettagli su un volume Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsEc2Volumeoggetto. Per visualizzare le descrizioni degli AwsEc2Volume attributi, vedere [AwsEc2 VolumeDetails](#) nell'AWS Security Hub API Reference.

Esempio

```
"AwsEc2Volume": {
  "Attachments": [
    {
      "AttachTime": "2017-10-17T14:47:11Z",
      "DeleteOnTermination": true,
      "InstanceId": "i-123abc456def789g",
      "Status": "attached"
    }
  ],
  "CreateTime": "2020-02-24T15:54:30Z",
  "Encrypted": true,
  "KmsKeyId": "arn:aws:kms:us-east-1:111122223333:key/wJa1rXUtnFEMI/K7MDENG/
bPxRfiCYEXAMPLEKEY",
  "Size": 80,
  "SnapshotId": "",
  "Status": "available"
}
```

AwsEc2Vpc

L'AwsEc2Vpcoggetto fornisce dettagli su un VPC Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. AwsEc2Vpc Per visualizzare le descrizioni degli AwsEc2Vpc attributi, vedere [AwsEc2 VpcDetails](#) nell'AWS Security Hub API Reference.

Esempio

```
"AwsEc2Vpc": {
  "CidrBlockAssociationSet": [
    {
      "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
      "CidrBlock": "192.0.2.0/24",
      "CidrBlockState": "associated"
    }
  ],
  "DhcpOptionsId": "dopt-4e42ce28",
}
```

```

    "Ipv6CidrBlockAssociationSet": [
      {
        "AssociationId": "vpc-cidr-assoc-0dc4c852f52abda97",
        "CidrBlockState": "associated",
        "Ipv6CidrBlock": "192.0.2.0/24"
      }
    ],
    "State": "available"
  }

```

AwsEc2VpcEndpointService

L'AwsEc2VpcEndpointService oggetto contiene dettagli sulla configurazione del servizio per un servizio endpoint VPC.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

AwsEc2VpcEndpointService Per visualizzare le descrizioni degli AwsEc2VpcEndpointService attributi, vedere [AwsEc2 VpcEndpointServiceDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

"AwsEc2VpcEndpointService": {
  "ServiceType": [
    {
      "ServiceType": "Interface"
    }
  ],
  "ServiceId": "vpce-svc-example1",
  "ServiceName": "com.amazonaws.vpce.us-east-1.vpce-svc-example1",
  "ServiceState": "Available",
  "AvailabilityZones": [
    "us-east-1"
  ],
  "AcceptanceRequired": true,
  "ManagesVpcEndpoints": false,
  "NetworkLoadBalancerArns": [
    "arn:aws:elasticloadbalancing:us-east-1:444455556666:loadbalancer/net/my-network-load-balancer/example1"
  ],
  "GatewayLoadBalancerArns": [],
  "BaseEndpointDnsNames": [
    "vpce-svc-04eec859668b51c34.us-east-1.vpce.amazonaws.com"
  ]
}

```

```
  ],
  "PrivateDnsName": "my-private-dns"
}
```

AwsEc2VpcPeeringConnection

L'`AwsEc2VpcPeeringConnection` oggetto fornisce dettagli sulla connessione di rete tra due VPC.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEc2VpcPeeringConnection` oggetto. Per visualizzare le descrizioni degli `AwsEc2VpcPeeringConnection` attributi, vedere [AwsEc2 VpcPeeringConnectionDetails](#) nell'AWS Security Hub API Reference.

Esempio

```
"AwsEc2VpcPeeringConnection": {
  "AcceptorVpcInfo": {
    "CidrBlock": "10.0.0.0/28",
    "CidrBlockSet": [{
      "CidrBlock": "10.0.0.0/28"
    }],
    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
    }],
    "OwnerId": "012345678910",
    "PeeringOptions": {
      "AllowDnsResolutionFromRemoteVpc": true,
      "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
      "AllowEgressFromLocalVpcToRemoteClassicLink": true
    },
    "Region": "us-west-2",
    "VpcId": "vpc-i123456"
  },
  "ExpirationTime": "2022-02-18T15:31:53.161Z",
  "RequesterVpcInfo": {
    "CidrBlock": "192.168.0.0/28",
    "CidrBlockSet": [{
      "CidrBlock": "192.168.0.0/28"
    }],
    "Ipv6CidrBlockSet": [{
      "Ipv6CidrBlock": "2002::1234:abcd:ffff:c0a8:101/64"
    }],
    "OwnerId": "012345678910",
```

```

"PeeringOptions": {
  "AllowDnsResolutionFromRemoteVpc": true,
  "AllowEgressFromLocalClassicLinkToRemoteVpc": false,
  "AllowEgressFromLocalVpcToRemoteClassicLink": true
},
"Region": "us-west-2",
"VpcId": "vpc-i123456"
},
"Status": {
  "Code": "initiating-request",
  "Message": "Active"
},
"VpcPeeringConnectionId": "pcx-1a2b3c4d"
}

```

AwsEc2VpnConnection

L'AwsEc2VpnConnection oggetto fornisce dettagli su una connessione VPN Amazon EC2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsEc2VpnConnection oggetto. Per visualizzare le descrizioni degli AwsEc2VpnConnection attributi, vedere [AwsEc2 VpnConnectionDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

"AwsEc2VpnConnection": {
  "VpnConnectionId": "vpn-205e4f41",
  "State": "available",
  "CustomerGatewayConfiguration": "",
  "CustomerGatewayId": "cgw-5699703f",
  "Type": "ipsec.1",
  "VpnGatewayId": "vgw-2ccb2245",
  "Category": "VPN"
  "TransitGatewayId": "tgw-09b6f3a659e2b5e1f",
  "VgwTelemetry": [
    {
      "OutsideIpAddress": "92.0.2.11",
      "Status": "DOWN",
      "LastStatusChange": "2016-11-11T23:09:32.000Z",
      "StatusMessage": "IPSEC IS DOWN",
      "AcceptedRouteCount": 0
    },
    {

```

```

    "OutsideIpAddress": "92.0.2.12",
    "Status": "DOWN",
    "LastStatusChange": "2016-11-11T23:10:51.000Z",
    "StatusMessage": "IPSEC IS DOWN",
    "AcceptedRouteCount": 0
  }
],
"Routes": [{
  "DestinationCidrBlock": "10.24.34.0/24",
  "State": "available"
}],
"Options": {
  "StaticRoutesOnly": true
  "TunnelOptions": [{
    "DpdTimeoutSeconds": 30,
    "IkeVersions": ["ikev1", "ikev2"],
    "Phase1DhGroupNumbers": [14, 15, 16, 17, 18],
    "Phase1EncryptionAlgorithms": ["AES128", "AES256"],
    "Phase1IntegrityAlgorithms": ["SHA1", "SHA2-256"],
    "Phase1LifetimeSeconds": 28800,
    "Phase2DhGroupNumbers": [14, 15, 16, 17, 18],
    "Phase2EncryptionAlgorithms": ["AES128", "AES256"],
    "Phase2IntegrityAlgorithms": ["SHA1", "SHA2-256"],
    "Phase2LifetimeSeconds": 28800,
    "PreSharedKey": "RltXC3REhTw1RADiM2s1uMfkkSDLyGJoe1QEWeGxqkQ=",
    "RekeyFuzzPercentage": 100,
    "RekeyMarginTimeSeconds": 540,
    "ReplayWindowSize": 1024,
    "TunnelInsideCidr": "10.24.34.0/23"
  ]
}
}
}

```

AwsEcr

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsEcr` risorse.

`AwsEcrContainerImage`

L'`AwsEcrContainerImage` oggetto fornisce informazioni su un'immagine Amazon ECR.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEcrContainerImage` oggetto. Per visualizzare le descrizioni degli `AwsEcrContainerImage` attributi, consulta [AwsEcrContainerImageDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsEcrContainerImage": {
  "RegistryId": "123456789012",
  "RepositoryName": "repository-name",
  "Architecture": "amd64"
  "ImageDigest":
  "sha256:a568e5c7a953fbeaa2904ac83401f93e4a076972dc1bae527832f5349cd2fb10",
  "ImageTags": ["00000000-0000-0000-0000-000000000000"],
  "ImagePublishedAt": "2019-10-01T20:06:12Z"
}
```

AwsEcrRepository

L'`AwsEcrRepository` oggetto fornisce informazioni su un repository Amazon Elastic Container Registry.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEcrRepository` oggetto. Per visualizzare le descrizioni degli `AwsEcrRepository` attributi, consulta [AwsEcrRepositoryDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsEcrRepository": {
  "LifecyclePolicy": {
    "RegistryId": "123456789012",
  },
  "RepositoryName": "sample-repo",
  "Arn": "arn:aws:ecr:us-west-2:111122223333:repository/sample-repo",
  "ImageScanningConfiguration": {
    "ScanOnPush": true
  },
  "ImageTagMutability": "IMMUTABLE"
}
```

AwsEcs

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsEcs` risorse.

AwsEcsCluster

L'`AwsEcsCluster` oggetto fornisce dettagli su un cluster Amazon Elastic Container Service.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEcsCluster` oggetto. Per visualizzare le descrizioni degli `AwsEcsCluster` attributi, consulta [AwsEcsClusterDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsEcsCluster": {
  "CapacityProviders": [],
  "ClusterSettings": [
    {
      "Name": "containerInsights",
      "Value": "enabled"
    }
  ],
  "Configuration": {
    "ExecuteCommandConfiguration": {
      "KmsKeyId": "kmsKeyId",
      "LogConfiguration": {
        "CloudWatchEncryptionEnabled": true,
        "CloudWatchLogGroupName": "cloudWatchLogGroupName",
        "S3BucketName": "s3BucketName",
        "S3EncryptionEnabled": true,
        "S3KeyPrefix": "s3KeyPrefix"
      },
      "Logging": "DEFAULT"
    }
  }
  "DefaultCapacityProviderStrategy": [
    {
      "Base": 0,
      "CapacityProvider": "capacityProvider",
      "Weight": 1
    }
  ]
}
```

AwsEcsContainer

L'`AwsEcsContainer` oggetto contiene dettagli su un contenitore Amazon ECS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEcsContainer` oggetto. Per visualizzare le descrizioni degli `AwsEcsContainer` attributi, consulta [AwsEcsContainerDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsEcsContainer": {
  "Image": "11111111/
knotejs@sha256:356131c9fef1111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
  "MountPoints": [{
    "ContainerPath": "/mnt/etc",
    "SourceVolume": "vol-03909e9"
  }],
  "Name": "knote",
  "Privileged": true
}
```

AwsEcsService

L'AwsEcsService oggetto fornisce dettagli su un servizio all'interno di un cluster Amazon ECS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsEcsService oggetto. Per visualizzare le descrizioni degli AwsEcsService attributi, consulta [AwsEcsServiceDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsEcsService": {
  "CapacityProviderStrategy": [
    {
      "Base": 12,
      "CapacityProvider": "",
      "Weight": ""
    }
  ],
  "Cluster": "arn:aws:ecs:us-east-1:111122223333:cluster/example-ecs-cluster",
  "DeploymentConfiguration": {
    "DeploymentCircuitBreaker": {
      "Enable": false,
      "Rollback": false
    },
    "MaximumPercent": 200,
    "MinimumHealthyPercent": 100
  },
  "DeploymentController": "",
  "DesiredCount": 1,
  "EnableEcsManagedTags": false,
```

```
"EnableExecuteCommand": false,
"HealthCheckGracePeriodSeconds": 1,
"LaunchType": "FARGATE",
"LoadBalancers": [
  {
    "ContainerName": "",
    "ContainerPort": 23,
    "LoadBalancerName": "",
    "TargetGroupArn": ""
  }
],
"Name": "sample-app-service",
"NetworkConfiguration": {
  "AwsVpcConfiguration": {
    "Subnets": [
      "Subnet-example1",
      "Subnet-example2"
    ],
    "SecurityGroups": [
      "Sg-0ce48e9a6e5b457f5"
    ],
    "AssignPublicIp": "ENABLED"
  }
},
"PlacementConstraints": [
  {
    "Expression": "",
    "Type": ""
  }
],
"PlacementStrategies": [
  {
    "Field": "",
    "Type": ""
  }
],
"PlatformVersion": "LATEST",
"PropagateTags": "",
"Role": "arn:aws:iam::111122223333:role/aws-servicerole/ecs.amazonaws.com/ServiceRoleForECS",
"SchedulingStrategy": "REPLICA",
"ServiceName": "sample-app-service",
"ServiceArn": "arn:aws:ecs:us-east-1:111122223333:service/example-ecs-cluster/sample-app-service",
```

```

    "ServiceRegistries": [
      {
        "ContainerName": "",
        "ContainerPort": 1212,
        "Port": 1221,
        "RegistryArn": ""
      }
    ],
    "TaskDefinition": "arn:aws:ecs:us-east-1:111122223333:task-definition/example-taskdef:1"
  }

```

AwsEcsTask

L'AwsEcsTaskoggetto fornisce dettagli su un'attività di Amazon ECS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsEcsTaskoggetto. Per visualizzare le descrizioni degli AwsEcsTask attributi, consulta [AwsEcsTask](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsEcsTask": {
  "ClusterArn": "arn:aws:ecs:us-west-2:123456789012:task/MyCluster/1234567890123456789",
  "CreatedAt": "1557134011644",
  "Group": "service:fargate-service",
  "StartedAt": "1557134011644",
  "StartedBy": "ecs-svc/1234567890123456789",
  "TaskDefinitionArn": "arn:aws:ecs:us-west-2:123456789012:task-definition/sample-fargate:2",
  "Version": 3,
  "Volumes": [{
    "Name": "string",
    "Host": {
      "SourcePath": "string"
    }
  }],
  "Containers": {
    "Image": "11111111/
knotejs@sha256:356131c9fef111111111111111115f4ed8de5f9dce4dc3bd34bg21846588a3",
    "MountPoints": [{
      "ContainerPath": "/mnt/etc",
      "SourceVolume": "vol-03909e9"
    }
  ]
}

```

```
  ]],  
  "Name": "knote",  
  "Privileged": true  
}  
}
```

AwsEcsTaskDefinition

L'`AwsEcsTaskDefinition` oggetto contiene dettagli sulla definizione di un'attività. Una definizione di attività descrive le definizioni di contenitore e volume di un'attività di Amazon Elastic Container Service.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsEcsTaskDefinition` oggetto. Per visualizzare le descrizioni degli `AwsEcsTaskDefinition` attributi, consulta [AwsEcsTaskDefinitionDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsEcsTaskDefinition": {  
  "ContainerDefinitions": [  
    {  
      "Command": ['ruby', 'hi.rb'],  
      "Cpu":128,  
      "Essential": true,  
      "HealthCheck": {  
        "Command": ["CMD-SHELL", "curl -f http://localhost/ || exit 1"],  
        "Interval": 10,  
        "Retries": 3,  
        "StartPeriod": 5,  
        "Timeout": 20  
      },  
      "Image": "tongueroo/sinatra:latest",  
      "Interactive": true,  
      "Links": [],  
      "LogConfiguration": {  
        "LogDriver": "awslogs",  
        "Options": {  
          "awslogs-group": "/ecs/sinatra-hi",  
          "awslogs-region": "ap-southeast-1",  
          "awslogs-stream-prefix": "ecs"  
        },  
        "SecretOptions": []  
      },  
      "SecretOptions": []  
    }  
  ]  
}
```

```

    },
    "MemoryReservation": 128,
    "Name": "web",
    "PortMappings": [
      {
        "ContainerPort": 4567,
        "HostPort": 4567,
        "Protocol": "tcp"
      }
    ],
    "Privileged": true,
    "StartTimeout": 10,
    "StopTimeout": 100,
  }
],
"Family": "sinatra-hi",
"NetworkMode": "host",
"RequiresCompatibilities": ["EC2"],
>Status": "ACTIVE",
"TaskRoleArn": "arn:aws:iam::111122223333:role/ecsTaskExecutionRole",
}

```

AwsEfs

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsEfs risorse.

AwsEfsAccessPoint

L'AwsEfsAccessPointoggetto fornisce dettagli sui file archiviati in Amazon Elastic File System.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsEfsAccessPointoggetto. Per visualizzare le descrizioni degli AwsEfsAccessPoint attributi, consulta [AwsEfsAccessPointDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsEfsAccessPoint": {
  "AccessPointId": "fsap-05c4c0e79ba0b118a",
  "Arn": "arn:aws:elasticfilesystem:us-east-1:863155670886:access-point/fsap-05c4c0e79ba0b118a",
  "ClientToken": "AccessPointCompliant-ASk06ZZSXsEp",
  "FileSystemId": "fs-0f8137f731cb32146",
  "PosixUser": {
    "Gid": "1000",

```

```

    "SecondaryGids": ["0", "4294967295"],
    "Uid": "1234"
  },
  "RootDirectory": {
    "CreationInfo": {
      "OwnerGid": "1000",
      "OwnerUid": "1234",
      "Permissions": "777"
    },
    "Path": "/tmp/example"
  }
}

```

AwsEks

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsEks risorse.

AwsEksCluster

L'AwsEksCluster oggetto fornisce dettagli su un cluster Amazon EKS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsEksCluster oggetto. Per visualizzare le descrizioni degli AwsEksCluster attributi, consulta [AwsEksClusterDetails](#) l'AWS Security Hub API Reference.

Esempio

```

{
  "AwsEksCluster": {
    "Name": "example",
    "Arn": "arn:aws:eks:us-west-2:222222222222:cluster/example",
    "CreatedAt": 1565804921.901,
    "Version": "1.12",
    "RoleArn": "arn:aws:iam::222222222222:role/example-cluster-ServiceRole-1XWBQWYSFRE2Q",
    "ResourcesVpcConfig": {
      "EndpointPublicAccess": false,
      "SubnetIds": [
        "subnet-021345abcdef6789",
        "subnet-abcdef01234567890",
        "subnet-1234567890abcdef0"
      ],
      "SecurityGroupIds": [
        "sg-abcdef01234567890"
      ]
    }
  }
}

```



```

    ]
  },
  "Logging": {
    "ClusterLogging": [
      {
        "Types": [
          "api",
          "audit",
          "authenticator",
          "controllerManager",
          "scheduler"
        ],
        "Enabled": true
      }
    ]
  },
  "Status": "CREATING",
  "CertificateAuthorityData": {},
}
}

```

AwsElasticBeanstalk

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsElasticBeanstalk` risorse.

AwsElasticBeanstalkEnvironment

L'`AwsElasticBeanstalkEnvironment` oggetto contiene dettagli su un AWS Elastic Beanstalk ambiente.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsElasticBeanstalkEnvironment` oggetto. Per visualizzare le descrizioni degli `AwsElasticBeanstalkEnvironment` attributi, consulta [AwsElasticBeanstalkEnvironmentDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsElasticBeanstalkEnvironment": {
  "ApplicationName": "MyApplication",
  "Cname": "myexampleapp-env.devo-2.elasticbeanstalk-internal.com",
  "DateCreated": "2021-04-30T01:38:01.090Z",
  "DateUpdated": "2021-04-30T01:38:01.090Z",

```

```
"Description": "Example description of my awesome application",
"EndpointUrl": "eb-dv-e-p-AWSEBLoa-abcdef01234567890-021345abcdef6789.us-
east-1.elb.amazonaws.com",
"EnvironmentArn": "arn:aws:elasticbeanstalk:us-east-1:123456789012:environment/
MyApplication/myapplication-env",
"EnvironmentId": "e-abcd1234",
"EnvironmentLinks": [
  {
    "EnvironmentName": "myexampleapp-env",
    "LinkName": "myapplicationLink"
  }
],
"EnvironmentName": "myapplication-env",
"OptionSettings": [
  {
    "Namespace": "aws:elasticbeanstalk:command",
    "OptionName": "BatchSize",
    "Value": "100"
  },
  {
    "Namespace": "aws:elasticbeanstalk:command",
    "OptionName": "Timeout",
    "Value": "600"
  },
  {
    "Namespace": "aws:elasticbeanstalk:command",
    "OptionName": "BatchSizeType",
    "Value": "Percentage"
  },
  {
    "Namespace": "aws:elasticbeanstalk:command",
    "OptionName": "IgnoreHealthCheck",
    "Value": "false"
  },
  {
    "Namespace": "aws:elasticbeanstalk:application",
    "OptionName": "Application Healthcheck URL",
    "Value": "TCP:80"
  }
],
"PlatformArn": "arn:aws:elasticbeanstalk:us-east-1::platform/Tomcat 8 with Java 8
running on 64bit Amazon Linux/2.7.7",
"SolutionStackName": "64bit Amazon Linux 2017.09 v2.7.7 running Tomcat 8 Java 8",
"Status": "Ready",
```

```

    "Tier": {
      "Name": "WebServer"
      "Type": "Standard"
      "Version": "1.0"
    },
    "VersionLabel": "Sample Application"
  }

```

AwsElasticSearch

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsElasticSearch` risorse.

AwsElasticSearchDomain

L'`AwsElasticSearchDomain` oggetto fornisce dettagli su un dominio Amazon OpenSearch Service.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsElasticSearchDomain` oggetto. Per visualizzare le descrizioni degli `AwsElasticSearchDomain` attributi, consulta [AwsElasticSearchDomainDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsElasticSearchDomain": {
  "AccessPolicies": "string",
  "DomainStatus": {
    "DomainId": "string",
    "DomainName": "string",
    "Endpoint": "string",
    "Endpoints": {
      "string": "string"
    }
  },
  "DomainEndpointOptions": {
    "EnforceHTTPS": boolean,
    "TLSSecurityPolicy": "string"
  },
  "ElasticsearchClusterConfig": {
    "DedicatedMasterCount": number,
    "DedicatedMasterEnabled": boolean,
    "DedicatedMasterType": "string",
    "InstanceCount": number,

```

```
    "InstanceType": "string",
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": number
    },
    "ZoneAwarenessEnabled": boolean
  },
  "ElasticsearchVersion": "string",
  "EncryptionAtRestOptions": {
    "Enabled": boolean,
    "KmsKeyId": "string"
  },
  "LogPublishingOptions": {
    "AuditLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    },
    "IndexSlowLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    },
    "SearchSlowLogs": {
      "CloudWatchLogsLogGroupArn": "string",
      "Enabled": boolean
    }
  },
  "NodeToNodeEncryptionOptions": {
    "Enabled": boolean
  },
  "ServiceSoftwareOptions": {
    "AutomatedUpdateDate": "string",
    "Cancellable": boolean,
    "CurrentVersion": "string",
    "Description": "string",
    "NewVersion": "string",
    "UpdateAvailable": boolean,
    "UpdateStatus": "string"
  },
  "VPCOptions": {
    "AvailabilityZones": [
      "string"
    ],
    "SecurityGroupIds": [
      "string"
    ]
  },
]
```

```

        "SubnetIds": [
            "string"
        ],
        "VPCId": "string"
    }
}

```

AwsElb

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsElb risorse.

AwsElbLoadBalancer

L'AwsElbLoadBalancer oggetto contiene dettagli su un Classic Load Balancer.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsElbLoadBalancer oggetto. Per visualizzare le descrizioni degli AwsElbLoadBalancer attributi, consulta [AwsElbLoadBalancerDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsElbLoadBalancer": {
  "AvailabilityZones": ["us-west-2a"],
  "BackendServerDescriptions": [
    {
      "InstancePort": 80,
      "PolicyNames": ["doc-example-policy"]
    }
  ],
  "CanonicalHostedZoneName": "Z3DZXE0EXAMPLE",
  "CanonicalHostedZoneNameID": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
  "CreatedTime": "2020-08-03T19:22:44.637Z",
  "DnsName": "my-load-balancer-444455556666.us-west-2.elb.amazonaws.com",
  "HealthCheck": {
    "HealthyThreshold": 2,
    "Interval": 30,
    "Target": "HTTP:80/png",
    "Timeout": 3,
    "UnhealthyThreshold": 2
  },
  "Instances": [
    {
      "InstanceId": "i-example"
    }
  ]
}

```

```

    }
  ],
  "ListenerDescriptions": [
    {
      "Listener": {
        "InstancePort": 443,
        "InstanceProtocol": "HTTPS",
        "LoadBalancerPort": 443,
        "Protocol": "HTTPS",
        "SslCertificateId": "arn:aws:iam::444455556666:server-certificate/my-
server-cert"
      },
      "PolicyNames": ["ELBSecurityPolicy-TLS-1-2-2017-01"]
    }
  ],
  "LoadBalancerAttributes": {
    "AccessLog": {
      "EmitInterval": 60,
      "Enabled": true,
      "S3BucketName": "doc-example-bucket",
      "S3BucketPrefix": "doc-example-prefix"
    },
    "ConnectionDraining": {
      "Enabled": false,
      "Timeout": 300
    },
    "ConnectionSettings": {
      "IdleTimeout": 30
    },
    "CrossZoneLoadBalancing": {
      "Enabled": true
    },
    "AdditionalAttributes": [{
      "Key": "elb.http.desyncmitigationmode",
      "Value": "strictest"
    }]
  },
  "LoadBalancerName": "example-load-balancer",
  "Policies": {
    "AppCookieStickinessPolicies": [
      {
        "CookieName": "",
        "PolicyName": ""
      }
    ]
  }
}

```

```

    }
  ],
  "LbCookieStickinessPolicies": [
    {
      "CookieExpirationPeriod": 60,
      "PolicyName": "my-example-cookie-policy"
    }
  ],
  "OtherPolicies": [
    "my-PublicKey-policy",
    "my-authentication-policy",
    "my-SSLNegotiation-policy",
    "my-ProxyProtocol-policy",
    "ELBSecurityPolicy-2015-03"
  ]
},
"Scheme": "internet-facing",
"SecurityGroups": ["sg-example"],
"SourceSecurityGroup": {
  "GroupName": "my-elb-example-group",
  "OwnerAlias": "444455556666"
},
"Subnets": ["subnet-example"],
"VpcId": "vpc-a01106c2"
}

```

AwsElbv2LoadBalancer

L'oggetto `AwsElbv2LoadBalancer` fornisce informazioni su un bilanciamento del carico.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsElbv2LoadBalancer` oggetto. Per visualizzare le descrizioni degli `AwsElbv2LoadBalancer` attributi, vedere [AwsElbv2 LoadBalancerDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

"AwsElbv2LoadBalancer": {
  "AvailabilityZones": {
    "SubnetId": "string",
    "ZoneName": "string"
  },
  "CanonicalHostedZoneId": "string",
  "CreatedTime": "string",

```

```

        "DNSName": "string",
        "IpAddressType": "string",
        "LoadBalancerAttributes": [
            {
                "Key": "string",
                "Value": "string"
            }
        ],
        "Scheme": "string",
        "SecurityGroups": [ "string" ],
        "State": {
            "Code": "string",
            "Reason": "string"
        },
        "Type": "string",
        "VpcId": "string"
    }

```

AwsEventBridge

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsEventBridge` risorse.

AwsEventSchemasRegistry

L'`AwsEventSchemasRegistry` oggetto fornisce informazioni su un registro di EventBridge schemi Amazon. Uno schema definisce la struttura degli eventi a cui vengono inviati EventBridge. I registri degli schemi sono contenitori che raccolgono e raggruppano logicamente gli schemi.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

`AwsEventSchemasRegistry` Per visualizzare le descrizioni degli `AwsEventSchemasRegistry` attributi, consulta [AwsEventSchemasRegistry](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsEventSchemasRegistry": {
    "Description": "This is an example event schema registry.",
    "RegistryArn": "arn:aws:schemas:us-east-1:123456789012:registry/schema-registry",
    "RegistryName": "schema-registry"
}

```


AwsEventsEndpoint

L'`AwsEventsEndpoint` oggetto fornisce informazioni su un endpoint EventBridge globale Amazon. L'endpoint può migliorare la disponibilità dell'applicazione rendendola tollerante ai guasti regionali.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

`AwsEventsEndpoint` Per visualizzare le descrizioni degli `AwsEventsEndpoint` attributi, consulta [AwsEventsEndpointDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsEventsEndpoint": {
  "Arn": "arn:aws:events:us-east-1:123456789012:endpoint/my-endpoint",
  "Description": "This is a sample endpoint.",
  "EndpointId": "04k1exajoy.veo",
  "EndpointUrl": "https://04k1exajoy.veo.endpoint.events.amazonaws.com",
  "EventBuses": [
    {
      "EventBusArn": "arn:aws:events:us-east-1:123456789012:event-bus/default"
    },
    {
      "EventBusArn": "arn:aws:events:us-east-2:123456789012:event-bus/default"
    }
  ],
  "Name": "my-endpoint",
  "ReplicationConfig": {
    "State": "ENABLED"
  },
  "RoleArn": "arn:aws:iam::123456789012:role/service-role/Amazon_EventBridge_Invoke_Event_Bus_1258925394",
  "RoutingConfig": {
    "FailoverConfig": {
      "Primary": {
        "HealthCheck": "arn:aws:route53:::healthcheck/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
      },
      "Secondary": {
        "Route": "us-east-2"
      }
    }
  },
  "State": "ACTIVE"
}
```

AwsEventsEventbus

L'`AwsEventsEventbus` oggetto fornisce informazioni su un endpoint EventBridge globale Amazon. L'endpoint può migliorare la disponibilità dell'applicazione rendendola tollerante ai guasti regionali.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

`AwsEventsEventbus` Per visualizzare le descrizioni degli `AwsEventsEventbus` attributi, consulta [AwsEventsEventbusDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsEventsEventbus":
  "Arn": "arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus",
  "Name": "my-event-bus",
  "Policy": "{\n\"Version\":\n\"2012-10-17\", \"Statement\": [\n\n{\n\n\"Sid\":\n\n\"AllowAllAccountsFromOrganizationToPutEvents\", \"Effect\": \"Allow\", \"Principal\": \"*\", \"Action\": \"events:PutEvents\", \"Resource\": \"arn:aws:events:us-east-1:123456789012:event-bus/my-event-bus\", \"Condition\": {\n\n\"StringEquals\": {\n\n\"aws:PrincipalOrgID\": \"o-ki7yjdkjv5\"}}}, {\n\n\"Sid\":\n\n\"AllowAccountToManageRulesTheyCreated\", \"Effect\": \"Allow\", \"Principal\": {\n\n\"AWS\": \"arn:aws:iam::123456789012:root\"}, \"Action\": [\"events:PutRule\", \"events:PutTargets\", \"events>DeleteRule\", \"events:RemoveTargets\", \"events:DisableRule\", \"events:EnableRule\", \"events:TagResource\", \"events:UntagResource\", \"events:DescribeRule\", \"events>ListTargetsByRule\", \"events>ListTagsForResource\"], \"Resource\": \"arn:aws:events:us-east-1:123456789012:rule/my-event-bus\", \"Condition\": {\n\n\"StringEqualsIfExists\": {\n\n\"events:creatorAccount\": \"123456789012\"}}}}]\"}
```

AwsGuardDuty

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsGuardDuty` risorse.

AwsGuardDutyDetector

L'`AwsGuardDutyDetector` oggetto fornisce informazioni su un GuardDuty rilevatore Amazon. Un rilevatore è un oggetto che rappresenta il GuardDuty servizio. È necessario un rilevatore per GuardDuty diventare operativo.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsGuardDutyDetector` oggetto. Per visualizzare le descrizioni degli `AwsGuardDutyDetector` attributi, consulta [AwsGuardDutyDetector](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsGuardDutyDetector": {
  "FindingPublishingFrequency": "SIX_HOURS",
  "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDuty",
  "Status": "ENABLED",
  "DataSources": {
    "CloudTrail": {
      "Status": "ENABLED"
    },
    "DnsLogs": {
      "Status": "ENABLED"
    },
    "FlowLogs": {
      "Status": "ENABLED"
    },
    "S3Logs": {
      "Status": "ENABLED"
    },
    "Kubernetes": {
      "AuditLogs": {
        "Status": "ENABLED"
      }
    },
    "MalwareProtection": {
      "ScanEc2InstanceWithFindings": {
        "EbsVolumes": {
          "Status": "ENABLED"
        }
      },
      "ServiceRole": "arn:aws:iam::123456789012:role/aws-service-role/malware-protection.guardduty.amazonaws.com/AWSServiceRoleForAmazonGuardDutyMalwareProtection"
    }
  }
}

```

AwsIam

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsIam risorse.

AwsIamAccessKey

L'AwsIamAccessKeyoggetto contiene dettagli su una chiave di accesso IAM correlata a un risultato.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsIamAccessKey` oggetto. Per visualizzare le descrizioni degli `AwsIamAccessKey` attributi, consulta [AwsIamAccessKeyDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsIamAccessKey": {
  "AccessKeyId": "string",
  "AccountId": "string",
  "CreatedAt": "string",
  "PrincipalId": "string",
  "PrincipalName": "string",
  "PrincipalType": "string",
  "SessionContext": {
    "Attributes": {
      "CreationDate": "string",
      "MfaAuthenticated": boolean
    },
    "SessionIssuer": {
      "AccountId": "string",
      "Arn": "string",
      "PrincipalId": "string",
      "Type": "string",
      "UserName": "string"
    }
  },
  "Status": "string"
}
```

AwsIamGroup

L'`AwsIamGroup` oggetto contiene dettagli su un gruppo IAM.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsIamGroup` oggetto. Per visualizzare le descrizioni degli `AwsIamGroup` attributi, consulta [AwsIamGroupDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsIamGroup": {
  "AttachedManagedPolicies": [
    {
      "PolicyArn": "arn:aws:iam::aws:policy/ExampleManagedAccess",

```

```

        "PolicyName": "ExampleManagedAccess",
      }
    ],
    "CreateDate": "2020-04-28T14:08:37.000Z",
    "GroupId": "AGPA4TPS3VLP7QEXAMPLE",
    "GroupName": "Example_User_Group",
    "GroupPolicyList": [
      {
        "PolicyName": "ExampleGroupPolicy"
      }
    ],
    "Path": "/"
  }
}

```

AwsIamPolicy

L'`AwsIamPolicy` oggetto rappresenta una politica di autorizzazioni IAM.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsIamPolicy` oggetto. Per visualizzare le descrizioni degli `AwsIamPolicy` attributi, consulta [AwsIamPolicyDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsIamPolicy": {
  "AttachmentCount": 1,
  "CreateDate": "2017-09-14T08:17:29.000Z",
  "DefaultVersionId": "v1",
  "Description": "Example IAM policy",
  "IsAttachable": true,
  "Path": "/",
  "PermissionsBoundaryUsageCount": 5,
  "PolicyId": "ANPAJ2UCCR6DPCEXAMPLE",
  "PolicyName": "EXAMPLE-MANAGED-POLICY",
  "PolicyVersionList": [
    {
      "VersionId": "v1",
      "IsDefaultVersion": true,
      "CreateDate": "2017-09-14T08:17:29.000Z"
    }
  ],
  "UpdateDate": "2017-09-14T08:17:29.000Z"
}

```

AwsIamRole

L'`AwsIamRole` oggetto contiene informazioni su un ruolo IAM, incluse tutte le politiche del ruolo.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsIamRole` oggetto. Per visualizzare le descrizioni degli `AwsIamRole` attributi, consulta [AwsIamRoleDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsIamRole": {
  "AssumeRolePolicyDocument": "{\"Version\": \"2012-10-17\", \"Statement\": [{\"Effect\": \"Allow\", \"Action\": \"sts:AssumeRole\"}]}",
  "AttachedManagedPolicies": [
    {
      "PolicyArn": "arn:aws:iam::aws:policy/ExamplePolicy1",
      "PolicyName": "Example policy 1"
    },
    {
      "PolicyArn": "arn:aws:iam::444455556666:policy/ExamplePolicy2",
      "PolicyName": "Example policy 2"
    }
  ],
  "CreateDate": "2020-03-14T07:19:14.000Z",
  "InstanceProfileList": [
    {
      "Arn": "arn:aws:iam::333333333333:ExampleProfile",
      "CreateDate": "2020-03-11T00:02:27Z",
      "InstanceProfileId": "AIPAIXEU4NUHUPEXAMPLE",
      "InstanceProfileName": "ExampleInstanceProfile",
      "Path": "/",
      "Roles": [
        {
          "Arn": "arn:aws:iam::444455556666:role/example-role",
          "AssumeRolePolicyDocument": "",
          "CreateDate": "2020-03-11T00:02:27Z",
          "Path": "/",
          "RoleId": "AR0AJ520TH4H7LEXAMPLE",
          "RoleName": "example-role",
        }
      ]
    }
  ],
  "MaxSessionDuration": 3600,
```

```

    "Path": "/",
    "PermissionsBoundary": {
      "PermissionsBoundaryArn": "arn:aws:iam::aws:policy/AdministratorAccess",
      "PermissionsBoundaryType": "PermissionsBoundaryPolicy"
    },
    "RoleId": "AR0A4TPS3VLEXAMPLE",
    "RoleName": "BONESBootstrapHydra-OverbridgeOpsFunctionsLambda",
    "RolePolicyList": [
      {
        "PolicyName": "Example role policy"
      }
    ]
  }
}

```

AwsIamUser

L'AwsIamUser oggetto fornisce informazioni su un utente.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsIamUser oggetto. Per visualizzare le descrizioni degli AwsIamUser attributi, consulta [AwsIamUserDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsIamUser": {
  "AttachedManagedPolicies": [
    {
      "PolicyName": "ExamplePolicy",
      "PolicyArn": "arn:aws:iam::aws:policy/ExampleAccess"
    }
  ],
  "CreateDate": "2018-01-26T23:50:05.000Z",
  "GroupList": [],
  "Path": "/",
  "PermissionsBoundary" : {
    "PermissionsBoundaryArn" : "arn:aws:iam::aws:policy/AdministratorAccess",
    "PermissionsBoundaryType" : "PermissionsBoundaryPolicy"
  },
  "UserId": "AIDACKCEVSQ6C2EXAMPLE",
  "UserName": "ExampleUser",
  "UserPolicyList": [
    {
      "PolicyName": "InstancePolicy"
    }
  ]
}

```

```
    }  
  ]  
}
```

AwsKinesis

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsKinesis` risorse.

AwsKinesisStream

L'`AwsKinesisStream` oggetto fornisce dettagli su Amazon Kinesis Data Streams.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

`AwsKinesisStream` Per visualizzare le descrizioni degli `AwsKinesisStream` attributi, consulta [AwsKinesisStreamDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsKinesisStream": {  
  "Name": "test-vir-kinesis-stream",  
  "Arn": "arn:aws:kinesis:us-east-1:293279581038:stream/test-vir-kinesis-stream",  
  "RetentionPeriodHours": 24,  
  "ShardCount": 2,  
  "StreamEncryption": {  
    "EncryptionType": "KMS",  
    "KeyId": "arn:aws:kms:us-east-1:293279581038:key/849cf029-4143-4c59-91f8-  
ea76007247eb"  
  }  
}
```

AwsKms

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsKms` risorse.

AwsKmsKey

L'`AwsKmsKey` oggetto fornisce dettagli su un AWS KMS key.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsKmsKey` oggetto. Per visualizzare le descrizioni degli `AwsKmsKey` attributi, consulta [AwsKmsKeyDetails](#) l'AWS Security Hub API Reference.

Esempio


```
"AwsKmsKey": {
    "AWSAccountId": "string",
    "CreationDate": "string",
    "Description": "string",
    "KeyId": "string",
    "KeyManager": "string",
    "KeyRotationStatus": boolean,
    "KeyState": "string",
    "Origin": "string"
}
```

AwsLambda

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per `AwsLambda` le risorse.

AwsLambdaFunction

L'oggetto `AwsLambdaFunction` fornisce dettagli sulla configurazione di una funzione Lambda.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto `AwsLambdaFunction`. Per visualizzare le descrizioni degli attributi `AwsLambdaFunction`, consulta [AwsLambdaFunctionDetails](#) AWS Security Hub API Reference.

Esempio

```
"AwsLambdaFunction": {
  "Architectures": [
    "x86_64"
  ],
  "Code": {
    "S3Bucket": "DOC-EXAMPLE-BUCKET",
    "S3Key": "samplekey",
    "S3ObjectVersion": "2",
    "ZipFile": "myzip.zip"
  },
  "CodeSha256": "1111111111111111111111111111111111111111111111111111111111111111",
  "DeadLetterConfig": {
    "TargetArn": "arn:aws:lambda:us-east-2:123456789012:queue:myqueue:2"
  },
  "Environment": {
    "Variables": {
      "Stage": "foobar"
    }
  },
}
```

```

    "Error": {
      "ErrorCode": "Sample-error-code",
      "Message": "Caller principal is a manager."
    }
  },
  "FunctionName": "CheckOut",
  "Handler": "main.py:lambda_handler",
  "KmsKeyArn": "arn:aws:kms:us-west-2:123456789012:key/mykey",
  "LastModified": "2001-09-11T09:00:00Z",
  "Layers": {
    "Arn": "arn:aws:lambda:us-east-2:123456789012:layer:my-layer:3",
    "CodeSize": 169
  },
  "PackageType": "Zip",
  "RevisionId": "23",
  "Role": "arn:aws:iam::123456789012:role/Accounting-Role",
  "Runtime": "go1.7",
  "Timeout": 15,
  "TracingConfig": {
    "Mode": "Active"
  },
  "Version": "$LATEST",
  "VpcConfig": {
    "SecurityGroupIds": ["sg-085912345678492fb", "sg-08591234567bdgdc"],
    "SubnetIds": ["subnet-071f712345678e7c8", "subnet-07fd123456788a036"]
  },
  "MasterArn": "arn:aws:lambda:us-east-2:123456789012:\$LATEST",
  "MemorySize": 2048
}

```

AwsLambdaLayerVersion

L'AwsLambdaLayerVersion oggetto fornisce dettagli su una versione del layer Lambda.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsLambdaLayerVersion oggetto. Per visualizzare le descrizioni degli AwsLambdaLayerVersion attributi, consulta [AwsLambdaLayerVersionDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsLambdaLayerVersion": {
  "Version": 2,

```

```

    "CompatibleRuntimes": [
      "java8"
    ],
    "CreateDate": "2019-10-09T22:02:00.274+0000"
  }

```

AwsMsk

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsMsk risorse.

AwsMskCluster

L'AwsMskCluster oggetto fornisce informazioni su un cluster Amazon Managed Streaming for Apache Kafka (Amazon MSK).

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. AwsMskCluster. Per visualizzare le descrizioni degli AwsMskCluster attributi, consulta [AwsMskClusterDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsMskCluster": {
  "ClusterInfo": {
    "ClientAuthentication": {
      "Sasl": {
        "Scram": {
          "Enabled": true
        },
        "Iam": {
          "Enabled": true
        }
      },
      "Tls": {
        "CertificateAuthorityArnList": [],
        "Enabled": false
      },
      "Unauthenticated": {
        "Enabled": false
      }
    },
    "ClusterName": "my-cluster",
    "CurrentVersion": "K2PWKAKR8XB7XF",
    "EncryptionInfo": {

```

```

    "EncryptionAtRest": {
      "DataVolumeKMSKeyId": "arn:aws:kms:us-east-1:123456789012:key/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
    },
    "EncryptionInTransit": {
      "ClientBroker": "TLS",
      "InCluster": true
    }
  },
  "EnhancedMonitoring": "PER_TOPIC_PER_BROKER",
  "NumberOfBrokerNodes": 3
}

```

AwsNetworkFirewall

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsNetworkFirewall` risorse.

AwsNetworkFirewallFirewall

L'`AwsNetworkFirewallFirewall` oggetto contiene dettagli su un AWS Network Firewall firewall.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsNetworkFirewallFirewall` oggetto. Per visualizzare le descrizioni degli `AwsNetworkFirewallFirewall` attributi, consulta [AwsNetworkFirewallFirewallDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsNetworkFirewallFirewall": {
  "DeleteProtection": false,
  "FirewallArn": "arn:aws:network-firewall:us-east-1:024665936331:firewall/
testfirewall",
  "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-
policy/InitialFirewall",
  "FirewallId": "dea7d8e9-ae38-4a8a-b022-672a830a99fa",
  "FirewallName": "testfirewall",
  "FirewallPolicyChangeProtection": false,
  "SubnetChangeProtection": false,
  "SubnetMappings": [
    {
      "SubnetId": "subnet-0183481095e588cdc"
    }
  ]
}

```

```

    },
    {
      "SubnetId": "subnet-01f518fad1b1c90b0"
    }
  ],
  "VpcId": "vpc-40e83c38"
}

```

AwsNetworkFirewallFirewallPolicy

L'AwsNetworkFirewallFirewallPolicy oggetto fornisce dettagli su una politica del firewall. Una politica firewall definisce il comportamento di un firewall di rete.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsNetworkFirewallFirewallPolicy oggetto. Per visualizzare le descrizioni degli AwsNetworkFirewallFirewallPolicy attributi, consulta [AwsNetworkFirewallFirewallPolicyDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsNetworkFirewallFirewallPolicy": {
  "FirewallPolicy": {
    "StatefulRuleGroupReferences": [
      {
        "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-rulegroup/PatchesOnly"
      }
    ],
    "StatelessDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessFragmentDefaultActions": [ "aws:forward_to_sfe" ],
    "StatelessRuleGroupReferences": [
      {
        "Priority": 1,
        "ResourceArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-rulegroup/Stateless-1"
      }
    ]
  },
  "FirewallPolicyArn": "arn:aws:network-firewall:us-east-1:444455556666:firewall-policy/InitialFirewall",
  "FirewallPolicyId": "9ceeda22-6050-4048-a0ca-50ce47f0cc65",
  "FirewallPolicyName": "InitialFirewall",
  "Description": "Initial firewall"
}

```

```
}
```

AwsNetworkFirewallRuleGroup

L'AwsNetworkFirewallRuleGroup oggetto fornisce dettagli su un gruppo di AWS Network Firewall regole. I gruppi di regole vengono utilizzati per ispezionare e controllare il traffico di rete. I gruppi di regole stateless si applicano ai singoli pacchetti. I gruppi di regole con stato si applicano ai pacchetti nel contesto del relativo flusso di traffico.

I gruppi di regole sono referenziati nelle politiche del firewall.

Gli esempi seguenti mostrano il AWS Security Finding Format (ASFF) per l'AwsNetworkFirewallRuleGroup oggetto. Per visualizzare le descrizioni degli AwsNetworkFirewallRuleGroup attributi, consulta [AwsNetworkFirewallRuleGroupDetails](#) l'AWS Security Hub API Reference.

Esempio: gruppo di regole stateless

```
"AwsNetworkFirewallRuleGroup": {
  "Capacity": 600,
  "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateless-
rulegroup/Stateless-1",
  "RuleGroupId": "fb13c4df-b6da-4c1e-91ec-84b7a5487493",
  "RuleGroupName": "Stateless-1"
  "Description": "Example of a stateless rule group",
  "Type": "STATELESS",
  "RuleGroup": {
    "RulesSource": {
      "StatelessRulesAndCustomActions": {
        "CustomActions": [],
        "StatelessRules": [
          {
            "Priority": 1,
            "RuleDefinition": {
              "Actions": [
                "aws:pass"
              ],
              "MatchAttributes": {
                "DestinationPorts": [
                  {
                    "FromPort": 443,
                    "ToPort": 443
                  }
                ]
              }
            }
          }
        ]
      }
    }
  }
}
```

```
    }
    ],
    "Destinations": [
      {
        "AddressDefinition": "192.0.2.0/24"
      }
    ],
    "Protocols": [
      6
    ],
    "SourcePorts": [
      {
        "FromPort": 0,
        "ToPort": 65535
      }
    ],
    "Sources": [
      {
        "AddressDefinition": "198.51.100.0/24"
      }
    ]
  }
}
}
}
}
}
}
```

Esempio: gruppo di regole stateful

```
"AwsNetworkFirewallRuleGroup": {
  "Capacity": 100,
  "RuleGroupArn": "arn:aws:network-firewall:us-east-1:444455556666:stateful-
rulegroup/tupletest",
  "RuleGroupId": "38b71c12-da80-4643-a6c5-03337f8933e0",
  "RuleGroupName": "ExampleRuleGroup",
  "Description": "Example of a stateful rule group",
  "Type": "STATEFUL",
  "RuleGroup": {
    "RuleSource": {
      "StatefulRules": [
```

```

    {
      "Action": "PASS",
      "Header": {
        "Destination": "Any",
        "DestinationPort": "443",
        "Direction": "ANY",
        "Protocol": "TCP",
        "Source": "Any",
        "SourcePort": "Any"
      },
      "RuleOptions": [
        {
          "Keyword": "sid:1"
        }
      ]
    }
  ]
}
}
}
}

```

Di seguito è riportato un elenco di esempi di valori validi per `AwsNetworkFirewallRuleGroup` gli attributi:

- **Action**

Valori validi: PASS | DROP | ALERT

- **Protocol**

Valori validi: IP | TCP | UDP | ICMP | HTTP | FTP | TLS | SMB | DNS | DCERPC | SSH | SMTP | IMAP | MSN | KRB5 | IKEV2 | TFTP | NTP | DHCP

- **Flags**

Valori validi: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

- **Masks**

Valori validi: FIN | SYN | RST | PSH | ACK | URG | ECE | CWR

AwsOpenSearchService

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsOpenSearchService` risorse.

AwsOpenSearchServiceDomain

L'`AwsOpenSearchServiceDomain` oggetto contiene informazioni su un dominio Amazon OpenSearch Service.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsOpenSearchServiceDomain` oggetto. Per visualizzare le descrizioni degli `AwsOpenSearchServiceDomain` attributi, consulta [AwsOpenSearchServiceDomainDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsOpenSearchServiceDomain": {
  "AccessPolicies": "IAM_Id",
  "AdvancedSecurityOptions": {
    "Enabled": true,
    "InternalUserDatabaseEnabled": true,
    "MasterUserOptions": {
      "MasterUserArn": "arn:aws:iam::123456789012:user/third-master-use",
      "MasterUserName": "third-master-use",
      "MasterUserPassword": "some-password"
    }
  },
  "Arn": "arn:aws:opensearch:us-east-1:111122223333:somedomain",
  "ClusterConfig": {
    "InstanceType": "c5.large.search",
    "InstanceCount": 1,
    "DedicatedMasterEnabled": true,
    "ZoneAwarenessEnabled": false,
    "ZoneAwarenessConfig": {
      "AvailabilityZoneCount": 2
    },
    "DedicatedMasterType": "c5.large.search",
    "DedicatedMasterCount": 3,
    "WarmEnabled": true,
    "WarmCount": 3,
    "WarmType": "ultrawarm1.large.search"
  },
}
```

```
"DomainEndpoint": "https://es-2021-06-23t17-04-qowmgghud5vofgb5e4wmi.eu-central-1.es.amazonaws.com",
"DomainEndpointOptions": {
  "EnforceHTTPS": false,
  "TLSSecurityPolicy": "Policy-Min-TLS-1-0-2019-07",
  "CustomEndpointCertificateArn": "arn:aws:acm:us-east-1:111122223333:certificate/bda1bff1-79c0-49d0-abe6-50a15a7477d4",
  "CustomEndpointEnabled": true,
  "CustomEndpoint": "example.com"
},
"DomainEndpoints": {
  "vpc": "vpc-endpoint-h2dsd34efgyghrtguk5gt6j2foh4.us-east-1.es.amazonaws.com"
},
"DomainName": "my-domain",
"EncryptionAtRestOptions": {
  "Enabled": false,
  "KmsKeyId": "1a2a3a4-1a2a-3a4a-5a6a-1a2a3a4a5a6a"
},
"EngineVersion": "7.1",
"Id": "123456789012",
"LogPublishingOptions": {
  "IndexSlowLogs": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/aes/domains/es-index-slow-logs",
    "Enabled": true
  },
  "SearchSlowLogs": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/aes/domains/es-slow-logs",
    "Enabled": true
  },
  "AuditLogs": {
    "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:111122223333:log-group:/aws/aes/domains/es-slow-logs",
    "Enabled": true
  }
},
"NodeToNodeEncryptionOptions": {
  "Enabled": true
},
"ServiceSoftwareOptions": {
  "AutomatedUpdateDate": "2022-04-28T14:08:37.000Z",
  "Cancellable": false,
  "CurrentVersion": "R20210331",
```

```

    "Description": "There is no software update available for this domain.",
    "NewVersion": "OpenSearch_1.0",
    "UpdateAvailable": false,
    "UpdateStatus": "COMPLETED",
    "OptionalDeployment": false
  },
  "VpcOptions": {
    "SecurityGroupIds": [
      "sg-2a3a4a5a"
    ],
    "SubnetIds": [
      "subnet-1a2a3a4a"
    ],
  }
}

```

AwsRds

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per `AwsRds` le risorse.

AwsRdsDbCluster

L'oggetto `AwsRdsDbCluster` fornisce dettagli su un cluster di database Amazon RDS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto `AwsRdsDbCluster`.

Per visualizzare le descrizioni degli attributi `AwsRdsDbCluster`, consulta

[AWSRdsDbClusterDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

"AwsRdsDbCluster": {
  "ActivityStreamStatus": "stopped",
  "AllocatedStorage": 1,
  "AssociatedRoles": [
    {
      "RoleArn": "arn:aws:iam::777788889999:role/aws-service-role/rds.amazonaws.com/AWSServiceRoleForRDS",
      "Status": "PENDING"
    }
  ],
  "AutoMinorVersionUpgrade": true,
  "AvailabilityZones": [
    "us-east-1a",
    "us-east-1c",

```

```
    "us-east-1e"
  ],
  "BackupRetentionPeriod": 1,
  "ClusterCreateTime": "2020-06-22T17:40:12.322Z",
  "CopyTagsToSnapshot": true,
  "CrossAccountClone": false,
  "CustomEndpoints": [],
  "DatabaseName": "Sample name",
  "DbClusterIdentifier": "database-3",
  "DbClusterMembers": [
    {
      "DbClusterParameterGroupStatus": "in-sync",
      "DbInstanceIdentifier": "database-3-instance-1",
      "IsClusterWriter": true,
      "PromotionTier": 1,
    }
  ],
  "DbClusterOptionGroupMemberships": [],
  "DbClusterParameterGroup": "cluster-parameter-group",
  "DbClusterResourceId": "cluster-example",
  "DbSubnetGroup": "subnet-group",
  "DeletionProtection": false,
  "DomainMemberships": [],
  "Status": "modifying",
  "EnabledCloudwatchLogsExports": [
    "audit",
    "error",
    "general",
    "slowquery"
  ],
  "Endpoint": "database-3.cluster-example.us-east-1.rds.amazonaws.com",
  "Engine": "aurora-mysql",
  "EngineMode": "provisioned",
  "EngineVersion": "5.7.mysql_aurora.2.03.4",
  "HostedZoneId": "ZONE1",
  "HttpEndpointEnabled": false,
  "IamDatabaseAuthenticationEnabled": false,
  "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
  "MasterUsername": "admin",
  "MultiAz": false,
  "Port": 3306,
  "PreferredBackupWindow": "04:52-05:22",
  "PreferredMaintenanceWindow": "sun:09:32-sun:10:02",
  "ReaderEndpoint": "database-3.cluster-ro-example.us-east-1.rds.amazonaws.com",
```

```

    "ReadReplicaIdentifiers": [],
    "Status": "Modifying",
    "StorageEncrypted": true,
    "VpcSecurityGroups": [
      {
        "Status": "active",
        "VpcSecurityGroupId": "sg-example-1"
      }
    ],
  }
}

```

AwsRdsDbClusterSnapshot

L'AwsRdsDbClusterSnapshot oggetto contiene informazioni su uno snapshot del cluster Amazon RDS DB.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

AwsRdsDbClusterSnapshot Per visualizzare le descrizioni degli AwsRdsDbClusterSnapshot attributi, consulta [AwsRdsDbClusterSnapshotDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsRdsDbClusterSnapshot": {
  "AllocatedStorage": 0,
  "AvailabilityZones": [
    "us-east-1a",
    "us-east-1d",
    "us-east-1e"
  ],
  "ClusterCreateTime": "2020-06-12T13:23:15.577Z",
  "DbClusterIdentifier": "database-2",
  "DbClusterSnapshotAttributes": [{
    "AttributeName": "restore",
    "AttributeValues": ["123456789012"]
  }],
  "DbClusterSnapshotIdentifier": "rds:database-2-2020-06-23-03-52",
  "Engine": "aurora",
  "EngineVersion": "5.6.10a",
  "IamDatabaseAuthenticationEnabled": false,
  "KmsKeyId": "arn:aws:kms:us-east-1:777788889999:key/key1",
  "LicenseModel": "aurora",
  "MasterUsername": "admin",
  "PercentProgress": 100,

```

```
"Port": 0,  
"SnapshotCreateTime": "2020-06-22T17:40:12.322Z",  
"SnapshotType": "automated",  
"Status": "available",  
"StorageEncrypted": true,  
"VpcId": "vpc-faf7e380"  
}
```

AwsRdsDbInstance

L'AwsRdsDbInstance oggetto fornisce dettagli su un'istanza database Amazon RDS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsRdsDbInstance oggetto. Per visualizzare le descrizioni degli AwsRdsDbInstance attributi, consulta [AwsRdsDbInstanceDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsRdsDbInstance": {  
  "AllocatedStorage": 20,  
  "AssociatedRoles": [],  
  "AutoMinorVersionUpgrade": true,  
  "AvailabilityZone": "us-east-1d",  
  "BackupRetentionPeriod": 7,  
  "CaCertificateIdentifier": "certificate1",  
  "CharacterSetName": "",  
  "CopyTagsToSnapshot": true,  
  "DbClusterIdentifier": "",  
  "DbInstanceArn": "arn:aws:rds:us-east-1:111122223333:db:database-1",  
  "DbInstanceClass": "db.t2.micro",  
  "DbInstanceIdentifier": "database-1",  
  "DbInstancePort": 0,  
  "DbInstanceStatus": "available",  
  "DbiResourceId": "db-EXAMPLE123",  
  "DbName": "",  
  "DbParameterGroups": [  
    {  
      "DbParameterGroupName": "default.mysql5.7",  
      "ParameterApplyStatus": "in-sync"  
    }  
  ],  
}
```

```
"DbSecurityGroups": [],

"DbSubnetGroup": {
  "DbSubnetGroupName": "my-group-123abc",
  "DbSubnetGroupDescription": "My subnet group",
  "VpcId": "vpc-example1",
  "SubnetGroupStatus": "Complete",
  "Subnets": [
    {
      "SubnetIdentifier": "subnet-123abc",
      "SubnetAvailabilityZone": {
        "Name": "us-east-1d"
      },
      "SubnetStatus": "Active"
    },
    {
      "SubnetIdentifier": "subnet-456def",
      "SubnetAvailabilityZone": {
        "Name": "us-east-1c"
      },
      "SubnetStatus": "Active"
    }
  ],
  "DbSubnetGroupArn": ""
},
"DeletionProtection": false,
"DomainMemberships": [],
"EnabledCloudWatchLogsExports": [],
"Endpoint": {
  "address": "database-1.example.us-east-1.rds.amazonaws.com",
  "port": 3306,
  "hostedZoneId": "ZONEID1"
},
"Engine": "mysql",
"EngineVersion": "5.7.22",
"EnhancedMonitoringResourceArn": "arn:aws:logs:us-east-1:111122223333:log-
group:Example:log-stream:db-EXAMPLE1",
"IamDatabaseAuthenticationEnabled": false,
"InstanceCreateTime": "2020-06-22T17:40:12.322Z",
"Iops": "",
"KmsKeyId": "",
"LatestRestorableTime": "2020-06-24T05:50:00.000Z",
"LicenseModel": "general-public-license",
```

```
"ListenerEndpoint": "",
"MasterUsername": "admin",
"MaxAllocatedStorage": 1000,
"MonitoringInterval": 60,
"MonitoringRoleArn": "arn:aws:iam::111122223333:role/rds-monitoring-role",
"MultiAz": false,
"OptionGroupMemberships": [
  {
    "OptionGroupName": "default:mysql-5-7",
    "Status": "in-sync"
  }
],
"PreferredBackupWindow": "03:57-04:27",
"PreferredMaintenanceWindow": "thu:10:13-thu:10:43",
"PendingModifiedValues": {
  "DbInstanceClass": "",
  "AllocatedStorage": "",
  "MasterUserPassword": "",
  "Port": "",
  "BackupRetentionPeriod": "",
  "MultiAZ": "",
  "EngineVersion": "",
  "LicenseModel": "",
  "Iops": "",
  "DbInstanceIdentifier": "",
  "StorageType": "",
  "CaCertificateIdentifier": "",
  "DbSubnetGroupName": "",
  "PendingCloudWatchLogsExports": "",
  "ProcessorFeatures": []
},
"PerformanceInsightsEnabled": false,
"PerformanceInsightsKmsKeyId": "",
"PerformanceInsightsRetentionPeriod": "",
"ProcessorFeatures": [],
"PromotionTier": "",
"PubliclyAccessible": false,
"ReadReplicaDBClusterIdentifiers": [],
"ReadReplicaDBInstanceIdentifiers": [],
"ReadReplicaSourceDBInstanceIdentifier": "",
"SecondaryAvailabilityZone": "",
"StatusInfos": [],
"StorageEncrypted": false,
"StorageType": "gp2",
```



```

    "TdeCredentialArn": "",
    "Timezone": "",
    "VpcSecurityGroups": [
      {
        "VpcSecurityGroupId": "sg-example1",
        "Status": "active"
      }
    ]
  }
}

```

AwsRdsDbSecurityGroup

L'AwsRdsDbSecurityGroup oggetto contiene informazioni su un Amazon Relational Database Service

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsRdsDbSecurityGroup oggetto. Per visualizzare le descrizioni degli AwsRdsDbSecurityGroup attributi, consulta [AwsRdsDbSecurityGroupDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsRdsDbSecurityGroup": {
  "DbSecurityGroupArn": "arn:aws:rds:us-west-1:111122223333:secgrp:default",
  "DbSecurityGroupDescription": "default",
  "DbSecurityGroupName": "mysecgroup",
  "Ec2SecurityGroups": [
    {
      "Ec2SecurityGroupuId": "myec2group",
      "Ec2SecurityGroupName": "default",
      "Ec2SecurityGroupOwnerId": "987654321021",
      "Status": "authorizing"
    }
  ],
  "IpRanges": [
    {
      "CidrIp": "0.0.0.0/0",
      "Status": "authorizing"
    }
  ],
  "OwnerId": "123456789012",
  "VpcId": "vpc-1234567f"
}

```

```
}
```

AwsRdsDbSnapshot

L'AwsRdsDbSnapshotoggetto contiene dettagli su uno snapshot del cluster Amazon RDS DB.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

AwsRdsDbSnapshot Per visualizzare le descrizioni degli AwsRdsDbSnapshot attributi, consulta [AwsRdsDbSnapshotDetails](#)l'AWS Security Hub API Reference.

Esempio

```
"AwsRdsDbSnapshot": {
  "DbSnapshotIdentifier": "rds:database-1-2020-06-22-17-41",
  "DbInstanceIdentifier": "database-1",
  "SnapshotCreateTime": "2020-06-22T17:41:29.967Z",
  "Engine": "mysql",
  "AllocatedStorage": 20,
  "Status": "available",
  "Port": 3306,
  "AvailabilityZone": "us-east-1d",
  "VpcId": "vpc-example1",
  "InstanceCreateTime": "2020-06-22T17:40:12.322Z",
  "MasterUsername": "admin",
  "EngineVersion": "5.7.22",
  "LicenseModel": "general-public-license",
  "SnapshotType": "automated",
  "Iops": null,
  "OptionGroupName": "default:mysql-5-7",
  "PercentProgress": 100,
  "SourceRegion": null,
  "SourceDbSnapshotIdentifier": "",
  "StorageType": "gp2",
  "TdeCredentialArn": "",
  "Encrypted": false,
  "KmsKeyId": "",
  "Timezone": "",
  "IamDatabaseAuthenticationEnabled": false,
  "ProcessorFeatures": [],
  "DbiResourceId": "db-resourceexample1"
}
```

AwsRdsEventSubscription

`AwsRdsEventSubscription` Contiene dettagli su un abbonamento per la notifica di eventi RDS. L'abbonamento consente a RDS di pubblicare eventi su un argomento SNS.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

`AwsRdsEventSubscription` Per visualizzare le descrizioni degli `AwsRdsEventSubscription` attributi, consulta [AwsRdsEventSubscriptionDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsRdsEventSubscription": {
  "CustSubscriptionId": "myawsuser-secgrp",
  "CustomerAwsId": "111111111111",
  "Enabled": true,
  "EventCategoriesList": [
    "configuration change",
    "failure"
  ],
  "EventSubscriptionArn": "arn:aws:rds:us-east-1:111111111111:es:my-instance-events",
  "SnsTopicArn": "arn:aws:sns:us-east-1:111111111111:myawsuser-RDS",
  "SourceIdsList": [
    "si-sample",
    "mysql-db-rr"
  ],
  "SourceType": "db-security-group",
  "Status": "creating",
  "SubscriptionCreationTime": "2021-06-27T01:38:01.090Z"
}
```

AwsRedshift

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsRedshift` risorse.

AwsRedshiftCluster

L'`AwsRedshiftCluster` oggetto contiene dettagli su un cluster Amazon Redshift.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsRedshiftCluster` oggetto. Per visualizzare le descrizioni degli `AwsRedshiftCluster` attributi, consulta [AwsRedshiftClusterDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsRedshiftCluster": {
  "AllowVersionUpgrade": true,
  "AutomatedSnapshotRetentionPeriod": 1,
  "AvailabilityZone": "us-west-2d",
  "ClusterAvailabilityStatus": "Unavailable",
  "ClusterCreateTime": "2020-08-03T19:22:44.637Z",
  "ClusterIdentifier": "redshift-cluster-1",
  "ClusterNodes": [
    {
      "NodeRole": "LEADER",
      "PrivateIPAddress": "192.0.2.108",
      "PublicIPAddress": "198.51.100.29"
    },
    {
      "NodeRole": "COMPUTE-0",
      "PrivateIPAddress": "192.0.2.22",
      "PublicIPAddress": "198.51.100.63"
    },
    {
      "NodeRole": "COMPUTE-1",
      "PrivateIPAddress": "192.0.2.224",
      "PublicIPAddress": "198.51.100.226"
    }
  ],
  "ClusterParameterGroups": [
    {
      "ClusterParameterStatusList": [
        {
          "ParameterName": "max_concurrency_scaling_clusters",
          "ParameterApplyStatus": "in-sync",
          "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
        },
        {
          "ParameterName": "enable_user_activity_logging",
          "ParameterApplyStatus": "in-sync",
          "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
        },
        {
          "ParameterName": "auto_analyze",
          "ParameterApplyStatus": "in-sync",
          "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
        }
      ]
    }
  ]
}
```

```
    {
      "ParameterName": "query_group",
      "ParameterApplyStatus": "in-sync",
      "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
      "ParameterName": "datestyle",
      "ParameterApplyStatus": "in-sync",
      "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
      "ParameterName": "extra_float_digits",
      "ParameterApplyStatus": "in-sync",
      "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
      "ParameterName": "search_path",
      "ParameterApplyStatus": "in-sync",
      "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
      "ParameterName": "statement_timeout",
      "ParameterApplyStatus": "in-sync",
      "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
      "ParameterName": "wlm_json_configuration",
      "ParameterApplyStatus": "in-sync",
      "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
      "ParameterName": "require_ssl",
      "ParameterApplyStatus": "in-sync",
      "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    },
    {
      "ParameterName": "use_fips_ssl",
      "ParameterApplyStatus": "in-sync",
      "ParameterApplyErrorDescription": "parameterApplyErrorDescription"
    }
  ],
  "ParameterApplyStatus": "in-sync",
  "ParameterGroupName": "temp"
}
```

```
],
"ClusterPublicKey": "Ja1rXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY Amazon-Redshift",
"ClusterRevisionNumber": 17498,
"ClusterSecurityGroups": [
  {
    "ClusterSecurityGroupName": "default",
    "Status": "active"
  }
],
"ClusterSnapshotCopyStatus": {
  "DestinationRegion": "us-west-2",
  "ManualSnapshotRetentionPeriod": -1,
  "RetentionPeriod": 1,
  "SnapshotCopyGrantName": "snapshotCopyGrantName"
},
"ClusterStatus": "available",
"ClusterSubnetGroupName": "default",
"ClusterVersion": "1.0",
"DBName": "dev",
"DeferredMaintenanceWindows": [
  {
    "DeferMaintenanceEndTime": "2020-10-07T20:34:01.000Z",
    "DeferMaintenanceIdentifier": "deferMaintenanceIdentifier",
    "DeferMaintenanceStartTime": "2020-09-07T20:34:01.000Z"
  }
],
"ElasticIpStatus": {
  "ElasticIp": "203.0.113.29",
  "Status": "active"
},
"ElasticResizeNumberOfNodeOptions": "4",
"Encrypted": false,
"Endpoint": {
  "Address": "redshift-cluster-1.example.us-west-2.redshift.amazonaws.com",
  "Port": 5439
},
"EnhancedVpcRouting": false,
"ExpectedNextSnapshotScheduleTime": "2020-10-13T20:34:01.000Z",
"ExpectedNextSnapshotScheduleTimeStatus": "OnTrack",
"HsmStatus": {
  "HsmClientCertificateIdentifier": "hsmClientCertificateIdentifier",
  "HsmConfigurationIdentifier": "hsmConfigurationIdentifier",
  "Status": "applying"
},
},
```

```
"IamRoles": [
  {
    "ApplyStatus": "in-sync",
    "IamRoleArn": "arn:aws:iam::111122223333:role/RedshiftCopyUnload"
  }
],
"KmsKeyId": "kmsKeyId",
"LoggingStatus": {
  "BucketName": "test-bucket",
  "LastFailureMessage": "test message",
  "LastFailureTime": "2020-08-09T13:00:00.000Z",
  "LastSuccessfulDeliveryTime": "2020-08-08T13:00:00.000Z",
  "LoggingEnabled": true,
  "S3KeyPrefix": "/"
},
"MaintenanceTrackName": "current",
"ManualSnapshotRetentionPeriod": -1,
"MasterUsername": "awsuser",
"NextMaintenanceWindowStartTime": "2020-08-09T13:00:00.000Z",
"NodeType": "dc2.large",
"NumberOfNodes": 2,
"PendingActions": [],
"PendingModifiedValues": {
  "AutomatedSnapshotRetentionPeriod": 0,
  "ClusterIdentifier": "clusterIdentifier",
  "ClusterType": "clusterType",
  "ClusterVersion": "clusterVersion",
  "EncryptionType": "None",
  "EnhancedVpcRouting": false,
  "MaintenanceTrackName": "maintenanceTrackName",
  "MasterUserPassword": "masterUserPassword",
  "NodeType": "dc2.large",
  "NumberOfNodes": 1,
  "PubliclyAccessible": true
},
"PreferredMaintenanceWindow": "sun:13:00-sun:13:30",
"PubliclyAccessible": true,
"ResizeInfo": {
  "AllowCancelResize": true,
  "ResizeType": "ClassicResize"
},
"RestoreStatus": {
  "CurrentRestoreRateInMegaBytesPerSecond": 15,
  "ElapsedTimeInSeconds": 120,
```

```

    "EstimatedTimeToCompletionInSeconds": 100,
    "ProgressInMegaBytes": 10,
    "SnapshotSizeInMegaBytes": 1500,
    "Status": "restoring"
  },
  "SnapshotScheduleIdentifier": "snapshotScheduleIdentifier",
  "SnapshotScheduleState": "ACTIVE",
  "VpcId": "vpc-example",
  "VpcSecurityGroups": [
    {
      "Status": "active",
      "VpcSecurityGroupId": "sg-example"
    }
  ]
}

```

AwsRoute53

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsRoute53` risorse.

AwsRoute53HostedZone

L'`AwsRoute53HostedZone` oggetto fornisce informazioni su una zona ospitata di Amazon Route 53, inclusi i quattro name server assegnati alla zona ospitata. Una zona ospitata rappresenta una raccolta di record che possono essere gestiti insieme, appartenenti a un unico nome di dominio principale.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsRoute53HostedZone` oggetto. Per visualizzare le descrizioni degli `AwsRoute53HostedZone` attributi, vedere [AwsRoute53 HostedZoneDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

"AwsRoute53HostedZone": {
  "HostedZone": {
    "Id": "Z06419652JEMG09TA2XKL",
    "Name": "asff.testing",
    "Config": {
      "Comment": "This is an example comment."
    }
  },
  "NameServers": [
    "ns-470.awsdns-32.net",

```



```

        "ns-1220.awsdns-12.org",
        "ns-205.awsdns-13.com",
        "ns-1960.awsdns-51.co.uk"
    ],
    "QueryLoggingConfig": {
        "CloudWatchLogsLogGroupArn": {
            "CloudWatchLogsLogGroupArn": "arn:aws:logs:us-east-1:123456789012:log-
group:asfftesting:*",
            "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
            "HostedZoneId": "Z00932193AF5H180PPNZD"
        }
    },
    "Vpcs": [
        {
            "Id": "vpc-05d7c6e36bc03ea76",
            "Region": "us-east-1"
        }
    ]
}

```

AwsS3

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per *AwsS3* le risorse.

AwsS3AccessPoint

AwsS3AccessPoint fornisce informazioni su un punto di accesso Amazon S3. I punti di accesso S3 sono endpoint di rete denominati collegati ai bucket S3 che è possibile utilizzare per eseguire operazioni sugli oggetti S3.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

AwsS3AccessPoint Per visualizzare le descrizioni degli *AwsS3AccessPoint* attributi, consulta [AWSS3 AccessPointDetails](#) nel AWS Security Hub riferimento API.

Esempio

```

"AwsS3AccessPoint": {
    "AccessPointArn": "arn:aws:s3:us-east-1:123456789012:accesspoint/asff-access-
point",
    "Alias": "asff-access-point-hrzrlukc5m36ft7okagglf3gmwluquse1b-s3alias",
    "Bucket": "DOC-EXAMPLE-BUCKET1",
    "BucketAccountId": "123456789012",
    "Name": "asff-access-point",

```

```
    "NetworkOrigin": "VPC",
    "PublicAccessBlockConfiguration": {
      "BlockPublicAcls": true,
      "BlockPublicPolicy": true,
      "IgnorePublicAcls": true,
      "RestrictPublicBuckets": true
    },
    "VpcConfiguration": {
      "VpcId": "vpc-1a2b3c4d5e6f1a2b3"
    }
  }
}
```

AwsS3AccountPublicAccessBlock

AwsS3AccountPublicAccessBlock fornisce informazioni sulla configurazione del blocco di accesso pubblico di Amazon S3 per gli account.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'*AwsS3AccountPublicAccessBlock* oggetto. Per visualizzare le descrizioni degli *AwsS3AccountPublicAccessBlock* attributi, consulta [AWSS3 AccountPublicAccessBlockDetails](#) nel AWS Security Hub riferimento API.

Esempio

```
"AwsS3AccountPublicAccessBlock": {
  "BlockPublicAcls": true,
  "BlockPublicPolicy": true,
  "IgnorePublicAcls": false,
  "RestrictPublicBuckets": true
}
```

AwsS3Bucket

L'*AwsS3Bucket* oggetto fornisce dettagli su un bucket Amazon S3.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. *AwsS3Bucket* Per visualizzare le descrizioni degli *AwsS3Bucket* attributi, consulta [AWSS3 BucketDetails](#) nel AWS Security Hub riferimento API.

Esempio

```
"AwsS3Bucket": {
```

```

"AccessControlList": "{\\"grantSet\\":null,\\"grantList\\":[{\\"grantee\\":{\\"id\\":
\\"4df55416215956920d9d056aa8b99803a294ea221222bb668b55a8c6bca81094\\"},\\"displayName
\\":null},\\"permission\\":\\"FullControl\\"},{\\"grantee\\":\\"AllUsers\\",\\"permission\\":
\\"ReadAcp\\"},{\\"grantee\\":\\"AuthenticatedUsers\\",\\"permission\\":\\"ReadAcp\\"}],
  "BucketLifecycleConfiguration": {
    "Rules": [
      {
        "AbortIncompleteMultipartUpload": {
          "DaysAfterInitiation": 5
        },
        "ExpirationDate": "2021-11-10T00:00:00.000Z",
        "ExpirationInDays": 365,
        "ExpiredObjectDeleteMarker": false,
        "Filter": {
          "Predicate": {
            "Operands": [
              {
                "Prefix": "tmp/",
                "Type": "LifecyclePrefixPredicate"
              },
              {
                "Tag": {
                  "Key": "ArchiveAge",
                  "Value": "9m"
                },
                "Type": "LifecycleTagPredicate"
              }
            ],
            "Type": "LifecycleAndOperator"
          }
        },
        "ID": "Move rotated logs to Glacier",
        "NoncurrentVersionExpirationInDays": -1,
        "NoncurrentVersionTransitions": [
          {
            "Days": 2,
            "StorageClass": "GLACIER"
          }
        ],
        "Prefix": "rotated/",
        "Status": "Enabled",
        "Transitions": [
          {
            "Date": "2020-11-10T00:00:00.000Z",

```

```

        "Days": 100,
        "StorageClass": "GLACIER"
      }
    ]
  }
]
},
"BucketLoggingConfiguration": {
  "DestinationBucketName": "s3serversideloggingbucket-858726136312",
  "LogFilePrefix": "buckettestreadwrite23435/"
},
"BucketName": "DOC-EXAMPLE-BUCKET1",
"BucketNotificationConfiguration": {
  "Configurations": [{
    "Destination": "arn:aws:lambda:us-east-1:123456789012:function:s3_public_write",
    "Events": [
      "s3:ObjectCreated:Put"
    ],
    "Filter": {
      "S3KeyFilter": {
        "FilterRules": [
          {
            "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.PREFIX",
            "Value": "pre"
          },
          {
            "Name": "AffS3BucketNotificationConfigurationS3KeyFilterRuleName.SUFFIX",
            "Value": "suf"
          }
        ]
      }
    },
    "Type": "LambdaConfiguration"
  ]
},
"BucketVersioningConfiguration": {
  "IsMfaDeleteEnabled": true,
  "Status": "Off"
},
"BucketWebsiteConfiguration": {
  "ErrorDocument": "error.html",
  "IndexDocumentSuffix": "index.html",
  "RedirectAllRequestsTo": {
    "HostName": "example.com",

```

```
"Protocol": "http"
},
"RoutingRules": [{
  "Condition": {
    "HttpErrorCodeReturnedEquals": "Redirected",
    "KeyPrefixEquals": "index"
  },
  "Redirect": {
    "HostName": "example.com",
    "HttpRedirectCode": "401",
    "Protocol": "HTTP",
    "ReplaceKeyPrefixWith": "string",
    "ReplaceKeyWith": "string"
  }
}]
},
"CreatedAt": "2007-11-30T01:46:56.000Z",
"ObjectLockConfiguration": {
  "ObjectLockEnabled": "Enabled",
  "Rule": {
    "DefaultRetention": {
      "Days": null,
      "Mode": "GOVERNANCE",
      "Years": 12
    }
  },
},
},
"OwnerId": "AIDACKCEVSQ6C2EXAMPLE",
"OwnerName": "s3bucketowner",
"PublicAccessBlockConfiguration": {
  "BlockPublicAcls": true,
  "BlockPublicPolicy": true,
  "IgnorePublicAcls": true,
  "RestrictPublicBuckets": true,
},
"ServerSideEncryptionConfiguration": {
  "Rules": [
    {
      "ApplyServerSideEncryptionByDefault": {
        "SSEAlgorithm": "AES256",
        "KMSEMasterKeyID": "12345678-abcd-abcd-abcd-123456789012"
      }
    }
  ]
}
```

```
}  
}
```

AwsS3Object

L'`AwsS3Object` oggetto fornisce informazioni su un oggetto Amazon S3.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsS3Object` oggetto. Per visualizzare le descrizioni degli `AwsS3Object` attributi, consulta [AWSS3 ObjectDetails](#) nel AWS Security Hub riferimento API.

Esempio

```
"AwsS3Object": {  
  "ContentType": "text/html",  
  "ETag": "\"30a6ec7e1a9ad79c203d05a589c8b400\"",  
  "LastModified": "2012-04-23T18:25:43.511Z",  
  "ServerSideEncryption": "aws:kms",  
  "SSEKMSKeyId": "arn:aws:kms:us-west-2:123456789012:key/4dff8393-e225-4793-a9a0-608ec069e5a7",  
  "VersionId": "ws310urg00jH_HH11IxPE35P.MELYaYh"  
}
```

AwsSageMaker

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsSageMaker` risorse.

AwsSageMakerNotebookInstance

L'`AwsSageMakerNotebookInstance` oggetto fornisce informazioni su un'istanza Amazon SageMaker Notebook, che è un'istanza di calcolo di machine learning che esegue l'app Jupyter Notebook.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto `AwsSageMakerNotebookInstance`. Per visualizzare le descrizioni degli `AwsSageMakerNotebookInstance` attributi, consulta [AwsSageMakerNotebookInstanceDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsSageMakerNotebookInstance": {
  "DirectInternetAccess": "Disabled",
  "InstanceMetadataServiceConfiguration": {
    "MinimumInstanceMetadataServiceVersion": "1",
  },
  "InstanceType": "ml.t2.medium",
  "LastModifiedTime": "2022-09-09 22:48:32.012000+00:00",
  "NetworkInterfaceId": "eni-06c09ac2541a1bed3",
  "NotebookInstanceArn": "arn:aws:sagemaker:us-east-1:001098605940:notebook-instance/sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm",
  "NotebookInstanceName":
  "SagemakerNotebookInstanceRootAccessDisabledComplia-8MYjcyofZiXm",
  "NotebookInstanceStatus": "InService",
  "PlatformIdentifier": "notebook-all-v1",
  "RoleArn": "arn:aws:iam::001098605940:role/sechub-SageMaker-1-scenar-SageMakerCustomExecution-1R0X32HGC38IW",
  "RootAccess": "Disabled",
  "SecurityGroups": [
    "sg-06b347359ab068745"
  ],
  "SubnetId": "subnet-02c0deea5fa64578e",
  "Url":
  "sagemakernotebookinstancerootaccessdisabledcomplia-8myjcyofzixm.notebook.us-east-1.sagemaker.aws",
  "VolumeSizeInGB": 5
}

```

AwsSecretsManager

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsSecretsManager risorse.

AwsSecretsManagerSecret

L'AwsSecretsManagerSecretoggetto fornisce dettagli su un segreto di Secrets Manager.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsSecretsManagerSecretoggetto. Per visualizzare le descrizioni degli AwsSecretsManagerSecret attributi, consulta [AwsSecretsManagerSecretDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsSecretsManagerSecret": {
  "RotationRules": {
    "AutomaticallyAfterDays": 30
  },
  "RotationOccurredWithinFrequency": true,
  "KmsKeyId": "kmsKeyId",
  "RotationEnabled": true,
  "RotationLambdaArn": "arn:aws:lambda:us-
west-2:777788889999:function:MyTestRotationLambda",
  "Deleted": false,
  "Name": "MyTestDatabaseSecret",
  "Description": "My test database secret"
}

```

AwsSns

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsSns risorse.

AwsSnsTopic

L'AwsSnsTopicoggetto contiene dettagli su un argomento di Amazon Simple Notification Service.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsSnsTopicoggetto. Per visualizzare le descrizioni degli AwsSnsTopic attributi, consulta [AwsSnsTopicDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsSnsTopic": {
  "ApplicationSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
ApplicationSuccessFeedbackRoleArn",
  "FirehoseFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseFailureFeedbackRoleArn",
  "FirehoseSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
FirehoseSuccessFeedbackRoleArn",
  "HttpFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpFailureFeedbackRoleArn",
  "HttpSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/
HttpSuccessFeedbackRoleArn",
  "KmsMasterKeyId": "alias/ExampleAlias",
  "Owner": "123456789012",
  "SqsFailureFeedbackRoleArn": "arn:aws:iam::123456789012:role/
SqsFailureFeedbackRoleArn",

```



```
"SqsSuccessFeedbackRoleArn": "arn:aws:iam::123456789012:role/SqsSuccessFeedbackRoleArn",
"Subscription": {
  "Endpoint": "http://sampleendpoint.com",
  "Protocol": "http"
},
"TopicName": "SampleTopic"
}
```

AwsSqs

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsSqs risorse.

AwsSqsQueue

L'AwsSqsQueueoggetto contiene informazioni su una coda di Amazon Simple Queue Service.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. AwsSqsQueue Per visualizzare le descrizioni degli AwsSqsQueue attributi, consulta [AwsSqsQueueDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsSqsQueue": {
  "DeadLetterTargetArn": "arn:aws:sqs:us-west-2:123456789012:queue/target",
  "KmsDataKeyReusePeriodSeconds": 60,,
  "KmsMasterKeyId": "1234abcd-12ab-34cd-56ef-1234567890ab",
  "QueueName": "sample-queue"
}
```

AwsSsm

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsSsm risorse.

AwsSsmPatchCompliance

L'AwsSsmPatchComplianceoggetto fornisce informazioni sullo stato di una patch su un'istanza in base alla linea di base della patch utilizzata per applicare la patch all'istanza.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsSsmPatchComplianceoggetto. Per visualizzare le descrizioni degli

AwsSsmPatchCompliance attributi, consulta [AwsSsmPatchComplianceDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsSsmPatchCompliance": {
  "Patch": {
    "ComplianceSummary": {
      "ComplianceType": "Patch",
      "CompliantCriticalCount": 0,
      "CompliantHighCount": 0,
      "CompliantInformationalCount": 0,
      "CompliantLowCount": 0,
      "CompliantMediumCount": 0,
      "CompliantUnspecifiedCount": 461,
      "ExecutionType": "Command",
      "NonCompliantCriticalCount": 0,
      "NonCompliantHighCount": 0,
      "NonCompliantInformationalCount": 0,
      "NonCompliantLowCount": 0,
      "NonCompliantMediumCount": 0,
      "NonCompliantUnspecifiedCount": 0,
      "OverallSeverity": "UNSPECIFIED",
      "PatchBaselineId": "pb-0c5b2769ef7cbe587",
      "PatchGroup": "ExamplePatchGroup",
      "Status": "COMPLIANT"
    }
  }
}
```

AwsStepFunctions

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le `AwsStepFunctions` risorse.

AwsStepFunctionStateMachine

L'oggetto `AwsStepFunctionStateMachine` fornisce informazioni su una macchina a `AWS Step Functions` stati, che è un flusso di lavoro costituito da una serie di passaggi basati sugli eventi.

L'esempio seguente mostra il `AWS Security Finding Format (ASFF)` per l'oggetto.

`AwsStepFunctionStateMachine` Per visualizzare le descrizioni degli

AwsStepFunctionStateMachine attributi, consulta [AwsStepFunctionStateMachine](#)l'AWS Security Hub API Reference.

Esempio

```
"AwsStepFunctionStateMachine": {
  "StateMachineArn": "arn:aws:states:us-
east-1:123456789012:stateMachine:StepFunctionsLogDisableNonCompliantResource-
fQLujTeXvwsb",
  "Name": "StepFunctionsLogDisableNonCompliantResource-fQLujTeXvwsb",
  "Status": "ACTIVE",
  "RoleArn": "arn:aws:iam::123456789012:role/teststepfunc-
StatesExecutionRole-1PNM71RV01UKT",
  "Type": "STANDARD",
  "LoggingConfiguration": {
    "Level": "OFF",
    "IncludeExecutionData": false
  },
  "TracingConfiguration": {
    "Enabled": false
  }
}
```

AwsWaf

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsWaf risorse.

AwsWafRateBasedRule

L'AwsWafRateBasedRule oggetto contiene dettagli su una regola AWS WAF basata sulla tariffa per le risorse globali. Una regola AWS WAF basata sulla tariffa fornisce impostazioni per indicare quando consentire, bloccare o contare una richiesta. Le regole basate sulla tariffa includono il numero di richieste che arrivano in un determinato periodo di tempo.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

AwsWafRateBasedRule Per visualizzare le descrizioni degli AwsWafRateBasedRule attributi, consulta [AwsWafRateBasedRuleDetails](#)l'AWS Security Hub API Reference.

Esempio

```
"AwsWafRateBasedRule":{
  "MatchPredicates" : [{
```

```

        "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
        "Negated" : "True",
        "Type" : "IPMatch" ,
    ]],
    "MetricName" : "MetricName",
    "Name" : "Test",
    "RateKey" : "IP",
    "RateLimit" : 235000,
    "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}

```

AwsWafRegionalRateBasedRule

L'oggetto `AwsWafRegionalRateBasedRule` contiene dettagli su una regola basata sulle tariffe per le risorse regionali. Una regola basata sulla tariffa fornisce impostazioni per indicare quando consentire, bloccare o contare una richiesta. Le regole basate sulla tariffa includono il numero di richieste che arrivano in un determinato periodo di tempo.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto.

`AwsWafRegionalRateBasedRule` Per visualizzare le descrizioni degli

`AwsWafRegionalRateBasedRule` attributi, consulta [AwsWafRegionalRateBasedRuleDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsWafRegionalRateBasedRule":{
  "MatchPredicates" : [{
    "DataId" : "391b7a7e-5f00-40d2-b114-3f27ceacbbb0",
    "Negated" : "True",
    "Type" : "IPMatch" ,
  }],
  "MetricName" : "MetricName",
  "Name" : "Test",
  "RateKey" : "IP",
  "RateLimit" : 235000,
  "RuleId" : "5dfb4085-f103-4ec6-b39a-d4a0dae5f47f"
}

```

AwsWafRegionalRule

L'oggetto `AwsWafRegionalRule` fornisce dettagli su una regola AWS WAF regionale. Questa regola identifica le richieste Web che desideri consentire, bloccare o contare.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'`AwsWafRegionalRule` oggetto. Per visualizzare le descrizioni degli `AwsWafRegionalRule` attributi, consulta [AwsWafRegionalRuleDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsWafRegionalRule": {
  "MetricName": "SampleWAF_Rule__Metric_1",
  "Name": "bb-waf-regional-rule-not-empty-conditions-compliant",
  "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de95fe",
  "PredicateList": [{
    "DataId": "127d9346-e607-4e93-9286-c1296fb5445a",
    "Negated": false,
    "Type": "GeoMatch"
  }]
}
```

AwsWafRegionalRuleGroup

L'`AwsWafRegionalRuleGroup` oggetto fornisce dettagli su un gruppo di regole AWS WAF regionali. Un gruppo di regole è una raccolta di regole predefinite che si aggiungono a un elenco di controllo degli accessi Web (Web ACL).

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto `AwsWafRegionalRuleGroup`. Per visualizzare le descrizioni degli `AwsWafRegionalRuleGroup` attributi, consulta [AwsWafRegionalRuleGroupDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsWafRegionalRuleGroup": {
  "MetricName": "SampleWAF_Metric_1",
  "Name": "bb-WAFClassicRuleGroupWithRuleCompliant",
  "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
  "Rules": [{
    "Action": {
      "Type": "ALLOW"
    }
  ]},
  "Priority": 1,
  "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
  "Type": "REGULAR"
```

```
}
```

AwsWafRegionalWebAcl

`AwsWafRegionalWebAcl` fornisce dettagli su un elenco AWS WAF regionale di controllo degli accessi Web (Web ACL). Un ACL Web contiene le regole che identificano le richieste che si desidera consentire, bloccare o contare.

Di seguito è riportato un esempio di `AwsWafRegionalWebAcl` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayV2Stage` attributi, consulta [AwsWafRegionalWebAclDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsWafRegionalWebAcl": {
  "DefaultAction": "ALLOW",
  "MetricName": "web-regional-webacl-metric-1",
  "Name": "WebACL_123",
  "RulesList": [
    {
      "Action": {
        "Type": "Block"
      },
      "Priority": 3,
      "RuleId": "24445857-852b-4d47-bd9c-61f05e4d223c",
      "Type": "REGULAR",
      "ExcludedRules": [
        {
          "ExclusionType": "Exclusion",
          "RuleId": "Rule_id_1"
        }
      ],
      "OverrideAction": {
        "Type": "OVERRIDE"
      }
    }
  ],
  "WebAclId": "443c76f4-2e72-4c89-a2ee-389d501c1f67"
}
```

AwsWafRule

`AwsWafRule` fornisce informazioni su una AWS WAF regola. Una AWS WAF regola identifica le richieste Web che desideri consentire, bloccare o contare.

Di seguito è riportato un esempio di `AwsWafRule` risultato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayV2Stage` attributi, consulta [AwsWafRuleDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsWafRule": {
  "MetricName": "AwsWafRule_Metric_1",
  "Name": "AwsWafRule_Name_1",
  "PredicateList": [{
    "DataId": "cdd225da-32cf-4773-1dc2-3bca3ed9c19c",
    "Negated": false,
    "Type": "GeoMatch"
  }],
  "RuleId": "8f651760-24fa-40a6-a9ed-4b60f1de953e"
}
```

AwsWafRuleGroup

`AwsWafRuleGroup` fornisce informazioni su un gruppo di AWS WAF regole. Un gruppo di AWS WAF regole è una raccolta di regole predefinite che si aggiungono a un elenco di controllo degli accessi Web (Web ACL).

Di seguito è riportato un esempio `AwsWafRuleGroup` trovato nel AWS Security Finding Format (ASFF). Per visualizzare le descrizioni degli `AwsApiGatewayV2Stage` attributi, consulta [AwsWafRuleGroupDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsWafRuleGroup": {
  "MetricName": "SampleWAF_Metric_1",
  "Name": "bb-WAFRuleGroupWithRuleCompliant",
  "RuleGroupId": "2012ca6d-e66d-4d9b-b766-bfb03ad77cfb",
  "Rules": [{
    "Action": {
      "Type": "ALLOW",
    },
  ]
}
```

```

    "Priority": 1,
    "RuleId": "cdd225da-32cf-4773-8dc5-3bca3ed9c19c",
    "Type": "REGULAR"
  ]]
}

```

AwsWafv2RuleGroup

L'AwsWafv2RuleGroupoggetto fornisce dettagli su un gruppo di regole AWS WAF V2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsWafv2RuleGroupoggetto. Per visualizzare le descrizioni degli AwsWafv2RuleGroup attributi, vedere [AwsWafv2 RuleGroupDetails](#) nell'AWS Security Hub API Reference.

Esempio

```

"AwsWafv2RuleGroup": {
  "Arn": "arn:aws:wafv2:us-east-1:123456789012:global/rulegroup/wafv2rulegroupasff/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Capacity": 1000,
  "Description": "Resource for ASFF",
  "Id": "a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Name": "wafv2rulegroupasff",
  "Rules": [{
    "Action": {
      "Allow": {
        "CustomRequestHandling": {
          "InsertHeaders": [
            {
              "Name": "AllowActionHeader1Name",
              "Value": "AllowActionHeader1Value"
            },
            {
              "Name": "AllowActionHeader2Name",
              "Value": "AllowActionHeader2Value"
            }
          ]
        }
      }
    },
    "Name": "RuleOne",
    "Priority": 1,
    "VisibilityConfig": {
      "CloudWatchMetricsEnabled": true,

```



```

    "MetricName": "rulegroupasff",
    "SampledRequestsEnabled": false
  }
}],
"VisibilityConfig": {
  "CloudWatchMetricsEnabled": true,
  "MetricName": "rulegroupasff",
  "SampledRequestsEnabled": false
}
}

```

AwsWafWebAcl

L'AwsWafWebAcl oggetto fornisce dettagli su un ACL AWS WAF web.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsWafWebAcl oggetto. Per visualizzare le descrizioni degli AwsWafWebAcl attributi, consulta [AwsWafWebAclDetails](#) l'AWS Security Hub API Reference.

Esempio

```

"AwsWafWebAcl": {
  "DefaultAction": "ALLOW",
  "Name": "MyWafAcl",
  "Rules": [
    {
      "Action": {
        "Type": "ALLOW"
      },
      "ExcludedRules": [
        {
          "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98"
        }
      ],
      "OverrideAction": {
        "Type": "NONE"
      },
      "Priority": 1,
      "RuleId": "5432a230-0113-5b83-bbb2-89375c5bfa98",
      "Type": "REGULAR"
    }
  ],
  "WebAclId": "waf-1234567890"
}

```

```
}
```

AwsWafv2WebAc1

L'AwsWafv2WebAc1 oggetto fornisce dettagli su un ACL Web AWS WAF V2.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'oggetto. AwsWafv2WebAc1 Per visualizzare le descrizioni degli AwsWafv2WebAc1 attributi, vedere [AwsWafv2 WebAc1Details](#) nell'AWS Security Hub API Reference.

Esempio

```
"AwsWafv2WebAc1": {
  "Arn": "arn:aws:wafv2:us-east-1:123456789012:regional/webacl/WebACL-RoaD4QexqSxG/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Capacity": 1326,
  "CaptchaConfig": {
    "ImmunityTimeProperty": {
      "ImmunityTime": 500
    }
  },
  "DefaultAction": {
    "Block": {}
  },
  "Description": "Web ACL for JsonBody testing",
  "ManagedbyFirewallManager": false,
  "Name": "WebACL-RoaD4QexqSxG",
  "Rules": [{
    "Action": {
      "RuleAction": {
        "Block": {}
      }
    },
    "Name": "TestJsonBodyRule",
    "Priority": 1,
    "VisibilityConfig": {
      "SampledRequestsEnabled": true,
      "CloudWatchMetricsEnabled": true,
      "MetricName": "JsonBodyMatchMetric"
    }
  }],
  "VisibilityConfig": {
    "SampledRequestsEnabled": true,
```

```
    "CloudWatchMetricsEnabled": true,  
    "MetricName": "TestingJsonBodyMetric"  
  }  
}
```

AwsXray

Di seguito sono riportati alcuni esempi del AWS Security Finding Format per le AwsXray risorse.

AwsXrayEncryptionConfig

L'AwsXrayEncryptionConfig oggetto contiene informazioni sulla configurazione di crittografia per AWS X-Ray.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'AwsXrayEncryptionConfig oggetto. Per visualizzare le descrizioni degli AwsXrayEncryptionConfig attributi, consulta [AwsXrayEncryptionConfigDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"AwsXRayEncryptionConfig":{  
  "KeyId": "arn:aws:kms:us-east-2:222222222222:key/example-key",  
  "Status": "UPDATING",  
  "Type": "KMS"  
}
```

Container

I dettagli del container correlati a un risultato.

L'esempio seguente mostra il AWS Security Finding Format (ASFF) per l'Container oggetto. Per visualizzare le descrizioni degli Container attributi, consulta [ContainerDetails](#) l'AWS Security Hub API Reference.

Esempio

```
"Container": {  
  "ContainerRuntime": "docker",  
  "ImageId": "image12",  
  "ImageName": "1111111/  
knotejs@sha256:372131c9fef1111111111111111115f4ed3ea5f9dce4dc3bd34ce21846588a3",
```

```
"LaunchedAt": "2018-09-29T01:25:54Z",
"Name": "knote",
"Privileged": true,
"VolumeMounts": [{
  "Name": "vol-03909e9",
  "MountPath": "/mnt/etc"
}]
}
```

Other

L'Otheroggetto consente di fornire campi e valori personalizzati. L'Otheroggetto viene utilizzato nei seguenti casi.

- Il tipo di risorsa non ha un Details oggetto corrispondente. Per fornire dettagli sulla risorsa, si utilizza l'Otheroggetto.
- L'Detailsoggetto per il tipo di risorsa non include tutti gli attributi che si desidera compilare. In questo caso, utilizzate l'Detailsoggetto relativo al tipo di risorsa per compilare gli attributi disponibili. Utilizzate l'Otheroggetto per compilare gli attributi che non sono presenti nell'oggetto specifico del tipo.
- Il tipo di risorsa non è uno dei tipi forniti. In questo caso, Resource .Type impostate e utilizzate l'Otheroggetto per compilare i dettagli. Other

Tipo: mappa di un massimo di 50 coppie chiave-valore

Ogni coppia chiave/valore deve soddisfare i seguenti requisiti.

- La chiave deve contenere meno di 128 caratteri.
- Il valore deve contenere meno di 1.024 caratteri.

Approfondimenti nel AWS Security Hub

Un AWS Security Hub insight è una raccolta di risultati correlati. Identificano un'area di sicurezza che richiede attenzione e intervento. Ad esempio, un'informazione dettagliata potrebbe indicare le istanze EC2 con risultati che rilevano procedure di sicurezza inadeguate. Un'informazione dettagliata riunisce i risultati di tutti i provider di ricerca.

Ogni informazione dettagliata è definita da un gruppo per istruzione e filtri facoltativi. Il gruppo per istruzione indica come raggruppare i risultati corrispondenti e identifica il tipo di elemento a cui si applica l'informazione dettagliata. Ad esempio, se un'informazione dettagliata è raggruppata per identificatore di risorsa, l'informazione dettagliata produce un elenco di identificatori di risorse. I filtri opzionali identificano i risultati corrispondenti all'analisi. Ad esempio, potresti voler visualizzare solo i risultati di fornitori specifici o i risultati associati a tipi specifici di risorse.

Security Hub offre diverse informazioni gestite integrate. Non è possibile modificare o eliminare le informazioni dettagliate gestite.

Puoi anche creare informazioni dettagliate personalizzate per tenere traccia dei problemi di sicurezza univoci per l'ambiente AWS e il suo utilizzo.

Un'analisi restituisce risultati solo se sono state abilitate integrazioni o standard che producono risultati corrispondenti. Ad esempio, il managed insight 29. Top resources in base al numero di controlli CIS non riusciti restituisce risultati solo se si abilita lo standard CIS AWS Foundations.

Argomenti

- [Visualizzazione e filtraggio dell'elenco di approfondimenti](#)
- [Visualizzazione e azioni su risultati e risultati di informazione dettagliata](#)
- [Informazioni dettagliate gestite](#)
- [Informazioni personalizzate](#)

Visualizzazione e filtraggio dell'elenco di approfondimenti

La pagina Insights mostra l'elenco degli approfondimenti disponibili.

Per impostazione predefinita, l'elenco mostra sia gli approfondimenti gestiti che quelli personalizzati. Per filtrare l'elenco di approfondimenti in base al tipo di analisi, scegli il tipo di analisi dal menu a discesa accanto al campo del filtro.

- Per visualizzare tutti gli approfondimenti disponibili, scegli Tutti gli approfondimenti. Questa è l'opzione predefinita.
- Per visualizzare solo le informazioni gestite, scegli le informazioni gestite da Security Hub.
- Per visualizzare solo approfondimenti personalizzati, scegli Informazioni personalizzate.

Puoi anche filtrare l'elenco degli approfondimenti in base al testo nel nome degli approfondimenti.

Nel campo del filtro, digita il testo da utilizzare per filtrare l'elenco. Il filtro non fa distinzione tra maiuscole e minuscole. Il filtro cerca gli approfondimenti che contengono il testo in un punto qualsiasi del nome dell'approfondimento.

Visualizzazione e azioni su risultati e risultati di informazione dettagliata

Per ogni analisi, AWS Security Hub determina innanzitutto i risultati che corrispondono ai criteri di filtro, quindi utilizza l'attributo grouping per raggruppare i risultati corrispondenti.

Dalla pagina della console Insights, puoi visualizzare e intervenire sui risultati e sui risultati.

Se abiliti l'aggregazione tra aree geografiche, nella regione di aggregazione i risultati per gli approfondimenti gestiti includono i risultati della regione di aggregazione e delle regioni collegate. Per i risultati di analisi personalizzati, se gli approfondimenti non vengono filtrati per regione, i risultati includono i risultati della regione di aggregazione e delle regioni collegate.

In altre regioni, i risultati delle analisi si riferiscono solo a quella regione.

Per informazioni su come configurare l'aggregazione tra regioni, vedere [Aggregazione tra regioni](#)

Visualizzazione e azione dei risultati delle analisi (console)

I risultati di informazione dettagliata sono costituiti dall'elenco raggruppato dei risultati dell'informazione dettagliata. Ad esempio, se gli approfondimenti sono raggruppati per identificatori di risorse, i risultati degli approfondimenti sono l'elenco degli identificatori di risorse. Ogni voce nell'elenco dei risultati indica il numero di risultati corrispondenti per la voce.

Tieni presente che se i risultati sono raggruppati per identificatore di risorsa o tipo di risorsa, i risultati includono tutte le risorse nei risultati corrispondenti. Ciò include le risorse che hanno un tipo diverso dal tipo di risorsa specificato nei criteri di filtro. Ad esempio, un'analisi identifica i risultati associati ai

bucket S3. Se un risultato corrispondente contiene sia una risorsa bucket S3 che una risorsa chiave di accesso IAM, i risultati dell'analisi elencano entrambe le risorse.

L'elenco dei risultati è ordinato dal numero maggiore al numero minore di risultati corrispondenti.

Security Hub può visualizzare solo 100 risultati. Se sono presenti più di 100 valori di raggruppamento, vengono visualizzati solo i primi 100.

Oltre all'elenco dei risultati, i risultati dell'informazione dettagliata visualizzano una serie di grafici riepilogativi con il numero di risultati corrispondenti per gli attributi seguenti.

- Etichetta di gravità: numero di risultati per ciascuna etichetta di gravità
- Account AWS ID: i cinque principali ID di account per i risultati corrispondenti
- Tipo di risorsa: i cinque principali tipi di risorse per i risultati corrispondenti
- ID risorsa: i cinque principali ID di risorsa per i risultati corrispondenti
- Nome del prodotto: i cinque principali fornitori di risultati per la ricerca dei risultati corrispondenti

Se sono state configurate azioni personalizzate, puoi inviare i risultati selezionati a un'azione personalizzata. L'azione deve essere associata a una CloudWatch regola per il tipo di Security Hub Insight Results evento. Per informazioni, consulta [the section called “Risposta e correzione automatizzate”](#).

Se non sono state configurate azioni personalizzate, il menu Azioni è disabilitato.

Per visualizzare e intraprendere un'azione nell'elenco dei risultati di informazione dettagliata

1. Aprire la console AWS Security Hub all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, seleziona Informazioni dettagliate.
3. Per visualizzare l'elenco dei risultati di informazione dettagliata, scegliere il nome dell'informazione dettagliata.
4. Selezionare la casella di controllo per ogni risultato da inviare all'azione personalizzata.
5. Dal menu Actions (Azioni) scegliere l'azione personalizzata.

Visualizzazione dei risultati delle analisi (API Security Hub, AWS CLI)

Per visualizzare i risultati degli approfondimenti, puoi utilizzare una chiamata API o il AWS Command Line Interface.

Per visualizzare i risultati delle analisi (API Security Hub, AWS CLI)

- API Security Hub: utilizza l'[GetInsightResults](#) operazione. Per identificare le informazioni da cui ottenere risultati, è necessario l'analisi ARN. Per ottenere gli insight ARN per approfondimenti personalizzati, utilizza l'[GetInsights](#) operazione.
- AWS CLI— Nella riga di comando, eseguire il [get-insight-results](#) comando.

```
aws securityhub get-insight-results --insight-arn <insight ARN>
```

Esempio:

```
aws securityhub get-insight-results --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Visualizzazione dei risultati per un risultato approfondito (console)

Dall'elenco dei risultati di informazione dettagliata puoi visualizzare l'elenco dei risultati per ciascun risultato.

Per visualizzare e intraprendere azioni sui risultati di informazione dettagliata

1. Aprire la console AWS Security Hub all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, seleziona Informazioni dettagliate.
3. Per visualizzare l'elenco dei risultati di informazione dettagliata, scegliere il nome dell'informazione dettagliata.
4. Per visualizzare l'elenco dei risultati per un risultato di informazione dettagliata, scegliere la voce dall'elenco dei risultati.

L'elenco dei risultati mostra i risultati attivi per il risultato di informazioni dettagliate selezionato che hanno uno stato del flusso di lavoro NEW o NOTIFIED.

Dall'elenco dei risultati puoi eseguire le seguenti operazioni.

- [Modificare filtri e raggruppamento dell'elenco](#)
- [Visualizzare i dettagli per i singoli risultati](#)
- [Aggiornare lo stato del flusso di lavoro dei risultati](#)

- [Inviare i risultati alle operazioni personalizzate](#)

Informazioni dettagliate gestite

AWS Security Hub fornisce diverse informazioni gestite.

Non è possibile modificare o eliminare le informazioni gestite da Security Hub. Puoi [visualizzare e agire in merito ai risultati e ai risultati di informazione dettagliata](#). Puoi anche [utilizzare un'informazione dettagliata gestita come base per una nuova informazione dettagliata personalizzata](#).

Come tutte le informazioni dettagliate, un'informazione dettagliata gestita restituisce i risultati solo se sono state abilitate le integrazioni di prodotti o standard di sicurezza che producono risultati corrispondenti.

Per gli approfondimenti raggruppati per identificatore di risorsa, i risultati includono gli identificatori di tutte le risorse nei risultati corrispondenti. Ciò include le risorse che hanno un tipo diverso dal tipo di risorsa indicato nei criteri di filtro. Ad esempio, insight 2 identifica i risultati associati ai bucket Amazon S3. Se un risultato corrispondente contiene sia una risorsa bucket S3 che una risorsa chiave di accesso IAM, i risultati dell'analisi includono entrambe le risorse.

Security Hub offre le seguenti informazioni gestite:

1. Risorse AWS con la maggior parte dei risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/1`

Raggruppati per: Identificatore di risorse

Ricerca dei filtri:

- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

2. Bucket S3 con autorizzazioni di lettura o scrittura pubblica

ARN: `arn:aws:securityhub:::insight/securityhub/default/10`

Raggruppati per: identificatore di risorse

Ricerca dei filtri:

- Il tipo inizia con Effects/Data Exposure

- Il tipo di risorsa è `AwsS3Bucket`
- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

3. AMI che generano la maggior parte dei risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/3`

Raggruppati per: ID dell'immagine dell'istanza EC2

Ricerca dei filtri:

- Il tipo di risorsa è `AwsEc2Instance`
- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

4. Istanze EC2 coinvolte in TTPs (Tactics, Techniques, and Procedures) note

ARN: `arn:aws:securityhub:::insight/securityhub/default/14`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo inizia con TTPs
- Il tipo di risorsa è `AwsEc2Instance`
- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

5. AWSpresidi con attività sospette relative alle chiavi di accesso

ARN: `arn:aws:securityhub:::insight/securityhub/default/9`

Raggruppati per: nome principale della chiave di accesso IAM

Ricerca dei filtri:

- Il tipo di risorsa è `AwsIamAccessKey`
- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

6. Istanze di risorse AWS che non soddisfano standard di sicurezza o best practice

ARN: `arn:aws:securityhub:::insight/securityhub/default/6`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo è Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

7. Risorse AWS associate a potenziale esfiltrazione di dati

ARN: `arn:aws:securityhub:::insight/securityhub/default/7`

Raggruppati per:: Resource ID

Ricerca dei filtri:

- Il tipo inizia con Effects/Data Exfiltration/
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

8. Risorse AWS associate a consumo di risorse non autorizzate

ARN: `arn:aws:securityhub:::insight/securityhub/default/8`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo inizia con Effects/Resource Consumption
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

9. Bucket S3 che non soddisfano standard di sicurezza o best practice

ARN: `arn:aws:securityhub:::insight/securityhub/default/11`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo di risorsa è AwsS3Bucket
- Il tipo è Software and Configuration Checks/Industry and Regulatory Standards/AWS Security Best Practices

- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

10. Bucket S3 con dati sensibili

ARN: `arn:aws:securityhub:::insight/securityhub/default/12`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo di risorsa è `AwsS3Bucket`
- Il tipo inizia con `Sensitive Data Identifications/`
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

11. Credenziali che possono essere state divulgate

ARN: `arn:aws:securityhub:::insight/securityhub/default/13`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo inizia con `Sensitive Data Identifications/Passwords/`
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

12. Istanze EC2 con patch di sicurezza mancanti per vulnerabilità importanti

ARN: `arn:aws:securityhub:::insight/securityhub/default/16`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo inizia con `Software and Configuration Checks/Vulnerabilities/CVE`
- Il tipo di risorsa è `AwsEc2Instance`
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

13. Istanze EC2 con comportamento insolito generale

ARN: `arn:aws:securityhub:::insight/securityhub/default/17`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo inizia con Unusual Behaviors
- Il tipo di risorsa è AwsEc2Instance
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

14. Istanze EC2 che dispongono di porte accessibili da Internet

ARN: `arn:aws:securityhub:::insight/securityhub/default/18`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo inizia con Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- Il tipo di risorsa è AwsEc2Instance
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

15. Istanze EC2 che non soddisfano standard di sicurezza o best practice

ARN: `arn:aws:securityhub:::insight/securityhub/default/19`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo inizia con uno dei seguenti valori:
 - Software and Configuration Checks/Industry and Regulatory Standards/
 - Software and Configuration Checks/AWS Security Best Practices
- Il tipo di risorsa è AwsEc2Instance
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

16. Istanze EC2 aperte a Internet

ARN: `arn:aws:securityhub:::insight/securityhub/default/21`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo inizia con Software and Configuration Checks/AWS Security Best Practices/Network Reachability
- Il tipo di risorsa è AwsEc2Instance
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

17. Istanze EC2 associate a riconoscimento avversario

ARN: `arn:aws:securityhub:::insight/securityhub/default/22`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo inizia con TTPS/Discovery/Recon
- Il tipo di risorsa è AwsEc2Instance
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

18. Risorse AWS associate a malware

ARN: `arn:aws:securityhub:::insight/securityhub/default/23`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo inizia con uno dei seguenti valori:
 - Effects/Data Exfiltration/Trojan
 - TTPs/Initial Access/Trojan
 - TTPs/Command and Control/Backdoor
 - TTPs/Command and Control/Trojan
 - Software and Configuration Checks/Backdoor
 - Unusual Behaviors/VM/Backdoor
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

19. Risorse AWS associate a problemi di criptovaluta

ARN: `arn:aws:securityhub:::insight/securityhub/default/24`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo inizia con uno dei seguenti valori:
 - `Effects/Resource Consumption/Cryptocurrency`
 - `TTPs/Command and Control/CryptoCurrency`
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

20. Risorse AWS con i tentativi di accesso non autorizzato

ARN: `arn:aws:securityhub:::insight/securityhub/default/25`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo inizia con uno dei seguenti valori:
 - `TTPs/Command and Control/UnauthorizedAccess`
 - `TTPs/Initial Access/UnauthorizedAccess`
 - `Effects/Data Exfiltration/UnauthorizedAccess`
 - `Unusual Behaviors/User/UnauthorizedAccess`
 - `Effects/Resource Consumption/UnauthorizedAccess`
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

21. Indicatori di intelligence delle minacce con la maggior parte delle occorrenze nell'ultima settimana

ARN: `arn:aws:securityhub:::insight/securityhub/default/26`

Ricerca di filtri:

- Creato negli ultimi 7 giorni

22. Principali account per numero di risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/27`

Raggruppati per: ID Account AWS

Ricerca dei filtri:

- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

23. Principali prodotti per numero di risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/28`

Raggruppati per: Nome del prodotto

Ricerca dei filtri:

- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

24. Gravità per numero di risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/29`

Raggruppati per: etichetta di severità

Ricerca dei filtri:

- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

25. Principali bucket S3 per numero di risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/30`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo di risorsa è AwsS3Bucket
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

26. Principali istanze EC2 per numero di risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/31`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Il tipo di risorsa è `AwsEc2Instance`
- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

27. Principali AMI per numero di risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/32`

Raggruppati per: ID dell'immagine dell'istanza EC2

Ricerca dei filtri:

- Il tipo di risorsa è `AwsEc2Instance`
- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

28. Principali utenti IAM per numero di risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/33`

Raggruppati per: ID della chiave di accesso IAM

Ricerca di filtri:

- Il tipo di risorsa è `AwsIamAccessKey`
- Lo stato del record è `ACTIVE`
- Lo stato del flusso di lavoro è `NEW` o `NOTIFIED`

29. Principali risorse per numero di controlli CIS non riusciti

ARN: `arn:aws:securityhub:::insight/securityhub/default/34`

Raggruppati per: Resource ID

Ricerca dei filtri:

- L'ID generatore inizia con `arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0/rule`
- Aggiornato nell'ultimo giorno
- Lo stato di conformità è `FAILED`

- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

30. Principali integrazioni per numero di risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/35`

Raggruppato per: ARN del prodotto

Ricerca dei filtri:

- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

31. Risorse con più controlli di sicurezza con esito negativo

ARN: `arn:aws:securityhub:::insight/securityhub/default/36`

Raggruppati per: Resource ID

Ricerca dei filtri:

- Aggiornato nell'ultimo giorno
- Lo stato di conformità è FAILED
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

32. Utenti IAM con attività sospette

ARN: `arn:aws:securityhub:::insight/securityhub/default/37`

Raggruppati per: utente IAM

Ricerca dei filtri:

- Il tipo di risorsa è `AwsIamUser`
- Lo stato del record è ACTIVE
- Lo stato del flusso di lavoro è NEW o NOTIFIED

33. Risorse con il maggior numero di AWS Health risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/38`

Raggruppati per: Resource ID

Ricerca dei filtri:

- `ProductName` è uguale `Health`

34. Risorse con il maggior numero di AWS Config risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/39`

Raggruppati per: Resource ID

Ricerca dei filtri:

- `ProductName` è uguale `Config`

35. Applicazioni con il maggior numero di risultati

ARN: `arn:aws:securityhub:::insight/securityhub/default/40`

Raggruppati per: ResourceApplicationArn

Ricerca dei filtri:

- `RecordState` è uguale `ACTIVE`
- `Workflow.Status` è uguale o `NEW NOTIFIED`

Informazioni personalizzate

Oltre alle informazioni gestite da Security Hub, puoi creare approfondimenti personalizzati in Security Hub per tenere traccia di problemi specifici del tuo ambiente. Le informazioni personalizzate forniscono un modo per tenere traccia di un sottoinsieme curato di problemi.

Ecco alcuni esempi di approfondimenti personalizzati che possono essere utili da configurare:

- Se possiedi un account amministratore, puoi configurare un'analisi personalizzata per tenere traccia dei risultati critici e ad alta gravità che influiscono sugli account dei membri.
- Se ti affidi a uno specifico [integrato AWS servizio](#), puoi impostare un'analisi personalizzata per tenere traccia dei risultati critici e ad alta gravità di quel servizio.
- Se ti affidi a [integrazione con terze parti](#), puoi impostare un'analisi personalizzata per tenere traccia dei risultati critici e ad alta gravità di quel prodotto integrato.

Puoi creare informazioni dettagliate personalizzate completamente nuove oppure iniziare da un'informazione dettagliata personalizzata o gestita già esistente.

Ogni informazione dettagliata viene configurata con le seguenti opzioni.

- **Attributo di raggruppamento**— L'attributo di raggruppamento determina quali elementi vengono visualizzati nell'elenco dei risultati di analisi. Ad esempio, se l'attributo di raggruppamento è Nome del prodotto, quindi i risultati di analisi mostrano il numero di risultati associati a ciascun fornitore di ricerca.
- **Filtri opzionali**— I filtri restringono i risultati corrispondenti per le informazioni.

Quando interroga i risultati, Security Hub applica la logica BOOLEANA AND al set di filtri. In altre parole, un risultato corrisponde solo se corrisponde a tutti i filtri forniti. Ad esempio, se i filtri sono "Nome prodotto è GuardDuty" e "Tipo di risorsa è AwsS3Bucket", i risultati corrispondenti devono corrispondere a entrambi questi criteri.

Tuttavia, Security Hub applica la logica OR booleana ai filtri che utilizzano lo stesso attributo ma valori diversi. Ad esempio, se i filtri sono «Il nome del prodotto è GuardDuty» e «Il nome del prodotto è Amazon Inspector», quindi una scoperta corrisponde se è stata generata da uno dei due GuardDuty o Amazon Inspector.

Tieni presente che se utilizzi l'identificatore o il tipo di risorsa come attributo di raggruppamento, i risultati di analisi includono tutte le risorse presenti nei risultati corrispondenti. L'elenco non è limitato alle risorse che corrispondono a un filtro per tipo di risorsa. Ad esempio, un'analisi identifica i risultati associati ai bucket S3 e li raggruppa per identificatore di risorsa. Una scoperta corrispondente contiene sia una risorsa bucket S3 che una risorsa chiave di accesso IAM. I risultati delle informazioni includono entrambe le risorse.

Creazione di informazioni personalizzate (console)

Dalla console è possibile creare un'informazione dettagliata completamente nuova.

Per creare un'analisi personalizzata

1. Apri il **AWS Console Security Hub** su <https://console.aws.amazon.com/securityhub/>.
2. Nel riquadro di navigazione, seleziona **Informazioni dettagliate**.
3. Scegliere **Create insight (Crea informazione dettagliata)**.
4. Per selezionare l'attributo di raggruppamento per l'informazione dettagliata:
 - a. Scegli la casella di ricerca per visualizzare le opzioni di filtro.
 - b. Scegliere **Group by (Raggruppa per)**.

- c. Seleziona l'attributo da utilizzare per raggruppare i risultati associati a questa analisi.
- d. Seleziona Apply (Applica).
5. (Facoltativo) Scegliere eventuali filtri aggiuntivi da utilizzare per questa informazione dettagliata. Per ogni filtro, definisci i criteri del filtro, quindi scegli Apply.
6. Scegliere Create insight (Crea informazione dettagliata).
7. Immettere un Insight name (Nome informazione dettagliata) e scegliere Create insight (Crea informazione dettagliata).

Creazione di un'analisi personalizzata (programmatica)

Scegli il tuo metodo preferito e segui i passaggi per creare in modo programmatico un'analisi personalizzata in Security Hub. È possibile specificare filtri per restringere la raccolta di risultati nell'analisi a un sottoinsieme specifico.

Le schede seguenti includono istruzioni in alcune lingue per creare informazioni personalizzate. Per il supporto in altre lingue, consulta [Strumenti su cui costruire AWS](#).

Security Hub API

1. Esegui il [CreateInsight](#) operazione.
2. Compila il `Name` parametro con un nome per la tua analisi personalizzata.
3. Compila il `Filters` parametro per specificare quali risultati includere nell'analisi.
4. Compila il `GroupByAttribute` parametro per specificare quale attributo viene utilizzato per raggruppare i risultati inclusi nell'analisi.
5. Facoltativamente, compila il `SortCriteria` parametro per ordinare i risultati in base a un campo specifico.

Se hai abilitato [aggregazione interregionale](#) e chiami questa API dalla regione di aggregazione, l'analisi si applica alla corrispondenza dei risultati nell'aggregazione e nelle regioni collegate.

AWS CLI

1. Nella riga di comando, esegui [create-insight](#) comando.
2. Compila il `name` parametro con un nome per la tua analisi personalizzata.
3. Compila il `filters` parametro per specificare quali risultati includere nell'analisi.

4. Compila il `group-by-attribute` parametro per specificare quale attributo viene utilizzato per raggruppare i risultati inclusi nell'analisi.

Se hai abilitato [aggregazione interregionale](#) ed esegui questo comando dalla regione di aggregazione, l'analisi si applica ai risultati corrispondenti dell'aggregazione e delle regioni collegate.

```
aws securityhub create-insight --name <insight name> --filters <filter values> --group-by-attribute <attribute name>
```

Esempio

```
aws securityhub create-insight --name "Critical role findings" --filters '{"ResourceType": [{"Comparison": "EQUALS", "Value": "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "CRITICAL"}]}' --group-by-attribute "ResourceId"
```

PowerShell

1. Usa il `New-SHUBInsight` cmdlet.
2. Compila il `Name` parametro con un nome per la tua analisi personalizzata.
3. Compila il `Filter` parametro per specificare quali risultati includere nell'analisi.
4. Compila il `GroupByAttribute` parametro per specificare quale attributo viene utilizzato per raggruppare i risultati inclusi nell'analisi.

Se hai abilitato [aggregazione interregionale](#) e utilizza questo cmdlet della regione di aggregazione, le informazioni si applicano alla corrispondenza dei risultati dell'aggregazione e delle regioni collegate.

Esempio

```
$Filter = @{
    AwsAccountId = [Amazon.SecurityHub.Model.StringFilter]{
        Comparison = "EQUALS"
        Value = "XXX"
    }
    ComplianceStatus = [Amazon.SecurityHub.Model.StringFilter]{
        Comparison = "EQUALS"
```

```
        Value = 'FAILED'
    }
}
New-SHUBInsight -Filter $Filter -Name TestInsight -GroupByAttribute ResourceId
```

Modifica di un'analisi personalizzata (console)

Puoi modificare un'informazione dettagliata personalizzata esistente per cambiare il valore di raggruppamento e i filtri. Dopo aver apportato le modifiche, puoi salvare gli aggiornamenti nell'informazione dettagliata originale o salvare la versione aggiornata come una nuova informazione dettagliata.

Per modificare un'informazione dettagliata

1. Apri ilAWSConsole Security Hub su<https://console.aws.amazon.com/securityhub/>.
2. Nel riquadro di navigazione, seleziona Informazioni dettagliate .
3. Scegliere l'informazione dettagliata personalizzata da modificare.
4. Modifica la configurazione di Insight in base alle tue esigenze.
 - Per modificare l'attributo utilizzato per raggruppare i risultati nell'informazione dettagliata:
 - a. Per rimuovere il raggruppamento esistente, scegliXaccanto alRaggruppa perimpostazione.
 - b. Scegli la casella di ricerca.
 - c. Selezionare l'attributo da utilizzare per il raggruppamento.
 - d. Seleziona Apply (Applica).
 - Per rimuovere un filtro dall'analisi, scegli il cerchiatoXaccanto al filtro.
 - Per aggiungere un filtro all'informazione dettagliata:
 - a. Scegli la casella di ricerca.
 - b. Selezionare l'attributo e il valore da utilizzare come filtro.
 - c. Seleziona Apply (Applica).
5. Al termine degli aggiornamenti, scegliere Save insight (Salva informazione dettagliata).
6. Quando richiesto, eseguire una delle operazioni seguenti:
 - Per aggiornare l'informazione dettagliata esistente per riflettere le modifiche, scegliere Update **<Insight_Name>** (Aggiorna <Insight_Name>) e selezionare Save insight (Salva informazione dettagliata).

- Per creare una nuova informazione dettagliata con gli aggiornamenti, scegliere Save new insight (Salva nuova informazione dettagliata). Immettere un Insight name (Nome informazione dettagliata), quindi scegliere Save insight (Salva informazione dettagliata).

Modifica di un'analisi personalizzata (programmatica)

Per modificare un'analisi personalizzata, scegli il tuo metodo preferito e segui le istruzioni.

Security Hub API

1. Esegui il [UpdateInsight](#) operazione.
2. Per identificare le informazioni personalizzate, fornisci l'Amazon Resource Name (ARN) dell'insight. Per ottenere l'ARN di un'analisi personalizzata, esegui [GetInsights](#) operazione.
3. Aggiorna il `Name`, `Filters`, e `GroupByAttribute` parametri in base alle esigenze.

AWS CLI

1. Nella riga di comando, esegui [update-insight](#) comando.
2. Per identificare le informazioni personalizzate, fornisci l'Amazon Resource Name (ARN) dell'insight. Per ottenere l'ARN di un'analisi personalizzata, esegui [get-insights](#) comando.
3. Aggiorna il `name`, `filters`, e `group-by-attribute` parametri in base alle esigenze.

```
aws securityhub update-insight --insight-arn <insight ARN> [--name <new name>] [--filters <new filters>] [--group-by-attribute <new grouping attribute>]
```

Esempio

```
aws securityhub update-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111" --filters '{"ResourceType": [{"Comparison": "EQUALS", "Value": "AwsIamRole"}], "SeverityLabel": [{"Comparison": "EQUALS", "Value": "HIGH"}]}' --name "High severity role findings"
```

PowerShell

1. Usa il `Update-SHUBInsightcmdlet`.

2. Per identificare le informazioni personalizzate, fornisci l'Amazon Resource Name (ARN) dell'insight. Per ottenere l'ARN di un'analisi personalizzata, usa `Get-SHUBInsightcmdlet`.
3. Aggiorna il `Name`, `Filter`, e `GroupByAttribute` parametri in base alle esigenze.

Esempio

```
$Filter = @{
    ResourceType = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "AwsIamRole"
    }
    SeverityLabel = [Amazon.SecurityHub.Model.StringFilter]@{
        Comparison = "EQUALS"
        Value = "HIGH"
    }
}

Update-SHUBInsight -InsightArn "arn:aws:securityhub:us-
west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111" -Filter $Filter -Name "High severity role findings"
```

Creazione di nuove informazioni personalizzate da un'analisi gestita (console)

Non è possibile modificare o eliminare un'informazione dettagliata gestita. Puoi utilizzare un'informazione dettagliata gestita come base per una nuova informazione dettagliata personalizzata.

Per creare una nuova informazione dettagliata personalizzata da un'informazione dettagliata gestita

1. Apri il **AWS Console Security Hub** su <https://console.aws.amazon.com/securityhub/>.
2. Nel riquadro di navigazione, seleziona **Informazioni dettagliate**.
3. Scegliere l'informazione dettagliata gestita da utilizzare.
4. Modifica la configurazione di Insight in base alle tue esigenze.
 - Per modificare l'attributo utilizzato per raggruppare i risultati nell'informazione dettagliata:
 - a. Per rimuovere il raggruppamento esistente, scegli **X** accanto a **Raggruppa** per impostazione.
 - b. Scegli la casella di ricerca.

- c. Selezionare l'attributo da utilizzare per il raggruppamento.
 - d. Seleziona Apply (Applica).
- Per rimuovere un filtro dall'analisi, scegli il cerchiato X accanto al filtro.
- Per aggiungere un filtro all'informazione dettagliata:
 - a. Scegli la casella di ricerca.
 - b. Selezionare l'attributo e il valore da utilizzare come filtro.
 - c. Seleziona Apply (Applica).
5. Al termine degli aggiornamenti, scegliere Create insight (Crea informazione dettagliata).
6. Quando richiesto, inserisci un Nome Insight, quindi scegli Crea informazioni.

Eliminazione di un'analisi personalizzata (console)

Quando un'informazione dettagliata personalizzata non è più richiesta, puoi eliminarla. Non puoi eliminare le informazioni dettagliate gestite.

Per eliminare un'informazione dettagliata personalizzata

1. Apri il **AWS Console Security Hub** su <https://console.aws.amazon.com/securityhub/>.
2. Nel riquadro di navigazione, seleziona **Informazioni dettagliate**.
3. Individuare l'informazione dettagliata personalizzata da eliminare.
4. Per ulteriori informazioni, scegli l'icona **Altre opzioni** (i tre punti nell'angolo in alto a destra della scheda).
5. Scegliere **Elimina**.

Eliminazione di un'analisi personalizzata (programmatica)

Per eliminare un'analisi personalizzata, scegli il tuo metodo preferito e segui le istruzioni.

Security Hub API

1. Esegui il [DeleteInsight](#) operazione.
2. Per identificare le informazioni personalizzate da eliminare, fornisci l'ARN dell'insight. Per ottenere l'ARN di un'analisi personalizzata, esegui [GetInsights](#) operazione.

AWS CLI

1. Nella riga di comando, esegui `delete-insight` comando.
2. Per identificare le informazioni personalizzate, fornisci l'ARN dell'analisi. Per ottenere l'ARN di un'analisi personalizzata, esegui `get-insights` comando.

```
aws securityhub delete-insight --insight-arn <insight ARN>
```

Esempio

```
aws securityhub delete-insight --insight-arn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

PowerShell

1. Usa il `Remove-SHUBInsightcmdlet`.
2. Per identificare le informazioni personalizzate, fornisci l'ARN dell'analisi. Per ottenere l'ARN di un'analisi personalizzata, usa `Get-SHUBInsightcmdlet`.

Esempio

```
-InsightArn "arn:aws:securityhub:us-west-1:123456789012:insight/123456789012/custom/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```

Automazioni

Le automazioni di Security Hub possono aiutarti a modificare e correggere rapidamente i risultati in base alle tue specifiche.

Security Hub attualmente supporta due tipi di automazioni:

- **Regole di automazione:** aggiorna e sopprime automaticamente i risultati quasi in tempo reale in base a criteri definiti dall'utente.
- **Risposta e correzione automatizzate:** crea EventBridge regole personalizzate che definiscono azioni automatiche da intraprendere in base a risultati e approfondimenti specifici.

Le regole di automazione si applicano prima EventBridge delle regole. Cioè, le regole di automazione vengono attivate e aggiornano un risultato prima che venga inviato a EventBridge. EventBridge le regole si applicano quindi al risultato aggiornato.

Quando configuri le automazioni per i controlli di sicurezza, consigliamo di filtrare in base all'ID del controllo anziché al titolo o alla descrizione. Mentre Security Hub aggiorna occasionalmente i titoli e le descrizioni dei controlli, gli ID di controllo rimangono invariati.

Argomenti

- [Regole di automazione](#)
- [Risposta e correzione automatizzate](#)

Regole di automazione

Le regole di automazione possono essere utilizzate per aggiornare automaticamente i risultati in Security Hub. Man mano che i risultati vengono acquisiti, Security Hub può applicare una serie di azioni relative alle regole, come sopprimere i risultati, modificarne la gravità e aggiungere note ai risultati. Tali azioni delle regole hanno effetto quando i risultati soddisfano i criteri specificati, ad esempio a quale risorsa o ID account è associato il risultato o al suo titolo.

Alcuni esempi di casi d'uso per le regole di automazione includono:

- Elevare il livello di severità di un risultato a CRITICAL un valore che l'ID della risorsa si riferisce a una risorsa fondamentale per l'azienda.

- Elevare la gravità di un risultato HIGH da CRITICAL se il risultato influisce sulle risorse di specifici account di produzione.
- Assegnazione di risultati specifici che hanno la stessa gravità dello stato del SUPPRESSED flusso INFORMATIONAL di lavoro.

Le regole di automazione possono essere utilizzate per aggiornare determinati campi di ricerca nel AWS Security Finding Format (ASFF). Le regole si applicano sia ai nuovi risultati che ai risultati aggiornati.

Puoi creare una regola personalizzata da zero o utilizzare un modello di regola fornito da Security Hub. Se si utilizza un modello di regola, è possibile modificarlo in base alle esigenze del caso d'uso.

Come funzionano le regole di automazione

L'amministratore del Security Hub può creare una regola di automazione definendo i criteri delle regole. Quando un risultato corrisponde ai criteri definiti, Security Hub applica l'azione della regola ad esso. Per ulteriori informazioni sui criteri e le azioni disponibili, vedere [Criteri e azioni delle regole disponibili](#).

Solo l'account amministratore di Security Hub può creare, eliminare, modificare e visualizzare le regole di automazione. Una regola creata da un amministratore si applica ai risultati nell'account amministratore e in tutti gli account dei membri. Fornendo gli ID degli account dei membri come criteri di regola, gli amministratori di Security Hub possono anche utilizzare le regole di automazione per aggiornare i risultati o intervenire sui risultati in account membri specifici.

Important

Una regola di automazione si applica solo nel luogo Regione AWS in cui è stata creata. Per applicare una regola in più regioni, l'amministratore delegato deve creare la regola in ciascuna regione. Questa operazione può essere eseguita tramite la console Security Hub, l'API Security Hub o [AWS CloudFormation](#). È inoltre possibile utilizzare uno [script di distribuzione multiregionale](#).

Per una cronologia di come le regole di automazione hanno modificato i risultati, consulta [Revisione della cronologia dei risultati](#).

Le regole di automazione si applicano ai risultati nuovi e aggiornati generati o acquisiti da Security Hub dopo la creazione della regola. Gli aggiornamenti di Security Hub controllano i risultati ogni 12-24

ore o quando la risorsa associata cambia stato. Per ulteriori informazioni, consulta [Pianificazione dell'esecuzione dei controlli di sicurezza](#).

Security Hub attualmente supporta un massimo di 100 regole di automazione per un account amministratore.

Ordine delle regole

Quando si creano regole di automazione, si assegna a ciascuna regola un ordine. Ciò determina l'ordine in cui Security Hub applica le regole di automazione e diventa importante quando più regole si riferiscono allo stesso campo di ricerca o ricerca.

Quando più azioni delle regole si riferiscono allo stesso campo di ricerca o di ricerca, la regola con il valore numerico più alto per l'ordine delle regole si applica per ultima e ha l'effetto finale.

Quando si crea una regola nella console di Security Hub, Security Hub assegna automaticamente l'ordine delle regole in base all'ordine di creazione delle regole. La regola creata più di recente ha il valore numerico più basso per l'ordine delle regole e pertanto viene applicata per prima. Security Hub applica le regole successive in ordine crescente.

Quando si crea una regola tramite l'API Security Hub o AWS CLI, Security Hub applica per `RuleOrder` prima la regola con il valore numerico più basso. Quindi applica le regole successive in ordine crescente. Se più risultati sono uguali `RuleOrder`, Security Hub applica prima una regola con un valore precedente per il `UpdatedAt` campo (ovvero, la regola che è stata modificata più di recente si applica per ultima).

È possibile modificare l'ordine delle regole in qualsiasi momento.

Esempio di ordine delle regole:

Regola A (l'ordine delle regole è **1**):

- Criteri della regola A
 - `ProductName = Security Hub`
 - `Resources.Type` è S3 Bucket
 - `Compliance.Status = FAILED`
 - `RecordState` è NEW
 - `Workflow.Status = ACTIVE`
- Azioni della regola A

- Aggiorna Confidence a 95
- Aggiorna Severity a CRITICAL

Regola B (l'ordine delle regole è 2):

- Criteri della regola B
 - AwsAccountId = 123456789012
- Azioni della regola B
 - Aggiorna Severity a INFORMATIONAL

Le azioni della Regola A si applicano innanzitutto ai risultati del Security Hub che soddisfano i criteri della Regola A. Successivamente, le azioni della Regola B si applicano ai risultati del Security Hub con l'ID account specificato. In questo esempio, poiché la regola B si applica per ultima, il valore finale dei Severity risultati derivanti dall'ID account specificato è INFORMATIONAL. In base all'azione della Regola A, il valore finale dei Confidence risultati corrispondenti è 95.

Criteri e azioni delle regole disponibili

I seguenti campi ASFF sono attualmente supportati come criteri per le regole di automazione.

Campo ASFF	Filtri	Tipo di campo
AwsAccountId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
AwsAccountName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
CompanyName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa

Campo ASFF	Filtri	Tipo di campo
ComplianceAssociatedStandardsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ComplianceSecurityControlId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ComplianceStatus	Is, Is Not	Seleziona: [FAILED,, NOT_AVAILABLE PASSED,WARNING]
Confidence	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Numero
CreatedAt	Start, End, DateRange	Data (formattata come 2022-12-01T 21:47:39.269 Z)
Criticality	Eq (equal-to), Gte (greater-than-equal), Lte (less-than-equal)	Numero
Description	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
FirstObservedAt	Start, End, DateRange	Data (formattata come 2022-12-01T 21:47:39.269 Z)

Campo ASFF	Filtri	Tipo di campo
GeneratorId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
Id	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
LastObservedAt	Start, End, DateRange	Data (formattata come 2022-12-01T 21:47:39.269 Z)
NoteText	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
NoteUpdatedAt	Start, End, DateRange	Data (formattata come 2022-12-01T 21:47:39.269 Z)
NoteUpdatedBy	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ProductName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa

Campo ASFF	Filtri	Tipo di campo
RecordState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
RelatedFindingsId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
RelatedFindingsProductArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ResourceApplicationArn	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ResourceApplicationName	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ResourceDetailsOther	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Eseguire la mappatura
ResourceId	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa

Campo ASFF	Filtri	Tipo di campo
ResourcePartition	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ResourceRegion	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
ResourceTags	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Eseguire la mappatura
ResourceType	Is, Is Not	Seleziona (vedi Risorse supportate da ASFF)
SeverityLabel	Is, Is Not	Seleziona: [CRITICAL,HIGH, MEDIUMLOW,INFORMATIONAL]
SourceUrl	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
Title	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
Type	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa

Campo ASFF	Filtri	Tipo di campo
UpdatedAt	Start, End, DateRange	Data (formattata come 2022-12-01T 21:47:39.269 Z)
UserDefinedFields	CONTAINS, EQUALS, NOT_CONTAINS, NOT_EQUALS	Eseguire la mappatura
VerificationState	CONTAINS, EQUALS, PREFIX, NOT_CONTAINS, NOT_EQUALS, PREFIX_NOT_EQUALS	Stringa
WorkflowStatus	Is, Is Not	Seleziona NEWRESOLVED: [NOTIFIED,,] SUPPRESSED

I seguenti campi ASFF sono attualmente supportati come azioni per le regole di automazione:

- Confidence
- Criticality
- Note
- RelatedFindings
- Severity
- Types
- UserDefinedFields
- VerificationState
- Workflow

[Per ulteriori informazioni su campi ASFF specifici, consulta la sintassi del AWS Security Finding Format \(ASFF\) e gli esempi ASFF.](#)

Tip

Se desideri che Security Hub smetta di generare risultati per un controllo specifico, ti consigliamo di disabilitare il controllo anziché utilizzare una regola di automazione. Quando disabiliti un controllo, Security Hub interrompe l'esecuzione dei controlli di sicurezza e la generazione dei relativi risultati, in modo da non incorrere in costi per tale controllo. Ti consigliamo di utilizzare le regole di automazione per modificare i valori di campi ASFF specifici per i risultati che soddisfano i criteri definiti. Per ulteriori informazioni sulla disabilitazione dei controlli, consulta [Abilitazione e disabilitazione dei controlli in tutti gli standard](#)

Creazione di regole di automazione

È possibile creare una regola personalizzata da zero o utilizzare un modello di regola Security Hub precompilato.

È possibile creare solo una regola di automazione alla volta. Per creare più regole di automazione, segui le procedure della console più volte oppure chiama l'API o il comando più volte con i parametri desiderati.

È necessario creare una regola di automazione in ogni regione e account in cui si desidera che la regola si applichi ai risultati.

Quando si crea una regola di automazione nella console di Security Hub, Security Hub mostra un'anteprima dei risultati a cui si applica la regola. L'anteprima al momento non è supportata se i criteri della regola includono un filtro CONTAINS o NOT_CONTAINS. Puoi scegliere questi filtri per i tipi di campi di tipo mappa e stringa.

Important

AWSconsiglia di non includere informazioni di identificazione personale, riservate o sensibili nel nome della regola, nella descrizione o in altri campi.

Creazione di una regola da un modello (solo console)

Attualmente, solo la console Security Hub supporta i modelli di regole. Questi modelli riflettono casi d'uso comuni per le regole di automazione e possono aiutarti a iniziare a utilizzare questa

funzionalità. Completa i seguenti passaggi per creare una regola di automazione da un modello nella console.

Console

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.
Accedi all'account amministratore di Security Hub.
2. Nel riquadro di navigazione, scegli Automazioni.
3. Scegli Crea regola. Per Tipo di regola, scegli Crea una regola dal modello.
4. Seleziona un modello di regola dal menu a discesa.
5. (Facoltativo) Se necessario per il tuo caso d'uso, modifica le sezioni Regola, Criteri e Azione automatizzata. È necessario specificare almeno un criterio di regola e un'azione della regola.

Se i criteri selezionati sono supportati, la console mostra un'anteprima dei risultati che corrispondono ai criteri specificati.

6. Per lo stato della regola, scegli se desideri che la regola sia abilitata o disabilitata dopo la sua creazione.
7. (Facoltativo) Espandi la sezione Impostazioni aggiuntive. Seleziona Ignora le regole successive per i risultati che corrispondono a questi criteri se desideri che questa regola sia l'ultima regola applicata ai risultati che soddisfano i criteri della regola.
8. (Facoltativo) Per i tag, aggiungi i tag come coppie chiave-valore per aiutarti a identificare facilmente la regola.
9. Scegli Crea regola.

Creazione di una regola personalizzata

Scegli il tuo metodo preferito e completa i passaggi seguenti per creare una regola di automazione personalizzata.

Console

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.
Accedi all'account amministratore di Security Hub.
2. Nel riquadro di navigazione, scegli Automazioni.
3. Scegli Crea regola. Per Tipo di regola, scegli Crea regola personalizzata.

4. Nella sezione Regola, fornisci un nome e una descrizione univoci per la regola.
5. Per Criteri, utilizza i menu a discesa Chiave, Operatore e Valore per specificare i criteri della regola. È necessario specificare almeno un criterio di regola.

Se supportato per i criteri selezionati, la console mostra un'anteprima dei risultati che corrispondono ai criteri specificati.

6. Per l'azione automatizzata, utilizza i menu a discesa per specificare quali campi di ricerca aggiornare quando i risultati soddisfano i criteri delle regole. È necessario specificare almeno un'azione relativa alla regola.
7. Per lo stato della regola, scegli se desideri che la regola sia abilitata o disabilitata dopo la creazione.
8. (Facoltativo) Espandi la sezione Impostazioni aggiuntive. Seleziona Ignora le regole successive per i risultati che corrispondono a questi criteri se desideri che questa regola sia l'ultima regola applicata ai risultati che soddisfano i criteri della regola.
9. (Facoltativo) Per i tag, aggiungi i tag come coppie chiave-valore per aiutarti a identificare facilmente la regola.
10. Scegli Crea regola.

API

1. Esegui [CreateAutomationRule](#) dall'account amministratore di Security Hub. Questa API crea una regola con un Amazon Resource Name (ARN) specifico.
2. Fornisci un nome e una descrizione per la regola.
3. Imposta il `IsTerminal` parametro su `true` se desideri che questa regola sia l'ultima regola applicata ai risultati che soddisfano i criteri della regola.
4. Per il `RuleOrder` parametro, specificate l'ordine della regola. Security Hub applica prima le regole con un valore numerico inferiore per questo parametro.
5. Per il `RuleStatus` parametro, specifica se desideri che Security Hub venga abilitato e inizia ad applicare la regola ai risultati dopo la creazione. Se non viene specificato alcun valore, il valore predefinito è `ENABLED`. Il valore di `DISABLED` indica che la regola viene messa in pausa dopo la creazione.
6. Per il `Criteria` parametro, fornisci i criteri che desideri che Security Hub utilizzi per filtrare i risultati. L'azione della regola si applicherà ai risultati che corrispondono ai criteri. Per un elenco dei criteri supportati, vedere [Criteri e azioni delle regole disponibili](#).

7. Per il `Actions` parametro, fornisci le azioni che desideri che Security Hub intraprenda quando c'è una corrispondenza tra un risultato e i criteri definiti. Per un elenco delle azioni supportate, consulta [Criteri e azioni delle regole disponibili](#).

Esempio di richiesta API:

```
{
  "Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
      "Workflow": {
        "Status": "SUPPRESSED"
      },
      "Note": {
        "Text": "Known issue that is not a risk.",
        "UpdatedBy": "sechub-automation"
      }
    }
  }],
  "Criteria": {
    "ProductName": [{
      "Value": "Security Hub",
      "Comparison": "EQUALS"
    }],
    "ComplianceStatus": [{
      "Value": "FAILED",
      "Comparison": "EQUALS"
    }],
    "RecordState": [{
      "Value": "ACTIVE",
      "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }],
    "GeneratorId": [{
      "Value": "aws-foundational-security-best-practices/v/1.0.0/IAM.1",
      "Comparison": "EQUALS"
    }]
  },
  "Description": "Sample rule description",
```



```
"IsTerminal": false,
"RuleName": "sample-rule-name",
"RuleOrder": 1,
"RuleStatus": "ENABLED",
}
```

AWS CLI

1. Esegui il [create-automation-rule](#) comando dall'account amministratore di Security Hub. Questo comando crea una regola con un Amazon Resource Name (ARN) specifico.
2. Fornisci un nome e una descrizione per la regola.
3. Includi il `is-terminal` parametro se desideri che questa regola sia l'ultima regola applicata ai risultati che soddisfano i criteri della regola. Altrimenti, includi il `no-is-terminal` parametro.
4. Per il `rule-order` parametro, specificate l'ordine della regola. Security Hub applica prima le regole con un valore numerico inferiore per questo parametro.
5. Per il `rule-status` parametro, specifica se desideri che Security Hub venga abilitato e inizia ad applicare la regola ai risultati dopo la creazione. Se non viene specificato alcun valore, il valore predefinito è `ENABLED`. Il valore di `DISABLED` indica che la regola viene messa in pausa dopo la creazione.
6. Per il `criteria` parametro, fornisci i criteri che desideri che Security Hub utilizzi per filtrare i risultati. L'azione della regola si applicherà ai risultati che corrispondono ai criteri. Per un elenco dei criteri supportati, vedere [Criteri e azioni delle regole disponibili](#).
7. Per il `actions` parametro, fornisci le azioni che desideri che Security Hub intraprenda quando c'è una corrispondenza tra un risultato e i criteri definiti. Per un elenco delle azioni supportate, consulta [Criteri e azioni delle regole disponibili](#).

Comando di esempio:

```
aws securityhub create-automation-rule \  
--actions '[{  
  "Type": "FINDING_FIELDS_UPDATE",  
  "FindingFieldsUpdate": {  
    "Severity": {  
      "Label": "HIGH"  
    },  
    "Note": {  
      "Text": "Known issue that is a risk. Updated by automation rules",
```

```
"UpdatedBy": "sechub-automation"
}
}
]]' \
--criteria '{
  "SeverityLabel": [{
    "Value": "INFORMATIONAL",
    "Comparison": "EQUALS"
  }]
}' \
--description "A sample rule" \
--no-is-terminal \
--rule-name "sample rule" \
--rule-order 1 \
--rule-status "ENABLED" \
--region us-east-1
```

Visualizzazione delle regole di automazione

Scegli il tuo metodo preferito e segui i passaggi per visualizzare le regole di automazione e i dettagli di ciascuna regola.

Console

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.

Accedi all'account amministratore di Security Hub.

2. Nel riquadro di navigazione, scegli Automazioni.
3. Scegli il nome di una regola. In alternativa, seleziona una regola.
4. Scegli Azioni e Visualizza.

API

1. Per visualizzare le regole di automazione per il tuo account, esegui [ListAutomationRules](#) dall'account amministratore di Security Hub. Questa API restituisce gli ARN delle regole e altri metadati relativi alle regole. Non sono richiesti parametri di input per questa API, ma puoi opzionalmente fornire un limite `MaxResults` al numero di risultati e `NextToken` come parametro di paginazione. Il valore iniziale di `NextToken` dovrebbe essere `NULL`.

Esempio di richiesta API:

```
{
  "MaxResults": 50,
  "NextToken": "cVpdnSampleTokenYcXgTockBW44c"
}
```

2. Per ulteriori dettagli sulla regola, inclusi i criteri e le azioni per una regola, esegui [BatchGetAutomationRules](#) dall'account amministratore di Security Hub.

Esempio di richiesta API:

```
{
  "AutomationRulesArns": [
    "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
    "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEEaaaaa"
  ]
}
```

AWS CLI

1. Per visualizzare le regole di automazione per il tuo account, esegui il [list-automation-rules](#) comando dall'account amministratore di Security Hub. Questo comando restituisce gli ARN delle regole e altri metadati per le regole. Non sono richiesti parametri di input per questo comando, ma è possibile facoltativamente fornire un parametro di impaginazione `max-results` per limitare il numero di risultati. `next-token`

Comando di esempio:

```
aws securityhub list-automation-rules \
--max-results 5 \
--next-token cVpdnSampleTokenYcXgTockBW44c \
--region us-east-1
```

2. Per ulteriori dettagli sulla regola, inclusi i criteri e le azioni per una regola, esegui il [batch-get-automation-rules](#) comando dall'account amministratore del Security Hub.

Comando di esempio:

```
aws securityhub batch-get-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-
east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
"arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-
cdef-EXAMPLE22222"]' \
--region us-east-1
```

Modifica delle regole di automazione

Quando si modifica una regola di automazione, le modifiche si applicano ai risultati nuovi e aggiornati che Security Hub genera o inserisce dopo la modifica della regola.

Scegli il tuo metodo preferito e segui i passaggi per modificare il contenuto di una regola di automazione. Puoi modificare una o più regole con una sola richiesta. Per istruzioni sulla modifica dell'ordine delle regole, vedere [Modifica dell'ordine delle regole](#).

Console

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.

Accedi all'account amministratore di Security Hub.

2. Nel riquadro di navigazione, scegli Automazioni.
3. Seleziona la regola che desideri modificare. Scegli Azione e Modifica.
4. Modifica la regola come desideri e scegli Salva modifiche.

API

1. Esegui [BatchUpdateAutomationRules](#) dall'account amministratore di Security Hub.
2. Per il `RuleArn` parametro, fornite l'ARN delle regole che desiderate modificare.
3. Fornite i nuovi valori per i parametri che desiderate modificare. È possibile modificare qualsiasi parametro tranne `RuleArn`.

Esempio di richiesta API:

```
{
  "UpdateAutomationRulesRequestItems": [
    {
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
      "RuleOrder": 15,
      "RuleStatus": "Enabled"
    },
    {
      "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
      "RuleStatus": "Disabled"
    }
  ]
}
```

AWS CLI

1. Esegui il [batch-update-automation-rules](#) comando dall'account amministratore di Security Hub.
2. Per il RuleArn parametro, fornite l'ARN delle regole che desiderate modificare.
3. Fornite i nuovi valori per i parametri che desiderate modificare. È possibile modificare qualsiasi parametro tranne RuleArn.

Comando di esempio:

```
aws securityhub batch-update-automation-rules \
--update-automation-rules-request-items '[
  {
    "Actions": [{
      "Type": "FINDING_FIELDS_UPDATE",
      "FindingFieldsUpdate": {
        "Note": {
          "Text": "Known issue that is a risk",
          "UpdatedBy": "sechub-automation"
        },
        "Workflow": {
          "Status": "NEW"
        }
      }
    }
  ]
```

```
    }
  ]],
  "Criteria": {
    "SeverityLabel": [{
      "Value": "LOW",
      "Comparison": "EQUALS"
    }]
  },
  "RuleArn": "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "RuleOrder": 14,
  "RuleStatus": "DISABLED",
}
]' \
--region us-east-1
```

Modifica dell'ordine delle regole

In alcuni casi, potresti voler mantenere invariati i criteri e le azioni della regola, ma modificare l'ordine in cui Security Hub applica una regola di automazione. Scegli il tuo metodo preferito e segui i passaggi per modificare l'ordine delle regole.

Console

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.

Accedi all'account amministratore di Security Hub.

2. Nel riquadro di navigazione, scegli Automazioni.
3. Seleziona la regola di cui desideri modificare l'ordine. Scegli Modifica priorità.
4. Scegli Sposta su per aumentare la priorità della regola di un'unità. Scegli Sposta giù per ridurre la priorità della regola di un'unità. Scegli Sposta in alto per assegnare alla regola un ordine pari a 1 (in questo modo la regola ha la precedenza sulle altre regole esistenti).

Note

Quando si crea una regola nella console di Security Hub, Security Hub assegna automaticamente l'ordine delle regole in base all'ordine di creazione delle regole. La

regola creata più di recente ha il valore numerico più basso per l'ordine delle regole e pertanto viene applicata per prima.

API

1. Esegui [BatchUpdateAutomationRules](#) dall'account amministratore di Security Hub.
2. Per il `RuleArn` parametro, fornite l'ARN delle regole di cui desiderate modificare l'ordine.
3. Modifica il valore del `RuleOrder` campo.

Note

Se più regole sono uguali `RuleOrder`, Security Hub applica prima una regola con un valore precedente per il `UpdatedAt` campo (ovvero, la regola che è stata modificata più di recente si applica per ultima).

AWS CLI

1. Esegui il [batch-update-automation-rules](#) comando dall'account amministratore di Security Hub.
2. Per il `RuleArn` parametro, fornite l'ARN delle regole di cui desiderate modificare l'ordine.
3. Modifica il valore del `RuleOrder` campo.

Note

Se più regole sono uguali `RuleOrder`, Security Hub applica prima una regola con un valore precedente per il `UpdatedAt` campo (ovvero, la regola che è stata modificata più di recente si applica per ultima).

Eliminazione delle regole di automazione

Quando elimini una regola di automazione, Security Hub la rimuove dal tuo account e non applica più la regola ai risultati.

Scegli il tuo metodo preferito e segui i passaggi per eliminare una regola di automazione. Puoi eliminare una o più regole in un'unica richiesta.

Tip

In alternativa all'eliminazione, puoi disabilitare una regola. Ciò mantiene la regola per usi futuri, ma Security Hub non applicherà la regola a nessun risultato corrispondente finché non lo abiliti.

Console

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.
Accedi all'account amministratore di Security Hub.
2. Nel riquadro di navigazione, scegli Automazioni.
3. Seleziona le regole che desideri eliminare. Scegliete Azione ed Elimina (per mantenere una regola, ma disattivarla temporaneamente, scegliete Disabilita).
4. Conferma la scelta e seleziona Delete (Elimina).

API

1. Esegui [BatchDeleteAutomationRules](#) dall'account amministratore di Security Hub.
2. Per il `AutomationRulesArns` parametro, fornisci l'ARN delle regole che desideri eliminare (per mantenere una regola, ma disabilitarla temporaneamente, inserisci `DISABLED` il `RuleStatus` parametro).

Esempio di richiesta API:

```
{
  "AutomationRulesArns": [
    "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
    "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE22222",
    "arn:aws:securityhub:us-east-1:123456789012:automation-rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE33333",
  ]
}
```



```

    "arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLEaaaa"
  ]
}

```

AWS CLI

1. Esegui il [batch-delete-automation-rules](#) comando dall'account amministratore di Security Hub.
2. Per il `automation-rules-arns` parametro, fornisci l'ARN delle regole che desideri eliminare (per mantenere una regola, ma disabilitarla temporaneamente, inserisci `DISABLED` il `RuleStatus` parametro).

Comando di esempio:

```

aws securityhub batch-delete-automation-rules \
--automation-rules-arns '["arn:aws:securityhub:us-east-1:123456789012:automation-
rule/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"]' \
--region us-east-1

```

Esempi di regole di automazione

Questa sezione include alcuni esempi di regole di automazione per casi d'uso comuni. Questi esempi corrispondono ai modelli di regole nella console Security Hub.

Elevate la severità a Critica quando una risorsa specifica, come un bucket S3, è a rischio

In questo esempio, i criteri della regola vengono soddisfatti quando il `ResourceId` risultato è un bucket Amazon Simple Storage Service (Amazon S3) specifico. L'azione della regola consiste nel modificare la gravità dei risultati corrispondenti in `CRITICAL`. È possibile modificare questo modello per applicarlo ad altre risorse.

Esempio di richiesta API:

```

{
  "IsTerminal": true,
  "RuleName": "Elevate severity of findings that relate to important resources",

```

```

"RuleOrder": 1,
"RuleStatus": "ENABLED",
"Description": "Elevate finding severity to CRITICAL when specific resource such as
an S3 bucket is at risk",
"Criteria": {
  "ProductName": [{
    "Value": "Security Hub",
    "Comparison": "EQUALS"
  }],
  "ComplianceStatus": [{
    "Value": "FAILED",
    "Comparison": "EQUALS"
  }],
  "RecordState": [{
    "Value": "ACTIVE",
    "Comparison": "EQUALS"
  }],
  "WorkflowStatus": [{
    "Value": "NEW",
    "Comparison": "EQUALS"
  }],
  "ResourceId": [{
    "Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",
    "Comparison": "EQUALS"
  }]
},
"Actions": [{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Severity": {
      "Label": "CRITICAL"
    },
    "Note": {
      "Text": "This is a critical resource. Please review ASAP.",
      "UpdatedBy": "sechub-automation"
    }
  }
}]
}

```

Esempio di comando CLI:

```
aws securityhub create-automation-rule \  
--is-terminal \  
--rule-name "Elevate severity of findings that relate to important resources" \  
--rule-order 1 \  
--rule-status "ENABLED" \  
  
--description "Elevate finding severity to CRITICAL when specific resource such as an  
S3 bucket is at risk" \  
--criteria '{  
"ProductName": [{  
"Value": "Security Hub",  
"Comparison": "EQUALS"  
}],  
"ComplianceStatus": [{  
"Value": "FAILED",  
"Comparison": "EQUALS"  
}],  
"RecordState": [{  
"Value": "ACTIVE",  
"Comparison": "EQUALS"  
}],  
"WorkflowStatus": [{  
"Value": "NEW",  
"Comparison": "EQUALS"  
}],  
"ResourceId": [{  
"Value": "arn:aws:s3:::examplebucket/developers/design_info.doc",  
"Comparison": "EQUALS"  
}]  
' \  
--actions '[{  
"Type": "FINDING_FIELDS_UPDATE",  
"FindingFieldsUpdate": {  
"Severity": {  
"Label": "CRITICAL"  
},  
"Note": {  
"Text": "This is a critical resource. Please review ASAP.",  
"UpdatedBy": "sechub-automation"  
}  
}  
}]' \  
--region us-east-1
```

Elevare la severità dei risultati relativi alle risorse negli account di produzione

In questo esempio, i criteri della regola vengono soddisfatti quando viene generato un risultato di HIGH gravità in conti di produzione specifici. L'azione della regola consiste nel modificare la gravità dei risultati corrispondenti in CRITICAL.

Esempio di richiesta API:

```
{
  "IsTerminal": false,
  "RuleName": "Elevate severity for production accounts",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Elevate finding severity from HIGH to CRITICAL for findings that relate to resources in specific production accounts",
  "Criteria": {
    "ProductName": [{
      "Value": "Security Hub",
      "Comparison": "EQUALS"
    }],
    "ComplianceStatus": [{
      "Value": "FAILED",
      "Comparison": "EQUALS"
    }],
    "RecordState": [{
      "Value": "ACTIVE",
      "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
      "Value": "NEW",
      "Comparison": "EQUALS"
    }],
    "SeverityLabel": [{
      "Value": "HIGH",
      "Comparison": "EQUALS"
    }],
    "AwsAccountId": [
      {
        "Value": "111122223333",
        "Comparison": "EQUALS"
      },
      {
        "Value": "123456789012",
```

```

        "Comparison": "EQUALS"
    }]
},
"Actions": [{
    "Type": "FINDING_FIELDS_UPDATE",
    "FindingFieldsUpdate": {
        "Severity": {
            "Label": "CRITICAL"
        },
        "Note": {
            "Text": "A resource in production accounts is at risk. Please review
ASAP.",
            "UpdatedBy": "sechub-automation"
        }
    }
}]
}

```

Esempio di comando CLI:

```

aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Elevate severity of findings that relate to resources in production
accounts" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Elevate finding severity from HIGH to CRITICAL for findings that relate
to resources in specific production accounts" \
--criteria '{
"ProductName": [{
"Value": "Security Hub",
"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
"Value": "FAILED",
"Comparison": "EQUALS"
}],
"RecordState": [{
"Value": "ACTIVE",
"Comparison": "EQUALS"
}],
"SeverityLabel": [{

```

```

"Value": "HIGH",
"Comparison": "EQUALS"
}],
"AwsAccountId": [
{
"Value": "111122223333",
"Comparison": "EQUALS"
},
{
"Value": "123456789012",
"Comparison": "EQUALS"
}]
}' \
--actions '[{
"Type": "FINDING_FIELDS_UPDATE",
"FindingFieldsUpdate": {
"Severity": {
"Label": "CRITICAL"
},
"Note": {
"Text": "A resource in production accounts is at risk. Please review ASAP.",
"UpdatedBy": "sechub-automation"
}
}
}]' \
--region us-east-1

```

Sopprime i risultati informativi

In questo esempio, i criteri della regola vengono rispettati per i risultati di INFORMATIONAL gravità inviati a Security Hub da Amazon GuardDuty. L'azione della regola consiste nel modificare lo stato del flusso di lavoro dei risultati corrispondenti in. SUPPRESSED

Esempio di richiesta API:

```

{
  "IsTerminal": false,
  "RuleName": "Suppress informational findings",
  "RuleOrder": 1,
  "RuleStatus": "ENABLED",
  "Description": "Suppress GuardDuty findings with INFORMATIONAL severity",
  "Criteria": {
    "ProductName": [{

```

```

        "Value": "GuardDuty",
        "Comparison": "EQUALS"
    ]],
    "RecordState": [{
        "Value": "ACTIVE",
        "Comparison": "EQUALS"
    }],
    "WorkflowStatus": [{
        "Value": "NEW",
        "Comparison": "EQUALS"
    }],
    "SeverityLabel": [{
        "Value": "INFORMATIONAL",
        "Comparison": "EQUALS"
    }
  ]
},
"Actions": [{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Workflow": {
      "Status": "SUPPRESSED"
    },
    "Note": {
      "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL
severity",
      "UpdatedBy": "sechub-automation"
    }
  }
}]
}

```

Esempio di comando CLI:

```

aws securityhub create-automation-rule \
--no-is-terminal \
--rule-name "Suppress informational findings" \
--rule-order 1 \
--rule-status "ENABLED" \
--description "Suppress GuardDuty findings with INFORMATIONAL severity" \
--criteria '{
"ProductName": [{
"Value": "GuardDuty",

```

```

"Comparison": "EQUALS"
}],
"ComplianceStatus": [{
  "Value": "FAILED",
  "Comparison": "EQUALS"
}],
"RecordState": [{
  "Value": "ACTIVE",
  "Comparison": "EQUALS"
}],
"WorkflowStatus": [{
  "Value": "NEW",
  "Comparison": "EQUALS"
}],
"SeverityLabel": [{
  "Value": "INFORMATIONAL",
  "Comparison": "EQUALS"
}]
}' \
--actions '[{
  "Type": "FINDING_FIELDS_UPDATE",
  "FindingFieldsUpdate": {
    "Workflow": {
      "Status": "SUPPRESSED"
    },
    "Note": {
      "Text": "Automatically suppress GuardDuty findings with INFORMATIONAL severity",
      "UpdatedBy": "sechub-automation"
    }
  }
}]' \
--region us-east-1

```

Risposta e correzione automatizzate

Con Amazon EventBridge, puoi automatizzare AWS i tuoi servizi per rispondere automaticamente a eventi di sistema come problemi di disponibilità delle applicazioni o modifiche delle risorse. Gli eventi AWS relativi ai servizi vengono forniti quasi EventBridge in tempo reale e su base garantita. Puoi scrivere semplici regole per indicare a quali eventi sei interessato e quali azioni automatiche intraprendere quando un evento corrisponde a una regola. Le azioni che possono essere attivate automaticamente includono le seguenti:

- Richiamo di una funzione AWS Lambda
- Richiamo del comando run di Amazon EC2
- Inoltro dell'evento a Amazon Kinesis Data Streams
- Attivazione di una macchina a stati AWS Step Functions
- Notifica di un argomento Amazon SNS o di una coda Amazon SQS
- Invio di una ricerca a uno strumento di gestione di ticket, chat, SIEM o risposta agli incidenti di terze parti

Security Hub invia automaticamente tutti i nuovi risultati e tutti gli aggiornamenti dei risultati esistenti EventBridge come EventBridge eventi. È inoltre possibile creare azioni personalizzate che consentono di inviare risultati selezionati e risultati di approfondimenti a EventBridge.

Quindi configuri EventBridge le regole per rispondere a ogni tipo di evento.

Per ulteriori informazioni sull'utilizzo EventBridge, consulta la [Amazon EventBridge User Guide](#).

Note

Come best practice, assicurati che le autorizzazioni concesse ai tuoi utenti per l'accesso EventBridge utilizzino politiche IAM con privilegi minimi che concedono solo le autorizzazioni richieste.

Per ulteriori informazioni, consulta [Gestione delle identità e degli accessi in Amazon EventBridge](#).

In Soluzioni è disponibile anche un set di modelli per la risposta e la correzione automatizzate tra più account. AWS I modelli sfruttano le regole EventBridge degli eventi e le funzioni Lambda. La soluzione viene distribuita utilizzando e. AWS CloudFormation AWS Systems Manager La soluzione può creare azioni di risposta e riparazione completamente automatizzate. Può anche utilizzare le azioni personalizzate di Security Hub per creare azioni di risposta e riparazione attivate dall'utente. Per i dettagli su come configurare e utilizzare la soluzione, consulta la pagina [Automated Security Response on AWS](#) solution.

Argomenti

- [Tipi di integrazione del Security Hub con EventBridge](#)
- [EventBridge formati di eventi per Security Hub](#)

- [Configurazione di una EventBridge regola per l'invio automatico dei risultati](#)
- [Utilizzo di azioni personalizzate per inviare risultati e approfondimenti a EventBridge](#)

Tipi di integrazione del Security Hub con EventBridge

Security Hub utilizza i seguenti tipi di EventBridge eventi per supportare i seguenti tipi di integrazione con EventBridge.

Nella EventBridge dashboard di Security Hub, All Events include tutti questi tipi di eventi.

Tutti i risultati (Security Hub Findings - Imported)

Security Hub invia automaticamente tutti i nuovi risultati e tutti gli aggiornamenti dei risultati esistenti EventBridge come Security Hub Findings - Imported eventi. Ogni Security Hub Findings - Imported evento contiene un singolo risultato.

Ogni [BatchImportFindingsBatchUpdateFindings](#) richiesta fa scattare un Security Hub Findings - Imported evento.

Per gli account amministratore, il feed degli eventi EventBridge include gli eventi relativi ai risultati sia del loro account che dei loro account membro.

In una regione di aggregazione, il feed degli eventi include gli eventi relativi ai risultati della regione di aggregazione e delle regioni collegate. I risultati interregionali sono inclusi nel feed degli eventi quasi in tempo reale. Per informazioni su come configurare l'aggregazione dei risultati, consulta.

[Aggregazione tra regioni](#)

Puoi definire regole EventBridge che indirizzino automaticamente i risultati a un bucket Amazon S3, un flusso di lavoro di riparazione o uno strumento di terze parti. Le regole possono includere filtri che applicano la regola solo se il risultato ha valori di attributo specifici.

Si utilizza questo metodo per inviare automaticamente tutti i risultati, o tutti i risultati con caratteristiche specifiche, a un flusso di lavoro di risposta o correzione.

Consulta [the section called "Configurazione di una regola per l'invio automatico dei risultati"](#).

Risultati per azioni personalizzate (Security Hub Findings - Custom Action)

Security Hub invia anche i risultati associati ad azioni personalizzate agli Security Hub Findings - Custom Action eventi EventBridge come.

Ciò è utile per gli analisti che lavorano con la console Security Hub e desiderano inviare un risultato specifico, o un piccolo insieme di risultati, a un flusso di lavoro di risposta o correzione. È possibile selezionare un'operazione personalizzata per un massimo di 20 risultati alla volta. Ogni risultato viene inviato EventBridge come evento separato EventBridge .

Quando si crea un'azione personalizzata, le si assegna un ID di azione personalizzato. Puoi utilizzare questo ID per creare una EventBridge regola che esegua un'azione specifica dopo aver ricevuto un risultato associato a quell'ID di azione personalizzato.

Consulta [the section called “Configurazione e utilizzo di azioni personalizzate”](#).

Ad esempio, è possibile creare un'azione personalizzata in Security Hub denominata `send_to_ticketing`. Successivamente EventBridge, si crea una regola che viene attivata quando si EventBridge riceve un risultato che include l'ID dell'azione `send_to_ticketing` personalizzato. La regola include la logica per inviare il risultato al sistema di ticket. È quindi possibile selezionare i risultati all'interno di Security Hub e utilizzare l'azione personalizzata in Security Hub per inviare manualmente i risultati al sistema di ticketing.

Per esempi su come inviare i risultati del Security Hub EventBridge per un'ulteriore elaborazione, consulta [Come integrare le azioni AWS Security Hub personalizzate con PagerDuty](#) e [Come abilitare le azioni personalizzate nel AWS Security Hub](#) blog AWS Partner Network (APN).

Risultati di analisi per le operazioni personalizzate (Security Hub Insight Results)

Puoi anche utilizzare azioni personalizzate per inviare serie di risultati di analisi EventBridge come Security Hub Insight Resultseventi. I risultati di Insight sono le risorse che corrispondono a un'intuizione. Tieni presente che quando invii i risultati degli approfondimenti a EventBridge, non invii i risultati a EventBridge. Stai inviando solo gli identificatori delle risorse associati ai risultati degli approfondimenti. È possibile inviare fino a 100 identificatori di risorse alla volta.

Analogamente alle azioni personalizzate per i risultati, devi prima creare l'azione personalizzata in Security Hub e quindi creare una regola in EventBridge.

Consulta [the section called “Configurazione e utilizzo di azioni personalizzate”](#).

Ad esempio, supponiamo di vedere un particolare risultato di interesse approfondito che desideri condividere con un collega. In tal caso, puoi utilizzare un'azione personalizzata per inviare il risultato di tale analisi al collega tramite una chat o un sistema di ticketing.

EventBridge formati di eventi per Security Hub

I tipi di Security Hub Insight Resultsevento Security Hub Findings - ImportedSecurity Findings - Custom Action, e utilizzano i seguenti formati di evento.

Il formato dell'evento è il formato utilizzato quando Security Hub invia un evento a EventBridge.

Security Hub Findings - Imported

Security Hub Findings - Importedeventi inviati da Security Hub per EventBridge utilizzare il seguente formato.

```
{
  "version":"0",
  "id":"CWE-event-id",
  "detail-type":"Security Hub Findings - Imported",
  "source":"aws.securityhub",
  "account":"111122223333",
  "time":"2019-04-11T21:52:17Z",
  "region":"us-west-2",
  "resources":[
    "arn:aws:securityhub:us-west-2::product/aws/macie/arn:aws:macie:us-west-2:111122223333:integtest/trigger/6294d71b927c41cbab915159a8f326a3/alert/f2893b211841"
  ],
  "detail":{
    "findings": [{
      <finding content>
    }]
  }
}
```

<finding content> è il contenuto, in formato JSON, del risultato inviato dall'evento. Ogni evento invia un singolo risultato.

Per un elenco completo degli attributi di ricerca, vedere [AWS Formato ASFF \(Security Finding Format\)](#).

Per informazioni su come configurare EventBridge le regole attivate da questi eventi, vedere [the section called "Configurazione di una regola per l'invio automatico dei risultati"](#).

Security Hub Findings - Custom Action

Security Hub Findings - Custom Action eventi inviati da Security Hub per EventBridge utilizzare il seguente formato. Ogni risultato viene inviato in un evento separato.

```
{
  "version": "0",
  "id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
  "detail-type": "Security Hub Findings - Custom Action",
  "source": "aws.securityhub",
  "account": "111122223333",
  "time": "2019-04-11T18:43:48Z",
  "region": "us-west-1",
  "resources": [
    "arn:aws:securityhub:us-west-1:111122223333:action/custom/custom-action-name"
  ],
  "detail": {
    "actionName": "custom-action-name",
    "actionDescription": "description of the action",
    "findings": [
      {
        <finding content>
      }
    ]
  }
}
```

<finding content> è il contenuto, in formato JSON, del risultato inviato dall'evento. Ogni evento invia un singolo risultato.

Per un elenco completo degli attributi di ricerca, vedere [AWS Formato ASFF \(Security Finding Format\)](#).

Per informazioni su come configurare EventBridge le regole attivate da questi eventi, vedere [the section called "Configurazione e utilizzo di azioni personalizzate"](#).

Security Hub Insight Results

Security Hub Insight Resultseventi inviati da Security Hub per EventBridge utilizzare il seguente formato.

```
{
```

```

"version": "0",
"id": "1a1111a1-b22b-3c33-444d-5555e5ee5555",
"detail-type": "Security Hub Insight Results",
"source": "aws.securityhub",
"account": "111122223333",
"time": "2017-12-22T18:43:48Z",
"region": "us-west-1",
"resources": [
  "arn:aws:securityhub:us-west-1:111122223333::product/aws/macie:us-
west-1:222233334444:test/trigger/1ec9cf700ef6be062b19584e0b7d84ec/alert/f2893b211841"
],
"detail": {
  "actionName": "name of the action",
  "actionDescription": "description of the action",
  "insightArn": "ARN of the insight",
  "insightName": "Name of the insight",
  "resultType": "ResourceAwsIamAccessKeyUserName",
  "number of results": "number of results, max of 100",
  "insightResults": [
    {"result 1": 5},
    {"result 2": 6}
  ]
}
}
}

```

Per informazioni su come creare una EventBridge regola attivata da questi eventi, vedi [the section called “Configurazione e utilizzo di azioni personalizzate”](#).

Configurazione di una EventBridge regola per l'invio automatico dei risultati

È possibile creare una regola EventBridge che definisca un'azione da intraprendere quando viene ricevuto un Security Hub Findings - Imported evento. Security Hub Findings - Imported gli eventi vengono attivati dagli aggiornamenti di entrambi [BatchImportFindings](#) e [BatchUpdateFindings](#).

Ogni regola contiene uno schema di eventi, che identifica gli eventi che attivano la regola. Il modello di evento contiene sempre l'origine dell'evento (`aws.securityhub`) e il tipo di evento (Security Hub Findings - Imported). Il modello di evento può anche specificare filtri per identificare i risultati a cui si applica la regola.

La regola identifica quindi gli obiettivi della regola. Gli obiettivi sono le azioni da intraprendere quando EventBridge riceve un evento Security Hub Findings - Imported e il risultato corrisponde ai filtri.

Le istruzioni fornite qui utilizzano la EventBridge console. Quando si utilizza la console, crea EventBridge automaticamente la politica basata sulle risorse richiesta che consente la scrittura nei EventBridge registri. CloudWatch

Puoi anche utilizzare il funzionamento dell'[PutRule](#) API. EventBridge Tuttavia, se utilizzi l' EventBridge API, devi creare la politica basata sulle risorse. Per i dettagli sulla politica richiesta, consulta [CloudWatch Logs permissions](#) nella Amazon EventBridge User Guide.

Formato del modello di evento

Il formato del pattern di eventi per Security Hub Findings - Imported events è il seguente:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      <attribute filter values>
    }
  }
}
```

- `source` identifica Security Hub come il servizio che genera l'evento.
- `detail-type` identifica il tipo di evento.
- `detail` è facoltativo e fornisce i valori del filtro per il modello di evento. Se il modello di evento non contiene un `detail` campo, tutti i risultati attivano la regola.

È possibile filtrare i risultati in base a qualsiasi attributo di ricerca. Per ogni attributo, fornisci una matrice separata da virgole di uno o più valori.

```
"<attribute name>": [ "<value1>", "<value2>" ]
```

Se si fornisce più di un valore per un attributo, tali valori vengono uniti. OR Un risultato corrisponde al filtro per un singolo attributo se il risultato contiene uno dei valori elencati. Ad esempio, se

si forniscono entrambi `INFORMATIONAL` e `LOW` come valori per `Severity.Label`, il risultato corrisponde se ha un'etichetta di gravità pari `INFORMATIONAL` o uguale a uno dei due `LOW`.

Gli attributi sono uniti da `AND`. Una ricerca corrisponde se corrisponde ai criteri di filtro per tutti gli attributi forniti.

Quando si fornisce un valore di attributo, questo deve riflettere la posizione di tale attributo all'interno della struttura `AWS Security Finding Format (ASFF)`.

Tip

Quando si filtrano i risultati del controllo, si consiglia di utilizzare i [campi `SecurityControlId` o `SecurityControlArn ASFF`](#) come filtri, anziché `Title` o `Description`. Questi ultimi campi possono cambiare occasionalmente, mentre l'ID di controllo e l'ARN sono identificatori statici.

Nell'esempio seguente, il pattern di eventi fornisce valori di filtro per `ProductArn` e `Severity.Label`, quindi, una ricerca corrisponde se è stata generata da Amazon Inspector e ha un'etichetta di gravità pari o `INFORMATIONAL` uguale a `LOW`.

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Imported"
  ],
  "detail": {
    "findings": {
      "ProductArn": ["arn:aws:securityhub:us-east-1::product/aws/inspector"],
      "Severity": {
        "Label": ["INFORMATIONAL", "LOW"]
      }
    }
  }
}
```


Creazione di una regola di evento

È possibile utilizzare un pattern di eventi predefinito o un pattern di eventi personalizzato in EventBridge per creare una regola. Se si seleziona un pattern predefinito, compila EventBridge automaticamente e. `source detail-type` EventBridge fornisce inoltre campi per specificare i valori di filtro per i seguenti attributi di ricerca:

- `AwsAccountId`
- `Compliance.Status`
- `Criticality`
- `ProductArn`
- `RecordState`
- `ResourceId`
- `ResourceType`
- `Severity.Label`
- `Types`
- `Workflow.Status`

Per creare una EventBridge regola

1. Apri la EventBridge console Amazon all'[indirizzo https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/).
2. Utilizzando i seguenti valori, crea una EventBridge regola che monitora la ricerca degli eventi:
 - Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
 - Scegliete come creare lo schema degli eventi.

Per creare lo schema dell'evento con...	Esegui questa operazione...	
Un modello	Nella sezione Schema di eventi, scegliete le seguenti opzioni: <ul style="list-style-type: none"> • Per Origine evento, scegli Servizi AWS. 	

Per creare lo schema dell'evento con...	Esegui questa operazione...	
	<ul style="list-style-type: none">• Per l'AWSassistenza, scegli Security Hub.• Per Tipo di evento, scegliete Security Hub Findings - Importato.• (Facoltativo) Per rendere la regola più specifica, aggiungi i valori del filtro. Ad esempio, per limitare la regola ai risultati con stati di record attivi, per Stato/i di record specifici, scegli Attivo.	

Per creare lo schema dell'evento con...	Esegui questa operazione...	
<p>Un modello di evento personalizzato</p> <p>(Utilizza un modello personalizzato se desideri filtrare i risultati in base ad attributi che non compaiono nella EventBridge console.)</p>	<ul style="list-style-type: none">Nella sezione Schema di eventi, scegli Modelli personalizzati (editor JSON), quindi incolla il seguente modello di evento nell'area di testo:<pre data-bbox="690 583 1062 1377">{ "source": ["aws.secu rityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "<attribut e name> ": ["<value1>", "<value2>"] } } }</pre>Aggiorna il modello di evento per includere l'attributo e i valori degli attributi che desideri utilizzare come filtro. <p>Ad esempio, per applicare la regola ai risultati con uno stato di verifica di TRUE_POSITIVE ,</p>	

Per creare lo schema dell'evento con...	Esegui questa operazione...	
	<p>utilizzate il seguente esempio di pattern:</p> <pre data-bbox="691 380 1062 1131">{ "source": ["aws.secu rityhub"], "detail-type": ["Security Hub Findings - Imported"], "detail": { "findings": { "Verifica tionState": ["TRUE_POSITIVE"] } } }</pre>	

- Per Tipi di destinazione scegli AWS Servizio, mentre per Seleziona una destinazione scegli una destinazione come un argomento Amazon SNS o una funzione AWS Lambda. La destinazione viene attivata quando viene ricevuto un evento che corrisponde al modello di evento definito nella regola.

Per informazioni dettagliate sulla creazione di regole, consulta [la sezione Creazione di EventBridge regole Amazon che reagiscono agli eventi](#) nella Amazon EventBridge User Guide.

Utilizzo di azioni personalizzate per inviare risultati e approfondimenti a EventBridge

Per utilizzare le azioni personalizzate di Security Hub a cui inviare risultati o approfondimenti EventBridge, devi prima creare l'azione personalizzata in Security Hub. Quindi, definisci le regole EventBridge che si applicano alle tue azioni personalizzate.

Puoi creare fino a 50 azioni personalizzate.

Se hai abilitato l'aggregazione tra regioni e gestisci i risultati dalla regione di aggregazione, crea azioni personalizzate nella regione di aggregazione.

La regola in EventBridge utilizza l'ARN dell'azione personalizzata.

Creazione di un'azione personalizzata (console)

Quando si crea un'azione personalizzata, si specificano il nome, la descrizione e un identificatore univoco.

Per creare un'azione personalizzata in Security Hub (console)

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.
2. Nel riquadro di navigazione, scegliere Settings (Impostazioni), quindi Custom actions (Operazioni personalizzate).
3. Scegliere Create custom action (Crea operazione personalizzata).
4. Fornire Name (Nome), Description (Descrizione) e Custom action ID (ID operazione personalizzata) per l'operazione.

Il campo Name (Nome) non deve contenere più di 20 caratteri.

L'ID dell'azione personalizzata deve essere unico per ogni AWS account.

5. Scegliere Create custom action (Crea operazione personalizzata).
6. Prendere nota dell'operazione ARN personalizzata. È necessario utilizzare l'ARN quando si crea una regola da associare a questa operazione in EventBridge.

Creazione di un'azione personalizzata (API Security Hub, AWS CLI)

Per creare un'azione personalizzata, puoi utilizzare una chiamata API o il AWS Command Line Interface.

Per creare un'azione personalizzata (API Security Hub,AWS CLI)

- API Security Hub: utilizza l'[CreateActionTarget](#)operazione. Quando crei un'azione personalizzata, fornisci il nome, la descrizione e l'identificatore dell'azione personalizzato.
- AWS CLI— Nella riga di comando, esegui il [create-action-target](#)comando.

```
create-action-target --name <customActionName> --
description <customActionDescription> --id <customActionIdentifier>
```

Esempio

```
aws securityhub create-action-target --name "Send to remediation" --description
"Action to send the finding for remediation tracking" --id "Remediation"
```

Definizione di una regola in EventBridge

Per elaborare l'azione personalizzata, è necessario creare una regola corrispondente in EventBridge. La definizione della regola include l'ARN dell'azione personalizzata.

Il modello di evento per un evento Security Hub Findings - Custom Action ha il seguente formato:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Findings - Custom Action"
  ],
  "resources": [ "<custom action ARN>" ]
}
```

Il modello di evento per un evento Security Hub Insight Results ha il seguente formato:

```
{
  "source": [
    "aws.securityhub"
  ],
  "detail-type": [
    "Security Hub Insight Results"
  ]
}
```

```
],  
  "resources": [ "<custom action ARN>" ]  
}
```

In entrambi i modelli, *<custom action ARN>* è l'ARN di un'azione personalizzata. È possibile configurare una regola che si applica a più di un'azione personalizzata.

Le istruzioni fornite qui si riferiscono alla EventBridge console. Quando si utilizza la console, crea EventBridge automaticamente la politica basata sulle risorse richiesta che consente la scrittura nei EventBridge registri. CloudWatch

Puoi anche utilizzare il funzionamento dell'[PutRule](#) API. EventBridge Tuttavia, se utilizzi l' EventBridge API, devi creare la politica basata sulle risorse. Per i dettagli sulla politica richiesta, consulta [CloudWatch Logs permissions](#) nella Amazon EventBridge User Guide.

Per definire una regola in EventBridge

1. Apri la EventBridge console Amazon all'[indirizzo https://console.aws.amazon.com/events/](https://console.aws.amazon.com/events/).
2. Nel pannello di navigazione, scegli Regole.
3. Scegli Create rule (Crea regola).
4. Immettere un nome e una descrizione per la regola.
5. Per Select event bus (Seleziona bus di eventi), scegli il bus di eventi che desideri associare a questa regola. Se vuoi che questa regola corrisponda agli eventi provenienti dal tuo account, seleziona Predefinito. Quando un servizio di AWS nell'account emette un evento, passa sempre al bus di eventi predefinito dell'account.
6. Per Rule type (Tipo di regola), scegli Rule with an event pattern (Regola con un modello di eventi).
7. Seleziona Avanti.
8. Per Event source (Origine eventi), seleziona AWS events (Eventi).
9. Per Modello di eventi, scegli Modulo di modello di eventi.
10. Per Origine evento, scegli Servizi AWS.
11. Per l'AWSassistenza, scegli Security Hub.
12. Per Event type (Tipo di evento), procedere in uno dei seguenti modi:
 - Per creare una regola da applicare quando invii i risultati a un'azione personalizzata, scegli Security Hub Findings - Azione personalizzata.

- Per creare una regola da applicare quando invii i risultati di analisi a un'azione personalizzata, scegli Security Hub Insight Results.
13. Scegli ARN per azioni personalizzate specifiche, aggiungi un ARN per azioni personalizzate.

Se la regola si applica a più azioni personalizzate, scegli Aggiungi per aggiungere altri ARN per azioni personalizzate.
 14. Seleziona Avanti.
 15. In Seleziona obiettivi, scegli e configura l'obiettivo da richiamare quando viene rispettata questa regola.
 16. Seleziona Avanti.
 17. (Facoltativo) Inserire uno o più tag per la regola. Per ulteriori informazioni, consulta i [EventBridge tag Amazon](#) nella Amazon EventBridge User Guide.
 18. Seleziona Avanti.
 19. Rivedi i dettagli della regola e scegli Create rule (Crea regola).

Quando esegui un'azione personalizzata sui risultati di scoperte o approfondimenti nel tuo account, gli eventi vengono generati in EventBridge.

Selezione di un'azione personalizzata per i risultati delle scoperte e degli approfondimenti

Dopo aver creato le azioni e le EventBridge regole personalizzate del Security Hub, puoi inviare risultati e approfondimenti EventBridge per un'ulteriore gestione ed elaborazione.

Gli eventi vengono inviati EventBridge solo all'account in cui vengono visualizzati. Se si visualizza un risultato utilizzando un account amministratore, l'evento viene inviato EventBridge all'account amministratore.

AWS Affinché le chiamate API siano efficaci, le implementazioni del codice di destinazione devono trasferire i ruoli negli account dei membri. Ciò significa anche che il ruolo a cui si passa deve essere assegnato a ciascun membro in cui è necessaria un'azione.

Per inviare i risultati a EventBridge

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.
2. Visualizzare un elenco di risultati:

- Da Findings, puoi visualizzare i risultati di tutte le integrazioni e i controlli di prodotto abilitati.
 - Da Standard di sicurezza, puoi accedere a un elenco di risultati generati da un controllo selezionato. Consulta [the section called “Visualizzazione dei dettagli di un controllo”](#).
 - Da Integrazioni, puoi accedere a un elenco di risultati generati da un'integrazione abilitata. Consulta [the section called “Visualizzazione dei risultati di un'integrazione”](#).
 - Da Insights, puoi accedere a un elenco di risultati per ottenere un risultato approfondito. Consulta [the section called “Visualizzazione dei risultati e dei risultati di informazione dettagliata”](#).
3. Seleziona i risultati a cui inviarli EventBridge. È possibile selezionare fino a 20 risultati alla volta.
 4. In Azioni, scegli l'azione personalizzata in linea con la EventBridge regola da applicare.

Security Hub invia un evento Security Hub Findings - Custom Action separato per ogni risultato.

Per inviare i risultati degli approfondimenti a EventBridge

1. Apri la console AWS Security Hub all'indirizzo <https://console.aws.amazon.com/securityhub/>.
2. Nel riquadro di navigazione, seleziona Informazioni dettagliate.
3. Nella pagina Insights, scegli l'analisi che include i risultati a cui inviare EventBridge.
4. Seleziona i risultati degli approfondimenti a cui inviarli EventBridge. Puoi selezionare fino a 20 risultati alla volta.
5. In Azioni, scegli l'azione personalizzata in linea con la EventBridge regola da applicare.

Integrazioni di prodotti in AWS Security Hub

AWS Security Hub può aggregare i dati relativi ai risultati di sicurezza provenienti da diversi AWS servizi e dalle soluzioni di sicurezza AWS Partner Network (APN) supportate. Questa aggregazione offre una visione completa della sicurezza e della conformità in tutto l'ambiente. AWS

È inoltre possibile inviare i risultati generati dai tuoi prodotti di sicurezza personalizzati.

Important

Dalle integrazioni dei prodotti supportati AWS e dei partner, Security Hub riceve e consolida solo i risultati generati dopo aver abilitato Security Hub nel tuo Account AWS. Il servizio non riceve e consolida retroattivamente i risultati di sicurezza generati prima dell'attivazione di Security Hub.

Per informazioni dettagliate su come Security Hub addebita i risultati acquisiti, consulta i prezzi di [Security Hub](#).

Argomenti

- [Gestione delle integrazioni di prodotti](#)
- [Servizio AWS integrazioni con AWS Security Hub](#)
- [Integrazioni di prodotti partner di terze parti disponibili](#)
- [Utilizzo di integrazioni di prodotti personalizzate per inviare i risultati a AWS Security Hub](#)

Gestione delle integrazioni di prodotti

La pagina Integrazioni AWS Management Console fornisce l'accesso a tutte le integrazioni di prodotti disponibili AWS e di terze parti. L'API AWS Security Hub fornisce anche operazioni che consentono di gestire le integrazioni.

Note

Alcune integrazioni non sono disponibili in tutte le regioni. Se un'integrazione non è supportata nella regione corrente, non è elencata nella pagina Integrazioni.

Consulta anche [the section called “Integrazioni supportate in Cina \(Pechino\) e Cina \(Ningxia\)”](#) e [the section called “Integrazioni supportate in AWS GovCloud \(Stati Uniti orientali\) e \(Stati Uniti occidentali\) AWS GovCloud ”](#).

Visualizzazione e filtraggio dell'elenco delle integrazioni (console)

Nella pagina Integrations (Integrazioni) puoi visualizzare e filtrare l'elenco delle integrazioni.

Per visualizzare l'elenco delle integrazioni

1. Aprire la console AWS Security Hub all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione Security Hub, scegli Integrazioni.

Nella pagina Integrations (Integrazioni) le integrazioni con altri servizi AWS sono elencate per prime, seguite dalle integrazioni con prodotti di terze parti.

Per ogni integrazione, la pagina Integrations (Integrazioni) fornisce le seguenti informazioni.

- Il nome della società
- Il nome del prodotto
- La descrizione dell'integrazione
- Le categorie a cui l'integrazione si applica
- Come abilitare l'integrazione
- Lo stato attuale dell'integrazione

Puoi filtrare l'elenco inserendo il testo nei seguenti campi.

- Company name (Nome dell'azienda)
- Product name (Nome del prodotto)
- Integration description (Descrizione dell'integrazione)
- Categories

Visualizzazione delle informazioni sulle integrazioni dei prodotti (API Security Hub, AWS CLI)

Per visualizzare informazioni sulle integrazioni dei prodotti, puoi utilizzare una chiamata API o il AWS Command Line Interface. Puoi visualizzare informazioni su tutte le integrazioni di prodotti o informazioni sulle integrazioni di prodotti che hai abilitato.

Per visualizzare informazioni su tutte le integrazioni di prodotti disponibili (API Security Hub, AWS CLI)

- API Security Hub: utilizza l'[DescribeProducts](#) operazione. Per identificare un'integrazione di prodotto specifica da restituire, utilizza il `ProductArn` parametro per fornire l'ARN di integrazione.
- AWS CLI— Nella riga di comando, eseguire il [describe-products](#) comando. Per identificare un'integrazione di prodotto specifica da restituire, fornisci l'ARN di integrazione.

```
aws securityhub describe-products --product-arn "<integrationARN>"
```

Esempio

```
aws securityhub describe-products --product-arn "arn:aws:securityhub:us-east-1::product/3coresec/3coresec"
```

Per visualizzare le informazioni sulle integrazioni dei prodotti che hai abilitato (Security Hub API, AWS CLI)

- API Security Hub: utilizza l'[ListEnabledProductsForImport](#) operazione.
- AWS CLI— Nella riga di comando, esegui il [list-enabled-products-for-import](#) comando.

```
aws securityhub list-enabled-products-for-import
```

Abilitazione di un'integrazione

Nella pagina Integrations (Integrazioni) ogni integrazione fornisce i passaggi necessari per abilitarla.

Per la maggior parte delle integrazioni con altri AWS servizi, l'unico passaggio richiesto è abilitare l'altro servizio. Le informazioni di integrazione includono un collegamento alla home page del servizio.

Quando si abilita l'altro servizio, viene quindi creata e applicata automaticamente un'autorizzazione a livello di risorsa che consente a Security Hub di ricevere i risultati dal servizio.

Per le integrazioni di prodotti di terze parti, potrebbe essere necessario acquistare l'integrazione da e quindi configurare Marketplace AWS l'integrazione. Le informazioni di integrazione forniscono i collegamenti per eseguire tali attività.

Se è disponibile più di una versione di un prodotto Marketplace AWS, seleziona la versione a cui abbonarti, quindi scegli Continua con l'abbonamento. Ad esempio, alcuni prodotti offrono una versione standard e una AWS GovCloud (US) versione.

Quando abiliti un'integrazione di prodotto, una policy delle risorse viene automaticamente collegata a tale sottoscrizione prodotto. Questa politica delle risorse definisce le autorizzazioni di cui Security Hub ha bisogno per ricevere i risultati da quel prodotto.

Disabilitazione e abilitazione del flusso di risultati di un'integrazione (Console)

Nella pagina Integrazioni, per le integrazioni che inviano risultati, le informazioni sullo stato indicano se al momento stai accettando i risultati.

Per interrompere l'accettazione dei risultati, scegli Stop accepting findings (Interrompi l'accettazione dei risultati).

Per riprendere l'accettazione dei risultati, scegliere Accept findings (Accetta risultati).

Disabilitazione del flusso di risultati da un'integrazione (API Security Hub, AWS CLI)

Per disabilitare il flusso di risultati da un'integrazione, puoi utilizzare una chiamata API o il AWS Command Line Interface.

Per disabilitare il flusso di risultati da un'integrazione (API Security Hub, AWS CLI)

- API Security Hub: utilizza l'[DisableImportFindingsForProduct](#) operazione. Per identificare l'integrazione da disabilitare, è necessario l'ARN dell'abbonamento. Per ottenere gli ARN dell'abbonamento per le integrazioni abilitate, utilizza l'operazione. [ListEnabledProductsForImport](#)
- AWS CLI— Nella riga di comando, esegui il [disable-import-findings-for-product](#) comando.

```
aws securityhub disable-import-findings-for-product --product-subscription-arn <subscription ARN>
```

Esempio

```
aws securityhub disable-import-findings-for-product --product-subscription-arn "arn:aws:securityhub:us-west-1:123456789012:product-subscription/crowdstrike/crowdstrike-falcon"
```

Abilitazione del flusso di risultati da un'integrazione (API Security Hub, AWS CLI)

Per abilitare il flusso dei risultati di un'integrazione, puoi utilizzare una chiamata API o il AWS Command Line Interface.

Per abilitare il flusso di risultati da un'integrazione (API Security Hub, AWS CLI)

- API Security Hub: utilizza l'[EnableImportFindingsForProduct](#) operazione. Per consentire a Security Hub di ricevere i risultati di un'integrazione, è necessario l'ARN del prodotto. Per ottenere gli ARN per le integrazioni disponibili, utilizza l'operazione. [DescribeProducts](#)
- AWS CLI: alla riga di comando, esegui il comando [enable-import-findings-for-product](#).

```
aws securityhub enable-import-findings-for-product --product-arn <integration ARN>
```

Esempio

```
aws securityhub enable-import-findings-for product --product-arn "arn:aws:securityhub:us-east-1:123456789333:product/crowdstrike/crowdstrike-falcon"
```

Visualizzazione dei risultati di un'integrazione

Per le integrazioni per le quali accetti i risultati (Lo stato è Accettazione dei risultati), per visualizzare un elenco di risultati, scegli Vedi risultati.

L'elenco dei risultati mostra i risultati attivi per l'integrazione selezionata che hanno lo stato del flusso di lavoro NEW o NOTIFIED.

Se abiliti l'aggregazione tra regioni, nella regione di aggregazione l'elenco include i risultati della regione di aggregazione e delle regioni collegate in cui è abilitata l'integrazione. Security Hub non abilita automaticamente le integrazioni basate sulla configurazione di aggregazione interregionale.

In altre regioni, l'elenco dei risultati di un'integrazione contiene solo i risultati della regione corrente.

Per informazioni su come configurare l'aggregazione tra regioni, vedere. [Aggregazione tra regioni](#)

Dall'elenco dei risultati puoi eseguire le seguenti operazioni.

- [Modificare filtri e raggruppamento dell'elenco](#)
- [Visualizzare i dettagli per i singoli risultati](#)
- [Aggiornare lo stato del flusso di lavoro dei risultati](#)
- [Inviare i risultati alle operazioni personalizzate](#)

Servizio AWS integrazioni con AWS Security Hub

AWS Security Hub supporta integrazioni con molti altri Servizi AWS.

Note

Alcune integrazioni sono disponibili solo in alcune versioni. Regioni AWS

Se un'integrazione non è supportata in una regione specifica, non è elencata nella pagina Integrazioni della console Security Hub.

Per ulteriori informazioni, consulta [Integrazioni supportate in Cina \(Pechino\) e Cina \(Ningxia\)](#) e [Integrazioni supportate in AWS GovCloud \(Stati Uniti orientali\) e \(Stati Uniti occidentali\) AWS GovCloud](#).

A meno che non sia indicato di seguito, Servizio AWS le integrazioni che inviano i risultati a Security Hub vengono attivate automaticamente dopo l'attivazione di Security Hub. Le integrazioni che ricevono i risultati del Security Hub potrebbero richiedere passaggi aggiuntivi per l'attivazione. Consulta le informazioni su ciascuna integrazione per saperne di più.

Panoramica delle integrazioni dei AWS servizi con Security Hub

Ecco una panoramica dei AWS servizi che inviano risultati a Security Hub o ricevono risultati da Security Hub.

AWS Servizio integrato	Direzione	
AWS Config	Invia i risultati	
AWS Firewall Manager	Invia i risultati	
Amazon GuardDuty	Invia risultati	
AWS Health	Invia i risultati	
AWS Identity and Access Management Access Analyzer	Invia i risultati	
Amazon Inspector	Invia i risultati	
AWS IoT Device Defender	Invia i risultati	
Amazon Macie	Invia i risultati	
AWS Systems Manager Gestione patch	Invia i risultati	
AWS Audit Manager	Riceve i risultati	
AWS Chatbot	Riceve i risultati	
Amazon Detective	Riceve i risultati	
Amazon Security Lake	Riceve i risultati	
AWS Systems Manager Explorer e OpsCenter	Riceve e aggiorna i risultati	
AWS Trusted Advisor	Riceve i risultati	

AWS servizi che inviano i risultati a Security Hub

I seguenti AWS servizi si integrano con Security Hub inviando i risultati a Security Hub. Security Hub trasforma i risultati nel [AWS Security Finding Format](#).

AWS Config (Invia i risultati)

AWS Config è un servizio che consente di valutare, controllare e valutare le configurazioni delle AWS risorse. AWS Config monitora e registra continuamente le configurazioni AWS delle risorse e consente di automatizzare la valutazione delle configurazioni registrate rispetto alle configurazioni desiderate.

Utilizzando l'integrazione con AWS Config, puoi vedere i risultati delle valutazioni delle regole AWS Config gestite e personalizzate come risultati in Security Hub. Questi esiti possono essere visualizzati insieme ad altri esiti di Security Hub, per fornire una panoramica completa della posizione di sicurezza.

AWS Config utilizza Amazon EventBridge per inviare valutazioni delle AWS Config regole a Security Hub. Security Hub trasforma le valutazioni delle regole in risultati che seguono il [AWS Security Finding Format](#). Security Hub arricchisce quindi i risultati con il massimo impegno ottenendo ulteriori informazioni sulle risorse interessate, come l'Amazon Resource Name (ARN) e la data di creazione. I tag delle risorse nelle valutazioni delle AWS Config regole non sono inclusi nei risultati del Security Hub.

Per ulteriori informazioni su questa integrazione, consulta le seguenti sezioni.

Come AWS Config invia i risultati a Security Hub

Tutti i risultati in Security Hub utilizzano il formato JSON standard di ASFF. ASFF include dettagli sull'origine del risultato, sulla risorsa interessata e sullo stato attuale del risultato. AWS Config invia valutazioni di regole gestite e personalizzate a Security Hub tramite EventBridge. Security Hub trasforma le valutazioni delle regole in risultati che seguono l'ASFF e arricchisce i risultati con il massimo impegno.

Tipi di risultati che vengono AWS Config inviati a Security Hub

Una volta attivata l'integrazione, AWS Config invia le valutazioni di tutte le regole AWS Config gestite e le regole personalizzate a Security Hub. Sono escluse solo le valutazioni [basate AWS Config sulle regole collegate ai servizi](#), come quelle utilizzate per eseguire i controlli di sicurezza.

Invio AWS Config dei risultati a Security Hub

Quando l'integrazione è attivata, Security Hub assegnerà automaticamente le autorizzazioni necessarie per ricevere i risultati da AWS Config Security Hub utilizza autorizzazioni di service-to-service livello che forniscono un modo sicuro per attivare questa integrazione e importare i risultati AWS Config tramite Amazon EventBridge.

Latenza per l'invio degli esiti

Quando si AWS Config crea un nuovo risultato, in genere è possibile visualizzarlo in Security Hub entro cinque minuti.

Nuovo tentativo quando Security Hub non è disponibile

AWS Config invia i risultati a Security Hub con la massima diligenza possibile tramite EventBridge. Quando un evento non viene consegnato correttamente a Security Hub, EventBridge riprova la consegna per un massimo di 24 ore o 185 volte, a seconda dell'evento che si verifica per primo.

Aggiornamento dei AWS Config risultati esistenti in Security Hub

Dopo aver AWS Config inviato un risultato a Security Hub, può inviare aggiornamenti dello stesso risultato a Security Hub per riflettere ulteriori osservazioni sull'attività di ricerca. Gli aggiornamenti vengono inviati solo per `ComplianceChangeNotification` gli eventi. Se non si verifica alcuna modifica della conformità, gli aggiornamenti non vengono inviati a Security Hub. Security Hub elimina i risultati 90 giorni dopo l'aggiornamento più recente o 90 giorni dopo la creazione se non si verifica alcun aggiornamento.

Security Hub non archivia i risultati inviati AWS Config anche se elimini la risorsa associata.

Regioni in cui esistono AWS Config i risultati

AWS Config i risultati avvengono su base regionale. AWS Config invia i risultati a Security Hub nella stessa regione o nelle stesse regioni in cui si verificano i risultati.

Visualizzazione dei AWS Config risultati in Security Hub

Per visualizzare i AWS Config risultati, scegli Findings dal riquadro di navigazione di Security Hub. Per filtrare i risultati in modo da visualizzare solo AWS Config i risultati, scegli Nome prodotto nel menu a discesa della barra di ricerca. Immettete Config e scegliete Applica.

Interpretazione dei nomi AWS Config dei risultati in Security Hub

Security Hub trasforma le valutazioni delle AWS Config regole in risultati che seguono il [AWS Formato ASFF \(Security Finding Format\)](#). AWS Config le valutazioni delle regole utilizzano un pattern di eventi diverso rispetto a ASFF. La tabella seguente mappa i campi di valutazione delle AWS Config regole con la loro controparte ASFF così come appaiono in Security Hub.

Tipo di risultato per la valutazione delle regole di Config	Tipo di risultati ASFF	Valore codificato
dettaglio. awsAccountId	AwsAccountId	
dettaglio. newEvaluationResult.resultRecordedTime	CreatedAt	
dettaglio. newEvaluationResult.resultRecordedTime	UpdatedAt	
	ProductArn	<partition><region>«arn ::securityhub:: :product/ aws/config»
	ProductName	«Config»
	CompanyName	"AWS"
	Regione	«eu-central-1"
configRuleArn	GeneratorId, ProductFields	
dettaglio. ConfigRuleARN/ Cerca/Hash	Id	
dettaglio. configRuleName	Titolo, ProductFields	
dettaglio. configRuleName	Descrizione	«Questo risultato è stato creato per una modifica della conformità delle risorse per la regola di configurazione: \${detail. ConfigRuleName} »
Elemento di configurazione «ARN» o ARN calcolato da Security Hub	Risorse [i] .id	

Tipo di risultato per la valutazione delle regole di Config	Tipo di risultati ASFF	Valore codificato
Detail.ResourceType	Risorse [i] .Type	"AwsS3Bucket"
	Risorse [i] .Partizione	"aws"
	Risorse [i] .Region	«eu-central-1"
Elemento di configurazione «configuration»	Risorse [i] .Dettagli	
	SchemaVersion	«2018-10-08"
	Etichetta di severità	Vedi «Interpretazione dell'etichetta di severità» di seguito
	Tipi	["Controlli del software e della configurazione"]
dettaglio. newEvaluationResult. Tipo di conformità	Conformità. Stato	«FAILED», «NOT_AVAILABLE», «PASSED» o «WARNING»
	Flusso di lavoro. Stato	«RISOLTO» se viene generato un AWS Config risultato con un valore Compliance.Status pari a «PASSED» o se Compliance.Status cambia da «FAILED» a «PASSED». Altrimenti, Workflow.Status sarà «NUOVO». È possibile modificare questo valore con l' BatchUpdateFinding operazione API.

Interpretazione dell'etichetta di gravità

Tutti i risultati delle valutazioni delle AWS Config regole hanno un'etichetta di gravità predefinita pari a MEDIUM nell'ASFF. È possibile aggiornare l'etichetta di gravità di un risultato con l'operazione [BatchUpdateFindingsAPI](#).

Risultato tipico di AWS Config

Security Hub trasforma le valutazioni delle AWS Config regole in risultati conformi all'ASFF. Di seguito è riportato un esempio di un risultato tipico dell' AWS Config ASFF.

Note

Se la descrizione è composta da più di 1024 caratteri, verrà troncata a 1024 caratteri e alla fine verrà visualizzato «(troncato)».

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/finding/45g070df80cb50b68fa6a43594kc6fda1e517932",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/config",
  "ProductName": "Config",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks"
  ],
  "CreatedAt": "2022-04-15T05:00:37.181Z",
  "UpdatedAt": "2022-04-19T21:20:15.056Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "s3-bucket-level-public-access-prohibited-config-integration-demo",
  "Description": "This finding is created for a resource compliance change for config rule: s3-bucket-level-public-access-prohibited-config-integration-demo",
  "ProductFields": {
    "aws/securityhub/ProductName": "Config",
```

```
"aws/securityhub/CompanyName": "AWS",
"aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
config/arn:aws:config:eu-central-1:123456789012:config-rule/config-rule-mburzq/
finding/46f070df80cd50b68fa6a43594dc5fda1e517902",
"aws/config/ConfigRuleArn": "arn:aws:config:eu-central-1:123456789012:config-rule/
config-rule-mburzq",
"aws/config/ConfigRuleName": "s3-bucket-level-public-access-prohibited-config-
integration-demo",
"aws/config/ConfigComplianceType": "NON_COMPLIANT"
},
"Resources": [{
  "Type": "AwsS3Bucket",
  "Id": "arn:aws:s3:::config-integration-demo-bucket",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
    "AwsS3Bucket": {
      "OwnerId": "4edbbba300f1caa608fba2aad2c8fcfe30c32ca32777f64451eec4fb2a0f10d8c",
      "CreatedAt": "2022-04-15T04:32:53.000Z"
    }
  }
}],
"Compliance": {
  "Status": "FAILED"
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM"
  }
},
"Types": [
  "Software and Configuration Checks"
]
}
```

Abilitazione e configurazione dell'integrazione

Dopo aver abilitato Security Hub, questa integrazione viene attivata automaticamente. AWS Config inizia immediatamente a inviare i risultati a Security Hub.

Interruzione dell'invio degli esiti a Security Hub

Per interrompere l'invio dei risultati a Security Hub, puoi utilizzare la console Security Hub, l'API Security Hub o AWS CLI.

Vedi [Disabilitazione e abilitazione del flusso di risultati di un'integrazione \(Console\)](#) o [Disabilitazione del flusso di risultati da un'integrazione \(API Security Hub, AWS CLI\)](#).

AWS Firewall Manager (Invia i risultati)

Firewall Manager invia i risultati a Security Hub quando una politica WAF (Web Application Firewall) per le risorse o una regola della lista di controllo degli accessi Web (Web Access Control List) non è conforme. Firewall Manager invia i risultati anche quando AWS Shield Advanced non protegge le risorse o quando viene identificato un attacco.

Dopo aver abilitato Security Hub, questa integrazione viene attivata automaticamente. Firewall Manager inizia immediatamente a inviare i risultati a Security Hub.

Per ulteriori informazioni sull'integrazione, visualizza la pagina Integrazioni nella console Security Hub.

Per ulteriori informazioni su Firewall Manager, consulta la [Guida per AWS WAF gli sviluppatori](#).

Amazon GuardDuty (invia i risultati)

GuardDuty invia tutti i risultati che genera a Security Hub.

I nuovi risultati GuardDuty vengono inviati a Security Hub entro cinque minuti. Gli aggiornamenti ai risultati vengono inviati in base all'impostazione Updated results per Amazon EventBridge nelle GuardDuty impostazioni.

Quando si generano risultati di GuardDuty esempio utilizzando la pagina GuardDuty Impostazioni, Security Hub riceve i risultati del campione e omette il prefisso [Sample] nel tipo di risultato. Ad esempio, il tipo di ricerca del campione GuardDuty [SAMPLE] Recon:IAMUser/ResourcePermissions viene visualizzato come Recon:IAMUser/ResourcePermissions in Security Hub.

Dopo aver abilitato Security Hub, questa integrazione viene attivata automaticamente. GuardDuty inizia immediatamente a inviare i risultati a Security Hub.

Per ulteriori informazioni sull' GuardDuty integrazione, consulta [Integration with AWS Security Hub](#) nella Amazon GuardDuty User Guide.

AWS Health (Invia i risultati)

AWS Health offre una visibilità continua sulle prestazioni delle risorse e sulla disponibilità dei AWS servizi e degli account. È possibile utilizzare AWS Health gli eventi per scoprire in che modo le modifiche ai servizi e alle risorse potrebbero influire sulle applicazioni su cui vengono eseguite AWS.

L'integrazione con AWS Health non utilizza `BatchImportFindings`. AWS Health Utilizza invece la messaggistica service-to-service degli eventi per inviare i risultati a Security Hub.

Per ulteriori informazioni sull'integrazione, consulta le seguenti sezioni.

Come AWS Health invia i risultati a Security Hub

Nella Centrale di sicurezza, i problemi di sicurezza vengono monitorati come esiti. Alcuni risultati derivano da problemi rilevati da altri AWS servizi o da partner terzi. Security Hub dispone inoltre di una serie di regole che utilizza per rilevare problemi di sicurezza e generare risultati.

Security Hub fornisce strumenti per gestire i risultati da tutte queste fonti. È possibile visualizzare e filtrare gli elenchi di risultati e visualizzare i dettagli per un riscontro. Per informazioni, consulta [Gestione e revisione dei dettagli e della cronologia dei risultati](#). È inoltre possibile monitorare lo stato di un'indagine in un esito. Per informazioni, consulta [Intervenire in base ai risultati in AWS Security Hub](#).

Tutti i risultati in Security Hub utilizzano un formato JSON standard chiamato [AWS Formato ASFF \(Security Finding Format\)](#). ASFF include dettagli sull'origine del problema, sulle risorse interessate e sullo stato attuale del risultato.

AWS Health è uno dei AWS servizi che invia i risultati a Security Hub.

Tipi di risultati che vengono AWS Health inviati a Security Hub

Una volta abilitata l'integrazione, AWS Health invia tutti i risultati relativi alla sicurezza generati a Security Hub. I risultati vengono inviati a Security Hub utilizzando il [AWS Formato ASFF \(Security Finding Format\)](#). I risultati relativi alla sicurezza sono definiti come segue:

- Qualsiasi risultato associato a un servizio di sicurezza AWS
- Qualsiasi risultato con le parole `security` o `certificate` nel AWS Health TypeCode **abuse**
- Qualsiasi risultato su dove si trova il AWS Health servizio o `risk abuse`

Invio AWS Health dei risultati a Security Hub

Quando scegli di accettare i risultati da AWS Health, Security Hub assegnerà automaticamente le autorizzazioni necessarie per ricevere i risultati da AWS Health Security Hub utilizza autorizzazioni di service-to-service livello che ti forniscono un modo semplice e sicuro per abilitare questa integrazione e importare i risultati AWS Health da Amazon per tuo EventBridge conto. La scelta di Accept Findings concede a Security Hub l'autorizzazione a utilizzare i risultati da AWS Health.

Latenza per l'invio degli esiti

Quando viene AWS Health creato un nuovo risultato, di solito viene inviato a Security Hub entro cinque minuti.

Nuovo tentativo quando Security Hub non è disponibile

AWS Health invia i risultati a Security Hub con la massima diligenza possibile tramite EventBridge. Quando un evento non viene recapitato correttamente a Security Hub, EventBridge riprova a inviarlo per 24 ore.

Aggiornamento degli esiti esistenti nella Centrale di sicurezza

Dopo aver AWS Health inviato un risultato a Security Hub, può inviare aggiornamenti allo stesso risultato per riflettere ulteriori osservazioni sull'attività di ricerca a Security Hub.

Regioni in cui esistono i risultati

Per gli eventi globali, AWS Health invia i risultati al Security Hub in us-east-1 AWS (partizione), cn-northwest-1 (partizione cinese) e -1 (partizione). gov-us-west GovCloud AWS Health invia eventi specifici della regione a Security Hub nella stessa regione o nelle stesse regioni in cui si verificano gli eventi.

Visualizzazione dei AWS Health risultati in Security Hub

Per visualizzare i AWS Health risultati in Security Hub, scegli Findings dal pannello di navigazione. Per filtrare i risultati in modo da visualizzare solo AWS Health i risultati, scegli Health dal campo Nome prodotto.

Interpretazione dei nomi AWS Health dei risultati in Security Hub

AWS Health invia i risultati a Security Hub utilizzando [AWS Formato ASFF \(Security Finding Format\)](#). AWS Health la ricerca utilizza un pattern di eventi diverso rispetto al formato ASFF di Security Hub. La tabella seguente descrive in dettaglio tutti i campi di AWS Health ricerca con la loro controparte ASFF così come appaiono in Security Hub.

Tipo di reperto sanitario	Tipo di risultati ASFF	Valore codificato
account	AwsAccountId	
Dettaglio. Ora di inizio	CreatedAt	
detail.eventdescription.Ultima descrizione	Descrizione	
dettaglio. eventTypeCode	GeneratorId	
detail.eventArn (incluso l'account) + hash di detail.startTime	Id	
«<region>arn:aws:securityhub:::product/aws/health»	ProductArn	
account o resourceID	Risorse [i] .id	
	Risorse [i] .Tipo	«Altro»
	SchemaVersion	«2018-10-08»
	Etichetta di severità	Vedi «Interpretazione dell'etichetta di severità» di seguito
Dettaglio «AWS Health -». eventTypeCode	Title	
-	Tipi	["Controlli del software e della configurazione"]

Tipo di reperto sanitario	Tipo di risultati ASFF	Valore codificato
event.time	UpdatedAt	
URL dell'evento sulla console Health	SourceUrl	

Interpretazione dell'etichetta di gravità

L'etichetta di gravità nel risultato ASFF viene determinata utilizzando la seguente logica:

- Severità CRITICA se:
 - Il service campo del AWS Health risultato ha il valore Risk
 - Il typeCode campo del AWS Health risultato ha il valore AWS_S3_OPEN_ACCESS_BUCKET_NOTIFICATION
 - Il typeCode campo del AWS Health risultato ha il valore AWS_SHIELD_INTERNET_TRAFFIC_LIMITATIONS_PLACED_IN_RESPONSE_TO_DDOS_ATTACK
 - Il typeCode campo del AWS Health risultato ha il valore AWS_SHIELD_IS_RESPONDING_TO_A_DDOS_ATTACK_AGAINST_YOUR_AWS_RESOURCES

Severità ALTA se:

- Il service campo del AWS Health risultato ha il valore Abuse
- Il typeCode campo del AWS Health risultato contiene il valore SECURITY_NOTIFICATION
- Il typeCode campo del AWS Health risultato contiene il valore ABUSE_DETECTION

Severità MEDIUM se:

- Il service campo del risultato è uno dei seguenti: ACM,,ARTIFACT,AUDITMANAGER,BACKUP,CLOUDENDURE,CLOUDHSM,CLOUDTRAIL,CLOUDWATCH,KMSMACIE,NETWORKFIREWALL,ORGANIZATIONS,RESILIENCEHUB,RESOURCEMANAGER,ROUTE53,SEC o WAF
- Il campo TypeCode del AWS Health risultato contiene il valore CERTIFICATE
- Il campo TypeCode del AWS Health risultato contiene il valore END_OF_SUPPORT

Risultato tipico di AWS Health

AWS Health invia i risultati a Security Hub utilizzando [AWS Formato ASFF \(Security Finding Format\)](#). Di seguito è riportato un esempio di un risultato tipico di AWS Health.

Note

Se la descrizione supera i 1024 caratteri, verrà troncata a 1024 caratteri e alla fine verrà riportata la dicitura (troncata).

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:health:us-east-1:123456789012:event/SES/
AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-
b533-78e29f49de96/101F7FBAEFC663977DA09CFF56A29236602834D2D361E6A8CA5140BFB3A69B30",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/health",
  "GeneratorId": "AWS_SES_CMF_PENDING_TO_SUCCESS",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks"
  ],
  "CreatedAt": "2022-01-07T16:34:04.000Z",
  "UpdatedAt": "2022-01-07T19:17:43.000Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "AWS Health - AWS_SES_CMF_PENDING_TO_SUCCESS",
  "Description": "Congratulations! Amazon SES has successfully detected the
MX record required to use 4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com as a custom MAIL FROM domain for verified identity cmf.pinpoint.sysmon-
iad.adzel.com in AWS Region US East (N. Virginia).\n\nYou can now use this MAIL
FROM domain with cmf.pinpoint.sysmon-iad.adzel.com and any other verified identity
that is configured to use it. For information about how to configure a verified
identity to use a custom MAIL FROM domain, see http://docs.aws.amazon.com/ses/latest/
DeveloperGuide/mail-from-set.html .\n\nPlease note that this email only applies to
AWS Region US East (N. Virginia).",
  "SourceUrl": "https://phd.aws.amazon.com/phd/home#/event-log?
eventID=arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
```

```

    "ProductFields": {
      "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/
aws/health/arn:aws:health:us-east-1::event/SES/AWS_SES_CMF_PENDING_TO_SUCCESS/
AWS_SES_CMF_PENDING_TO_SUCCESS_303388638044_33fe2115-8dad-40ce-b533-78e29f49de96",
      "aws/securityhub/ProductName": "Health",
      "aws/securityhub/CompanyName": "AWS"
    },
    "Resources": [
      {
        "Type": "Other",
        "Id": "4557227d-9257-4e49-8d5b-18a99ced4be9.cmf.pinpoint.sysmon-
iad.adzel.com"
      }
    ],
    "WorkflowState": "NEW",
    "Workflow": {
      "Status": "NEW"
    },
    "RecordState": "ACTIVE",
    "FindingProviderFields": {
      "Severity": {
        "Label": "MEDIUM"
      },
      "Types": [
        "Software and Configuration Checks"
      ]
    }
  }
]
}

```

Abilitazione e configurazione dell'integrazione

Dopo aver abilitato Security Hub, questa integrazione viene attivata automaticamente. AWS Health inizia immediatamente a inviare i risultati a Security Hub.

Interruzione dell'invio degli esiti a Security Hub

Per interrompere l'invio dei risultati a Security Hub, puoi utilizzare la console Security Hub, l'API Security Hub o AWS CLI.

Vedi [Disabilitazione e abilitazione del flusso di risultati di un'integrazione \(Console\)](#) o [Disabilitazione del flusso di risultati da un'integrazione \(API Security Hub, AWS CLI\)](#).

AWS Identity and Access Management Access Analyzer (Invia i risultati)

Con IAM Access Analyzer, tutti i risultati vengono inviati a Security Hub.

IAM Access Analyzer utilizza il ragionamento basato sulla logica per analizzare le politiche basate sulle risorse applicate alle risorse supportate nel tuo account. IAM Access Analyzer genera un risultato quando rileva una dichiarazione di policy che consente a un principale esterno di accedere a una risorsa del tuo account.

In IAM Access Analyzer, solo l'account amministratore può visualizzare i risultati degli analizzatori che si applicano a un'organizzazione. Per gli analizzatori di organizzazioni, il campo `AwsAccountId` ASFF riflette l'ID dell'account amministratore. Sotto `ProductFields`, il `ResourceOwnerAccount` campo indica l'account in cui è stato scoperto il risultato. Se abiliti gli analizzatori singolarmente per ogni account, Security Hub genera più risultati, uno che identifica l'ID dell'account amministratore e uno che identifica l'ID dell'account della risorsa.

Per ulteriori informazioni, consulta [Integration with AWS Security Hub](#) nella IAM User Guide.

Amazon Inspector (invia i risultati)

Amazon Inspector è un servizio di gestione delle vulnerabilità che analizza continuamente i carichi di lavoro alla ricerca AWS di eventuali vulnerabilità. Amazon Inspector rileva e analizza automaticamente le istanze e le immagini dei container di Amazon EC2 che si trovano nell'Amazon Elastic Container Registry. La scansione cerca le vulnerabilità del software e l'esposizione involontaria della rete.

Dopo aver abilitato Security Hub, questa integrazione viene attivata automaticamente. Amazon Inspector inizia immediatamente a inviare tutti i risultati generati a Security Hub.

Per ulteriori informazioni sull'integrazione, consulta [Integration with AWS Security Hub](#) nella Amazon Inspector User Guide.

Security Hub può anche ricevere risultati da Amazon Inspector Classic. Amazon Inspector Classic invia a Security Hub i risultati generati tramite esecuzioni di valutazione per tutti i pacchetti di regole supportati.

Per ulteriori informazioni sull'integrazione, consulta [Integration with AWS Security Hub](#) nella Amazon Inspector Classic User Guide.

I risultati di Amazon Inspector e Amazon Inspector Classic utilizzano lo stesso ARN del prodotto. I risultati di Amazon Inspector riportano la seguente voce: `ProductFields`

```
"aws/inspector/ProductVersion": "2",
```

AWS IoT Device Defender (Invia i risultati)

AWS IoT Device Defender è un servizio di sicurezza che verifica la configurazione dei dispositivi IoT, monitora i dispositivi connessi per rilevare comportamenti anomali e aiuta a mitigare i rischi per la sicurezza.

Dopo aver abilitato entrambi AWS IoT Device Defender e Security Hub, visita la [pagina delle integrazioni della console di Security Hub](#) e scegli Accetta risultati per Audit, Detect o entrambi. AWS IoT Device Defender Audit and Detect inizia a inviare tutti i risultati a Security Hub.

AWS IoT Device Defender Audit invia riepiloghi dei controlli a Security Hub, che contengono informazioni generali per un tipo di controllo e un'attività di controllo specifici. AWS IoT Device Defender Detect invia i risultati delle violazioni per i comportamenti statici, statistici e di apprendimento automatico (ML) a Security Hub. Audit invia anche gli aggiornamenti dei risultati a Security Hub.

Per ulteriori informazioni su questa integrazione, consulta [Integration with AWS Security Hub](#) nella AWS IoT Developer Guide.

Amazon Macie (invia risultati)

Un risultato di Macie può indicare che esiste una potenziale violazione delle politiche o che dati sensibili, come le informazioni di identificazione personale (PII), sono presenti nei dati archiviati dalla tua organizzazione in Amazon S3.

Dopo aver abilitato Security Hub, Macie inizia automaticamente a inviare i risultati delle policy a Security Hub. Puoi configurare l'integrazione per inviare anche i risultati dei dati sensibili a Security Hub.

In Security Hub, il tipo di ricerca per una policy o una ricerca di dati sensibili viene modificato in un valore compatibile con ASFF. Ad esempio, il tipo di Policy:IAMUser/S3BucketPublic ricerca in Macie viene visualizzato come Effects/Data Exposure/Policy:IAMUser-S3BucketPublic in Security Hub.

Macie invia anche i risultati dei campioni generati a Security Hub. Per i risultati di esempio, il nome della risorsa interessata è macie-sample-finding-bucket e il valore del Sample campo è true.

Per ulteriori informazioni, consulta [l'integrazione di Amazon Macie con AWS Security Hub nella Guida per l'utente di Amazon Macie](#).

AWS Systems Manager Patch Manager (invia i risultati)

AWS Systems Manager Patch Manager invia i risultati a Security Hub quando le istanze del parco macchine di un cliente non sono conformi allo standard di conformità delle patch.

Patch Manager automatizza il processo di applicazione di patch alle istanze gestite con aggiornamenti relativi alla sicurezza e di altro tipo.

Dopo aver abilitato Security Hub, questa integrazione viene attivata automaticamente. Systems Manager Patch Manager inizia immediatamente a inviare i risultati a Security Hub.

Per ulteriori informazioni sull'utilizzo di Patch Manager, vedere [AWS Systems Manager Patch Manager](#) nella Guida AWS Systems Manager per l'utente.

AWS servizi che ricevono risultati da Security Hub

I seguenti AWS servizi sono integrati con Security Hub e ricevono i risultati da Security Hub.

Dove indicato, il servizio integrato può anche aggiornare i risultati. In questo caso, la ricerca degli aggiornamenti apportati nel servizio integrato si rifletterà anche in Security Hub.

AWS Audit Manager (Riceve i risultati)

AWS Audit Manager riceve i risultati da Security Hub. Questi risultati aiutano gli utenti di Audit Manager a prepararsi per gli audit.

Per ulteriori informazioni su Audit Manager, consulta la [Guida per l'utente di AWS Audit Manager](#). [AWS I controlli Security Hub supportati da AWS Audit Manager](#) elencano i controlli per i quali Security Hub invia i risultati all'Audit Manager.

AWS Chatbot (Riceve i risultati)

AWS Chatbot è un agente interattivo che ti aiuta a monitorare e interagire con AWS le tue risorse nei canali Slack e nelle chat room di Amazon Chime.

AWS Chatbot riceve i risultati da Security Hub.

Per ulteriori informazioni sull' AWS Chatbot integrazione con Security Hub, consulta la [panoramica sull'integrazione di Security Hub](#) nella Guida per l'AWS Chatbot amministratore.

Amazon Detective (riceve i risultati)

Detective raccoglie automaticamente i dati di registro dalle tue AWS risorse e utilizza l'apprendimento automatico, l'analisi statistica e la teoria dei grafi per aiutarti a visualizzare e condurre indagini di sicurezza più rapide ed efficienti.

L'integrazione di Security Hub con Detective ti consente di passare dai GuardDuty risultati di Amazon in Security Hub a Detective. Puoi quindi utilizzare gli strumenti e le visualizzazioni del Detective per indagare su di essi. L'integrazione non richiede alcuna configurazione aggiuntiva in Security Hub o Detective.

Per i risultati ricevuti da altri Servizi AWS, il pannello dei dettagli dei risultati sulla console Security Hub include una sottosezione Investigate in Detective. Quella sottosezione contiene un collegamento a Detective dove puoi approfondire il problema di sicurezza segnalato dalla scoperta. Puoi anche creare un grafico comportamentale in Detective basato sui risultati del Security Hub per condurre indagini più efficaci. Per ulteriori informazioni, consulta [i risultati AWS di sicurezza](#) nell'Amazon Detective Administration Guide.

Se l'aggregazione tra regioni è abilitata, quando si esegue il pivot dalla regione di aggregazione, Detective si apre nella regione in cui ha avuto origine il risultato.

Se un collegamento non funziona, per consigli sulla risoluzione dei problemi, consulta la sezione relativa alla [risoluzione dei problemi del pivot](#).

Amazon Security Lake (riceve i risultati)

Security Lake è un servizio di data lake di sicurezza completamente gestito. Puoi utilizzare Security Lake per centralizzare automaticamente i dati di sicurezza provenienti da fonti cloud, locali e personalizzate in un data lake archiviato nel tuo account. Gli abbonati possono utilizzare i dati di Security Lake per casi d'uso investigativi e di analisi.

Per attivare questa integrazione, è necessario abilitare entrambi i servizi e aggiungere Security Hub come origine nella console di Security Lake, nell'API di Security Lake o AWS CLI. Una volta completati questi passaggi, Security Hub inizia a inviare tutti i risultati a Security Lake.

Security Lake normalizza automaticamente i risultati di Security Hub e li converte in uno schema open source standardizzato chiamato Open Cybersecurity Schema Framework (OCSF). In Security Lake, puoi aggiungere uno o più abbonati per utilizzare i risultati di Security Hub.

Per ulteriori informazioni su questa integrazione, comprese le istruzioni sull'aggiunta di Security Hub come fonte e sulla creazione di abbonati, consulta [Integration with AWS Security Hub](#) nella Amazon Security Lake User Guide.

AWS Systems Manager Explorer e OpsCenter (riceve e aggiorna i risultati)

AWS Systems Manager Esplora e OpsCenter ricevi i risultati da Security Hub e aggiorna tali risultati in Security Hub.

Explorer ti offre una dashboard personalizzabile, che fornisce approfondimenti e analisi chiave sullo stato operativo e sulle prestazioni del tuo AWS ambiente.

OpsCenter offre una posizione centrale per visualizzare, esaminare e risolvere gli elementi di lavoro operativi.

Per ulteriori informazioni su Explorer e OpsCenter, vedere [Gestione delle operazioni](#) nella Guida AWS Systems Manager per l'utente.

AWS Trusted Advisor (Riceve i risultati)

Trusted Advisor si basa sulle migliori pratiche apprese servendo centinaia di migliaia di AWS clienti. Trusted Advisor ispeziona l' AWS ambiente e quindi formula raccomandazioni quando esistono opportunità per risparmiare denaro, migliorare la disponibilità e le prestazioni del sistema o contribuire a colmare le lacune di sicurezza.

Quando abiliti Trusted Advisor sia Security Hub che Security Hub, l'integrazione viene aggiornata automaticamente.

Security Hub invia i risultati dei controlli relativi alle Buone Pratiche di Sicurezza AWS Fondamentali a Trusted Advisor.

Per ulteriori informazioni sull'integrazione di Security Hub con Trusted Advisor, vedere [Visualizzazione dei controlli AWS di Security Hub AWS Trusted Advisor nella AWS Support User Guide](#).

Integrazioni di prodotti partner di terze parti disponibili

AWS Security Hub si integra con diversi prodotti partner di terze parti. Un'integrazione può eseguire una o più delle seguenti azioni:

- Invia i risultati che genera a Security Hub.

- Ricevi i risultati da Security Hub.
- Aggiorna i risultati in Security Hub.

Tutte le integrazioni che inviano i risultati a Security Hub hanno un Amazon Resource Name (ARN).

Note

Alcune integrazioni sono disponibili solo in alcune versioni. Regioni AWS

La pagina Integrazioni della console Security Hub elenca tutte le integrazioni supportate per la regione corrente.

Per ulteriori informazioni, consulta [Integrazioni supportate in Cina \(Pechino\) e Cina \(Ningxia\)](#) e [Integrazioni supportate in AWS GovCloud \(Stati Uniti orientali\) e \(Stati Uniti occidentali\) AWS GovCloud](#).

Se disponi di una soluzione di sicurezza e sei interessato a diventare un partner del Security Hub, invia un'e-mail a <securityhub-partners@amazon.com>. Per ulteriori informazioni, consulta la [AWS Security Hub Partner Integration Guide](#).

Panoramica delle integrazioni di terze parti con Security Hub

Ecco una panoramica delle integrazioni di terze parti che inviano risultati a Security Hub o ricevono risultati da Security Hub.

Integrazione	Direzione	ARN (se applicabile)
3CORESec – 3CORESec NTA	Invia i risultati	arn:aws:securityhub:<REGION>:product/3coresec/3coresec
Alert Logic – SIEMless Threat Management	Invia i risultati	arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement
Aqua Security – Aqua Cloud Native Security Platform	Invia i risultati	arn:aws:securityhub:<REGION>:product

Integrazione	Direzione	ARN (se applicabile)
		/aquasecurity/aqua security
Aqua Security – Kube-bench	Invia i risultati	arn:aws:securityhub: <REGION>::product/aqua-security/kube-bench
Armor – Armor Anywhere	Invia i risultati	arn:aws:securityhub: <REGION>:679703615338:product/armor-defense/armoranywhere
AttackIQ – AttackIQ	Invia i risultati	arn:aws:securityhub: <REGION>::product/attackiq/attackiq-platform
Barracuda Networks – Cloud Security Guardian	Invia i risultati	arn:aws:securityhub: <REGION>:151784055945:product/barracuda/cloudsecurity-guardian
BigID – BigID Enterprise	Invia i risultati	arn:aws:securityhub: <REGION>::product/bigid/bigid-enterprise
Blue Hexagon – Blue Hexagon forAWS	Invia i risultati	arn:aws:securityhub: <REGION>::product/blue-hexagon/blue-hexagon-for-aws

Integrazione	Direzione	ARN (se applicabile)
Capitis Solutions – C2VS	Invia i risultati	arn:aws:securityhub: <REGION>::product/capitis/c2vs
Check Point – CloudGuard IaaS	Invia i risultati	arn:aws:securityhub: <REGION>:758245563457:product/checkpoint/cloudguard-iaas
Check Point – CloudGuard Posture Management	Invia i risultati	arn:aws:securityhub: <REGION>:634729597623:product/checkpoint/dome9-arc
Clarity – xDome	Invia i risultati	arn:aws:securityhub: <REGION>::product/clarity/xdome
Cloud Storage Security—Antivirus for Amazon S3	Invia i risultati	arn:aws:securityhub: <REGION>::product/cloud-storage-security/antivirus-for-amazon-s3
Contrast Security	Invia i risultati	arn:aws:securityhub: <REGION>::product/contrast-security/security-assess
CrowdStrike – CrowdStrike Falcon	Invia i risultati	arn:aws:securityhub: <REGION>:517716713836:product/crowdstrike/crowdstrike-falcon

Integrazione	Direzione	ARN (se applicabile)
CyberArk – Privileged Threat Analytics	Invia i risultati	arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta
Data Theorem – Data Theorem	Invia i risultati	arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure
Drata	Invia i risultati	arn:aws:securityhub:<REGION>::product/drata/drata-integration
Forcepoint – Forcepoint CASB	Invia i risultati	arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb
Forcepoint – Forcepoint Cloud Security Gateway	Invia i risultati	arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway
Forcepoint – Forcepoint DLP	Invia i risultati	arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp

Integrazione	Direzione	ARN (se applicabile)
Forcepoint – Forcepoint NGFW	Invia i risultati	arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw
Fugue – Fugue	Invia i risultati	arn:aws:securityhub:<REGION>::product/fugue/fugue
Guardicore – Centra 4.0	Invia i risultati	arn:aws:securityhub:<REGION>::product/guardicore/guardicore
HackerOne – Vulnerability Intelligence	Invia i risultati	arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence
JFrog – Xray	Invia i risultati	arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray
Juniper Networks – vSRX Next Generation Firewall	Invia i risultati	arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall
k9 Security – Access Analyzer	Invia i risultati	arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer

Integrazione	Direzione	ARN (se applicabile)
Lacework – Lacework	Invia i risultati	arn:aws:securityhub: <REGION>::product/lacework/lacework
McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)	Invia i risultati	arn:aws:securityhub: <REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws
NETSCOUT – NETSCOUT Cyber Investigator	Invia i risultati	arn:aws:securityhub:us-east-1::product/netscout/netscout-cyber-investigator
Palo Alto Networks – Prisma Cloud Compute	Invia i risultati	arn:aws:securityhub: <REGION>:496947949261:product/twistlock/twistlock-enterprise
Palo Alto Networks – Prisma Cloud Enterprise	Invia i risultati	arn:aws:securityhub: <REGION>:188619942792:product/paloaltonetworks/redlock
Plerion – Cloud Security Platform	Invia i risultati	arn:aws:securityhub: <REGION>::product/plerion/cloud-security-platform
Prowler – Prowler	Invia i risultati	arn:aws:securityhub: <REGION>::product/prowler/prowler

Integrazione	Direzione	ARN (se applicabile)
Qualys – Vulnerability Management	Invia i risultati	arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm
Rapid7 – InsightVM	Invia i risultati	arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm
SecureCloudDB – SecureCloudDB	Invia i risultati	arn:aws:securityhub:<REGION>::product/secureclouddb/secureclouddb
SentinelOne – SentinelOne	Invia i risultati	arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection
Snyk	Invia i risultati	arn:aws:securityhub:<region>::product/snyk/snyk
Sonrai Security – Sonrai Dig	Invia i risultati	arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig
Sophos – Server Protection	Invia i risultati	arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection

Integrazione	Direzione	ARN (se applicabile)
StackRox – StackRox Kubernetes Security	Invia i risultati	arn:aws:securityhub: <REGION>::product/stackrox/kubernetes-security
Sumo Logic – Machine Data Analytics	Invia i risultati	arn:aws:securityhub: <REGION>:956882708938:product/sumologicinc/sumologic-mda
Symantec – Cloud Workload Protection	Invia i risultati	arn:aws:securityhub: <REGION>:754237914691:product/symantec-corp/symantec-cwp
Tenable – Tenable.io	Invia i risultati	arn:aws:securityhub: <REGION>:422820575223:product/tenable/tenable-io
Trend Micro – Cloud One	Invia i risultati	arn:aws:securityhub: <REGION>::product/trend-micro/cloud-one
Vectra – Cognito Detect	Invia i risultati	arn:aws:securityhub: <REGION>:978576646331:product/vectra-ai/cognito-detect
Wiz	Invia i risultati	arn:aws:securityhub: <REGION>::product/wiz-security/wiz-security

Integrazione	Direzione	ARN (se applicabile)
Atlassian - Jira Service Management	Riceve e aggiorna i risultati	Non applicabile
Atlassian - Jira Service Management Cloud	Riceve e aggiorna i risultati	Non applicabile
Atlassian – Opsgenie	Riceve i risultati	Non applicabile
Fortinet – FortiCNP	Riceve i risultati	Non applicabile
IBM – QRadar	Riceve i risultati	Non applicabile
Logz.io Cloud SIEM	Riceve i risultati	Non applicabile
MetricStream	Riceve i risultati	Non applicabile
MicroFocus – MicroFocus Arcsight	Riceve i risultati	Non applicabile
New Relic Vulnerability Management	Riceve i risultati	Non applicabile
PagerDuty – PagerDuty	Riceve i risultati	Non applicabile
Palo Alto Networks – Cortex XSOAR	Riceve i risultati	Non applicabile
Palo Alto Networks – VM-Series	Riceve i risultati	Non applicabile
Rackspace Technology – Cloud Native Security	Riceve i risultati	Non applicabile
Rapid7 – InsightConnect	Riceve i risultati	Non applicabile
RSA – RSA Archer	Riceve i risultati	Non applicabile
ServiceNow – ITSM	Riceve e aggiorna i risultati	Non applicabile

Integrazione	Direzione	ARN (se applicabile)
Slack – Slack	Riceve i risultati	Non applicabile
Splunk – Splunk Enterprise	Riceve i risultati	Non applicabile
Splunk – Splunk Phantom	Riceve i risultati	Non applicabile
ThreatModeler	Riceve i risultati	Non applicabile
Trellix – Trellix Helix	Riceve i risultati	Non applicabile
Caveonix – Caveonix Cloud	Invia e riceve i risultati	arn:aws:securityhub: <REGION>::product/caveonix/caveonix-cloud
Cloud Custodian – Cloud Custodian	Invia e riceve i risultati	arn:aws:securityhub: <REGION>::product/cloud-custodian/cloud-custodian
DisruptOps, Inc. – DisruptOPS	Invia e riceve i risultati	arn:aws:securityhub: <REGION>::product/disruptops-inc/disruptops
Kion	Invia e riceve i risultati	arn:aws:securityhub: <REGION>::product/cloudtamerio/cloudtamerio
Turbot – Turbot	Invia e riceve i risultati	arn:aws:securityhub: <REGION>:453761072151:product/turbot/turbot

Integrazioni di terze parti che inviano i risultati a Security Hub

Le seguenti integrazioni di prodotti di partner terzi inviano i risultati a Security Hub. Security Hub trasforma i risultati nel [AWS Security Finding Format](#).

3CORESec – 3CORESec NTA

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/3coresec/3coresec`

3CORESec fornisce servizi di rilevamento gestiti sia per ambienti locali che per sistemi. AWS La loro integrazione con Security Hub consente la visibilità su minacce come malware, escalation dei privilegi, movimenti laterali e segmentazione impropria della rete.

[Link al prodotto](#)

[Documentazione dei partner](#)

Alert Logic – SIEMless Threat Management

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:733251395267:product/alertlogic/althreatmanagement`

Ottieni il giusto livello di copertura: visibilità delle vulnerabilità e degli asset, rilevamento delle minacce e gestione degli incidenti e opzioni assegnate agli analisti SOC. AWS WAF

[Link al prodotto](#)

[Documentazione dei partner](#)

Aqua Security – Aqua Cloud Native Security Platform

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/aquasecurity/aquasecurity`

Aqua Cloud Native Security Platform (CSP) offre la sicurezza completa del ciclo di vita per le applicazioni basate su container e serverless, dalla pipeline CI/CD agli ambienti di produzione in fase di esecuzione.

[Link al prodotto](#)

[Documentazione dei partner](#)

Aqua Security – Kube-bench

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/aqua-security/kube-bench`

Kube-bench è uno strumento open source che esegue il benchmark Kubernetes Center for Internet Security (CIS) nel tuo ambiente.

[Link al prodotto](#)

[documentazione per i partner](#)

Armor – Armor Anywhere

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:679703615338:product/armordefense/armoranywhere`

Armor Anywhere offre sicurezza e conformità gestite per AWS.

[Link al prodotto](#)

[documentazione per i partner](#)

AttackIQ – AttackIQ

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/attackiq/attackiq-platform`

AttackIQ Platform emula un comportamento antagonista reale in linea con il MITRE ATT&CK Framework per aiutare a convalidare e migliorare il livello di sicurezza generale.

[Link al prodotto](#)

[Documentazione dei partner](#)

Barracuda Networks – Cloud Security Guardian

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:151784055945:product/barracuda/cloudsecurityguardian`

Barracuda Cloud Security Sentry aiuta le organizzazioni a rimanere sicure durante la creazione di applicazioni e lo spostamento dei carichi di lavoro nel cloud pubblico.

[AWS Link al Marketplace](#)

[Link al prodotto](#)

BigID – BigID Enterprise

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/bigid/bigid-enterprise`

BigID Enterprise Privacy Management Platform aiuta le aziende a gestire e proteggere i dati sensibili (PII) su tutti i loro sistemi.

[Link al prodotto](#)

[Documentazione dei partner](#)

Blue Hexagon— Blue Hexagon per AWS

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/blue-hexagon/blue-hexagon-for-aws`

Blue Hexagon è una piattaforma di rilevamento delle minacce in tempo reale. Utilizza i principi del deep learning per rilevare minacce note e sconosciute, inclusi malware e anomalie di rete.

[AWS Link al Marketplace](#)

[Documentazione dei partner](#)

Capitis Solutions – C2VS

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/capitis/c2vs`

C2VS è una soluzione di conformità personalizzabile progettata per identificare automaticamente le configurazioni errate specifiche dell'applicazione e la loro causa principale.

[Link al prodotto](#)

[documentazione per i partner](#)

Check Point – CloudGuard IaaS

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:758245563457:product/checkpoint/cloudguard-iaas`

Check Point CloudGuard estende facilmente la sicurezza completa per la prevenzione delle minacce proteggendo al AWS contempo le risorse nel cloud.

[Link al prodotto](#)

[Documentazione dei partner](#)

Check Point – CloudGuard Posture Management

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:634729597623:product/checkpoint/dome9-arc`

Una piattaforma SaaS che offre sicurezza di rete cloud verificabile, protezione IAM avanzata e conformità e governance complete.

[Link al prodotto](#)

[Documentazione dei partner](#)

Claroty – xDome

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/claroty/xdome`

Claroty xDome aiuta le organizzazioni a proteggere i propri sistemi cyber-fisici attraverso l'Extended Internet of Things (XIoT) all'interno di ambienti industriali (OT), sanitari (IoMT) e aziendali (IoT).

[Link al prodotto](#)

[Documentazione dei partner](#)

Cloud Storage Security— Antivirus for Amazon S3

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/cloud-storage-security/antivirus-for-amazon-s3`

Cloud Storage Security fornisce una scansione antimalware e antivirus nativa per il cloud per oggetti Amazon S3.

Antivirus for Amazon S3 offre scansioni pianificate e in tempo reale di oggetti e file in Amazon S3 alla ricerca di malware e minacce. Fornisce visibilità e risoluzione di problemi e file infetti.

[Link al prodotto](#)

[Documentazione dei partner](#)

Contrast Security – Contrast Assess

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/contrast-security/security-assess`

Contrast Security Contrast Assess è uno strumento IAST che offre il rilevamento delle vulnerabilità in tempo reale in app Web, API e microservizi. Contrast Assess si integra con Security Hub per contribuire a fornire visibilità e risposta centralizzate per tutti i carichi di lavoro.

[Link al prodotto](#)

[Documentazione dei partner](#)

CrowdStrike – CrowdStrike Falcon

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:517716713836:product/crowdstrike/crowdstrike-falcon`

Il sensore CrowdStrike Falcon unico e leggero unisce l'antivirus di nuova generazione, il rilevamento e la risposta degli endpoint e la caccia gestita 24 ore su 24, 7 giorni su 7 attraverso il cloud.

[Link al prodotto](#)

[Documentazione dei partner](#)

CyberArk – Privileged Threat Analytics

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:749430749651:product/cyberark/cyberark-pta`

Privileged Threat Analytics raccoglie, rileva, avvisa e risponde alle attività e ai comportamenti ad alto rischio degli account privilegiati per contenere gli attacchi in corso.

[Link al prodotto](#)

[Documentazione dei partner](#)

Data Theorem – Data Theorem

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/data-theorem/api-cloud-web-secure`

Data Theorem analizza continuamente applicazioni Web, API e risorse cloud alla ricerca di falle di sicurezza e lacune nella privacy dei dati per prevenire violazioni dei dati. AppSec

[Link al prodotto](#)

[Documentazione dei partner](#)

Drata

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/drata/drata-integration`

Drata è una piattaforma di automazione della conformità che consente di raggiungere e mantenere la conformità con vari framework, come SOC2, ISO e GDPR. L'integrazione tra Drata e Security Hub ti aiuta a centralizzare i risultati di sicurezza in un'unica posizione.

[AWS Link al Marketplace](#)

[Documentazione dei partner](#)

Forcepoint – Forcepoint CASB

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-casb`

Forcepoint CASB consente di scoprire l'uso delle applicazioni cloud, analizzare i rischi e applicare controlli appropriati per SaaS e applicazioni personalizzate.

[Link al prodotto](#)

[Documentazione dei partner](#)

Forcepoint – Forcepoint Cloud Security Gateway

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/forcepoint/forcepoint-cloud-security-gateway`

Forcepoint Cloud Security Gateway è un servizio di sicurezza cloud convergente che offre visibilità, controllo e protezione dalle minacce per utenti e dati, ovunque si trovino.

[Link al prodotto](#)

[Documentazione dei partner](#)

Forcepoint – Forcepoint DLP

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-dlp`

Forcepoint DLPaffronta il rischio incentrato sull'uomo con visibilità e controllo ovunque lavorino i dipendenti e ovunque risiedano i dati.

[Link al prodotto](#)

[documentazione per i partner](#)

Forcepoint – Forcepoint NGFW

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:365761988620:product/forcepoint/forcepoint-ngfw`

Forcepoint NGFWconsente di connettere AWS l'ambiente alla rete aziendale con la scalabilità, la protezione e le informazioni necessarie per gestire la rete e rispondere alle minacce.

[Link al prodotto](#)

[Documentazione dei partner](#)

Fugue – Fugue

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/fugue/fugue`

Fugueè una piattaforma cloud-native scalabile e senza agente che automatizza la convalida continua degli ambienti di infrastructure-as-code runtime cloud utilizzando le stesse policy.

[Link al prodotto](#)

[Documentazione dei partner](#)

Guardicore – Centra 4.0

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/guardicore/guardicore`

Guardicore Centraforne la visualizzazione del flusso, la microsegmentazione e il rilevamento delle violazioni per i carichi di lavoro nei data center e nei cloud moderni.

[Link al prodotto](#)

[Documentazione dei partner](#)

HackerOne – Vulnerability Intelligence

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/hackerone/vulnerability-intelligence`

La HackerOne piattaforma collabora con la comunità globale di hacker per scoprire i problemi di sicurezza più rilevanti. Vulnerability Intelligence consente all'organizzazione di andare oltre la scansione automatica. Condivide le vulnerabilità che gli hacker HackerOne etici hanno convalidato e fornito misure per riprodurre.

[AWS link al marketplace](#)

[documentazione per i partner](#)

JFrog – Xray

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/jfrog/jfrog-xray`

JFrog Xray è uno strumento universale di analisi della composizione del software (SCA) per la sicurezza delle applicazioni che analizza continuamente i file binari per verificare la conformità delle licenze e le vulnerabilità di sicurezza, in modo da poter gestire una catena di fornitura software sicura.

[AWS Link al Marketplace](#)

[Documentazione dei partner](#)

Juniper Networks – vSRX Next Generation Firewall

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/juniper-networks/vsrx-next-generation-firewall`

Juniper Networks'vSRx Virtual Next Generation Firewall offre un firewall virtuale completo basato sul cloud con sicurezza avanzata, SD-WAN sicura, rete robusta e automazione integrata.

[AWS Link al Marketplace](#)

[Documentazione dei partner](#)

[Link al prodotto](#)

k9 Security – Access Analyzer

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/k9-security/access-analyzer`

k9 Security ti avvisa quando vengono apportate importanti modifiche all'accesso nel tuo AWS Identity and Access Management account. Con k9 Security, puoi comprendere l'accesso che gli utenti e i ruoli IAM hanno ai dati critici Servizi AWS e ai tuoi dati.

k9 Security è progettato per la distribuzione continua e consente di rendere operativo IAM con audit di accesso attuabili e una semplice automazione delle politiche per Terraform e AWS CDK.

[Link al prodotto](#)

[Documentazione dei partner](#)

Lacework – Lacework

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/lacework/lacework`

Lacework è la piattaforma di sicurezza basata sui dati per il cloud. La Lacework Cloud Security Platform automatizza la sicurezza del cloud su larga scala in modo da poter innovare con velocità e sicurezza.

[Link al prodotto](#)

[Documentazione dei partner](#)

McAfee – MVISION Cloud Native Application Protection Platform (CNAPP)

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/mcafee-skyhigh/mcafee-mvision-cloud-aws`

McAfee MVISION Cloud Native Application Protection Platform (CNAPP) offre Cloud Security Posture Management (CSPM) e Cloud Workload Protection Platform (CWPP) per il tuo ambiente. AWS

[Link al prodotto](#)

[documentazione per i partner](#)

NETSCOUT – NETSCOUT Cyber Investigator

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/netscout/netscout-cyber-investigator`

NETSCOUT Cyber Investigator è una piattaforma di analisi forense, indagine sui rischi e analisi forense delle minacce di rete a livello aziendale che aiuta a ridurre l'impatto delle minacce informatiche sulle aziende.

[Link al prodotto](#)

[Documentazione dei partner](#)

Palo Alto Networks – Prisma Cloud Compute

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:496947949261:product/twistlock/twistlock-enterprise`

Prisma Cloud Compute è una piattaforma di sicurezza informatica nativa per il cloud che protegge VM, container e piattaforme serverless.

[Link al prodotto](#)

[Documentazione dei partner](#)

Palo Alto Networks – Prisma Cloud Enterprise

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:188619942792:product/paloaltonetworks/redlock`

Protegge la tua AWS implementazione con analisi della sicurezza nel cloud, rilevamento avanzato delle minacce e monitoraggio della conformità.

[Link al prodotto](#)

[Documentazione dei partner](#)

Plerion – Cloud Security Platform

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/plerion/cloud-security-platform`

Plerion è una piattaforma di sicurezza cloud con un approccio unico basato sulle minacce e basato sul rischio che offre azioni preventive, investigative e correttive per tutti i carichi di lavoro. L'integrazione tra Plerion e Security Hub consente ai clienti di centralizzare e agire in base ai propri risultati di sicurezza in un unico posto.

[AWS Link al Marketplace](#)

[Documentazione dei partner](#)

Prowler – Prowler

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/prowler/prowler`

Prowler è uno strumento di sicurezza open source per eseguire AWS controlli relativi alle migliori pratiche di sicurezza, al rafforzamento e al monitoraggio continuo.

[Link al prodotto](#)

[Documentazione dei partner](#)

Qualys – Vulnerability Management

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:805950163170:product/qualys/qualys-vm`

Qualys Vulnerability Management (VM) analizza e identifica continuamente le vulnerabilità, proteggendo le tue risorse.

[Link al prodotto](#)

[Documentazione dei partner](#)

Rapid7 – InsightVM

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:336818582268:product/rapid7/insightvm`

Rapid7 InsightVM fornisce la gestione delle vulnerabilità per gli ambienti moderni, consentendoti di individuare, assegnare priorità e correggere in modo efficiente le vulnerabilità.

[Link al prodotto](#)

[Documentazione dei partner](#)

SecureCloudDB – SecureCloudDB

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/secureclouddb/secureclouddb`

SecureCloudDB è uno strumento di sicurezza dei database nativo del cloud che offre una visibilità completa delle posizioni e delle attività di sicurezza interne ed esterne. Segnala le violazioni di sicurezza e fornisce soluzioni alle vulnerabilità sfruttabili del database.

[Link al prodotto](#)

[Documentazione dei partner](#)

SentinelOne – SentinelOne

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/sentinelone/endpoint-protection`

SentinelOne è una piattaforma autonoma di rilevamento e risposta estesa (XDR) che comprende prevenzione, rilevamento, risposta e caccia basati sull'intelligenza artificiale su endpoint, container, carichi di lavoro cloud e dispositivi IoT.

[AWS Link al Marketplace](#)

[Link al prodotto](#)

Snyk

Tipo di integrazione: Invia

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/snyk/snyk`

Snyk fornisce una piattaforma di sicurezza che analizza i componenti delle app alla ricerca di rischi per la sicurezza nei carichi di lavoro in esecuzione. AWS Questi rischi vengono inviati a Security Hub come risultati, aiutando gli sviluppatori e i team di sicurezza a visualizzarli e assegnare priorità insieme al resto dei risultati di sicurezza. AWS

[AWS Link al Marketplace](#)

[Documentazione dei partner](#)

Sonrai Security – Sonrai Dig

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/sonrai-security/sonrai-dig`

Sonrai Dig monitora e corregge le configurazioni errate del cloud e le violazioni delle policy, in modo da poter migliorare il livello di sicurezza e conformità.

[Link al prodotto](#)

[Documentazione dei partner](#)

Sophos – Server Protection

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:062897671886:product/sophos/sophos-server-protection`

Sophos Server Protection difende le applicazioni e i dati critici alla base dell'organizzazione, utilizzando tecniche complete *defense-in-depth*.

[Link al prodotto](#)

[Documentazione dei partner](#)

StackRox – StackRox Kubernetes Security

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/stackrox/kubernetes-security`

StackRox aiuta le aziende a proteggere le implementazioni di container e Kubernetes su larga scala applicando le politiche di conformità e sicurezza durante l'intero ciclo di vita dei container: creazione, implementazione ed esecuzione.

[Link al prodotto](#)

[Documentazione dei partner](#)

Sumo Logic – Machine Data Analytics

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:956882708938:product/sumologicinc/sumologic-mda`

Sumo Logic è una piattaforma di analisi dei dati automatici sicura che consente ai team operativi di sviluppo e sicurezza di creare, eseguire e proteggere AWS le proprie applicazioni.

[Link al prodotto](#)

[Documentazione dei partner](#)

Symantec – Cloud Workload Protection

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:754237914691:product/symantec-corp/symantec-cwp`

Cloud Workload Protection fornisce una protezione completa per le istanze Amazon EC2 con antimalware, prevenzione delle intrusioni e monitoraggio dell'integrità dei file.

[Link al prodotto](#)

[Documentazione dei partner](#)

Tenable – Tenable.io

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:422820575223:product/tenable/tenable-io`

Identifica, analizza e definisce la priorità delle vulnerabilità. Gestito nel cloud.

[Link al prodotto](#)

[Documentazione dei partner](#)

Trend Micro – Cloud One

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/trend-micro/cloud-one`

Trend Micro Cloud One fornisce le informazioni di sicurezza giuste ai team nel momento e nel luogo giusti. Questa integrazione invia i risultati di sicurezza a Security Hub in tempo reale, migliorando la visibilità AWS delle risorse e dei dettagli Trend Micro Cloud One degli eventi in Security Hub.

[AWS Link al Marketplace](#)

[Documentazione dei partner](#)

Vectra – Cognito Detect

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>:978576646331:product/vectra-ai/cognito-detect`

Vectrasta trasformando la sicurezza informatica applicando l'intelligenza artificiale avanzata per rilevare e rispondere agli aggressori informatici nascosti prima che possano rubare o causare danni.

[AWS Link al Marketplace](#)

[Documentazione dei partner](#)

Wiz – Wiz Security

Tipo di integrazione: invio

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/wiz-security/wiz-security`

Wiz analizza continuamente configurazioni, vulnerabilità, reti, impostazioni IAM, segreti e altro ancora tra utenti e carichi di lavoro per scoprire problemi critici che rappresentano un rischio effettivo. Account AWS Integra Wiz con Security Hub per visualizzare e rispondere ai problemi rilevati da Wiz dalla console Security Hub.

[AWS Link al Marketplace](#)

[Documentazione dei partner](#)

Integrazioni di terze parti che ricevono risultati da Security Hub

Le seguenti integrazioni di prodotti di partner terzi ricevono i risultati di Security Hub. Dove indicato, i prodotti possono anche aggiornare i risultati. In questo caso, la ricerca degli aggiornamenti apportati al prodotto partner si rifletterà anche in Security Hub.

Atlassian - Jira Service Management

Tipo di integrazione: ricezione e aggiornamento

Il AWS Service Management Connector for Jira invia i risultati da Security Hub a Jira. I Jira problemi vengono creati in base ai risultati. Quando i Jira problemi vengono aggiornati, i risultati corrispondenti vengono aggiornati in Security Hub.

L'integrazione supporta solo Jira Server e Jira Data Center.

Per una panoramica dell'integrazione e di come funziona, guarda il video [AWS Security Hub — Integrazione bidirezionale](#) con Atlassian Jira Service Management

[Link al prodotto](#)

[Documentazione dei partner](#)

Atlassian - Jira Service Management Cloud

Tipo di integrazione: ricezione e aggiornamento

Jira Service Management Cloud è il componente cloud di Jira Service Management.

Il AWS Service Management Connector for Jira invia i risultati da Security Hub a Jira. I risultati innescano la creazione di problemi in Jira Service Management Cloud. Quando aggiorni questi problemi in Jira Service Management Cloud, i risultati corrispondenti vengono aggiornati anche in Security Hub.

[Link al prodotto](#)

[Documentazione dei partner](#)

Atlassian – Opsgenie

Tipo di integrazione: ricezione

Opsgenie è una moderna soluzione di gestione degli incidenti per la gestione di servizi sempre attivi, che consente ai team di sviluppo e operativi di pianificare le interruzioni del servizio e mantenere il controllo durante gli incidenti.

L'integrazione con Security Hub garantisce che gli incidenti di sicurezza mission critical vengano indirizzati ai team appropriati per una risoluzione immediata.

[Link al prodotto](#)

[Documentazione dei partner](#)

Fortinet – FortiCNP

Tipo di integrazione: ricezione

FortiCNP è un prodotto Cloud Native Protection che aggrega i risultati sulla sicurezza in informazioni fruibili e dà priorità alle informazioni sulla sicurezza in base al punteggio di rischio per ridurre l'affaticamento degli avvisi e accelerare la correzione.

[AWS Link al Marketplace](#)[Documentazione dei partner](#)

IBM – QRadar

Tipo di integrazione: ricezione

IBM QRadarSIEM offre ai team di sicurezza la capacità di rilevare, assegnare priorità, indagare e rispondere alle minacce in modo rapido e preciso.

[Link al prodotto](#)[Documentazione dei partner](#)

Logz.io Cloud SIEM

Tipo di integrazione: ricezione

Logz.io è un fornitore Cloud SIEM che fornisce una correlazione avanzata di dati di log ed eventi per aiutare i team di sicurezza a rilevare, analizzare e rispondere alle minacce alla sicurezza in tempo reale.

[Link al prodotto](#)[Documentazione dei partner](#)

MetricStream – CyberGRC

Tipo di integrazione: ricezione

MetricStream CyberGRCTi aiuta a gestire, misurare e mitigare i rischi di sicurezza informatica. Ricevendo i risultati del Security Hub, CyberGRC offre una maggiore visibilità su questi rischi, in modo da poter dare priorità agli investimenti in sicurezza informatica e rispettare le politiche IT.

[AWS Link al Marketplace](#)[Link al prodotto](#)

MicroFocus – MicroFocus Arcsight

Tipo di integrazione: Ricevere

ArcSight accelera il rilevamento e la risposta efficaci alle minacce in tempo reale, integrando la correlazione degli eventi e l'analisi supervisionata e non supervisionata con l'automazione e l'orchestrazione della risposta.

[Link al prodotto](#)

[Documentazione dei partner](#)

New Relic Vulnerability Management

Tipo di integrazione: ricezione

New Relic Vulnerability Management riceve i risultati di sicurezza da Security Hub, in modo da poter ottenere una visione centralizzata della sicurezza insieme alla telemetria delle prestazioni nel contesto dell'intero stack.

[AWS Link al Marketplace](#)

[Documentazione dei partner](#)

PagerDuty – PagerDuty

Tipo di integrazione: ricezione

La piattaforma di gestione delle operazioni PagerDuty digitali consente ai team di mitigare in modo proattivo i problemi che hanno un impatto sui clienti trasformando automaticamente qualsiasi segnale in informazioni e azioni corrette.

AWS gli utenti possono utilizzare il PagerDuty set di AWS integrazioni per scalare i propri ambienti ibridi con sicurezza. AWS

Se abbinato agli avvisi di sicurezza aggregati e organizzati di Security Hub, PagerDuty consente ai team di automatizzare il processo di risposta alle minacce e di impostare rapidamente azioni personalizzate per prevenire potenziali problemi.

PagerDuty gli utenti che stanno intraprendendo un progetto di migrazione al cloud possono agire rapidamente, riducendo al contempo l'impatto dei problemi che si verificano durante il ciclo di vita della migrazione.

[Link al prodotto](#)

[Documentazione dei partner](#)

Palo Alto Networks – Cortex XSOAR

Tipo di integrazione: ricezione

Cortex XSOAR è una piattaforma SOAR (Security Orchestration, Automation and Response) che si integra con l'intero stack di prodotti di sicurezza per accelerare la risposta agli incidenti e le operazioni di sicurezza.

[Link al prodotto](#)

[Documentazione dei partner](#)

Palo Alto Networks – VM-Series

Tipo di integrazione: ricezione

Palo Alto VM-Series l'integrazione con Security Hub raccoglie informazioni sulle minacce e le invia al firewall di VM-Series nuova generazione come aggiornamento automatico della politica di sicurezza che blocca le attività dannose degli indirizzi IP.

[Link al prodotto](#)

[documentazione per i partner](#)

Rackspace Technology – Cloud Native Security

Tipo di integrazione: ricezione

Rackspace Technology fornisce servizi di sicurezza gestiti oltre a prodotti di AWS sicurezza nativi per il monitoraggio 24 ore su 24, 7 giorni su 7, 365 giorni l'anno tramite Rackspace SOC, l'analisi avanzata e la risoluzione delle minacce.

[Link al prodotto](#)

Rapid7 – InsightConnect

Tipo di integrazione: Ricevi

Rapid7 InsightConnect è una soluzione di orchestrazione e automazione della sicurezza che consente al team di ottimizzare le operazioni SOC con poco o nessun codice.

[Link al prodotto](#)

[Documentazione dei partner](#)

RSA – RSA Archer

Tipo di integrazione: ricezione

RSA ArcherLa gestione dei rischi IT e di sicurezza consente di determinare quali risorse sono fondamentali per l'azienda, stabilire e comunicare politiche e standard di sicurezza, rilevare e rispondere agli attacchi, identificare e correggere le carenze di sicurezza e stabilire chiare best practice di gestione del rischio IT.

[Link al prodotto](#)

[Documentazione dei partner](#)

ServiceNow – ITSM

Tipo di integrazione: ricezione e aggiornamento

L'ServiceNowintegrazione con Security Hub consente di visualizzare all'interno i risultati di sicurezza di Security HubServiceNow ITSM. Puoi anche configurare ServiceNow per creare automaticamente un incidente o un problema quando riceve un risultato da Security Hub.

Qualsiasi aggiornamento a questi incidenti e problemi comporta l'aggiornamento dei risultati in Security Hub.

Per una panoramica dell'integrazione e di come funziona, guarda il video [AWS Security Hub - Integrazione bidirezionale](#) con. ServiceNow ITSM

[Link al prodotto](#)

[Documentazione dei partner](#)

Slack – Slack

Tipo di integrazione: ricezione

Slackè un livello dello stack tecnologico aziendale che riunisce persone, dati e applicazioni. Si tratta di un unico luogo in cui le persone possono collaborare in modo efficiente, trovare informazioni importanti e accedere a centinaia di migliaia di applicazioni e servizi critici per svolgere al meglio il loro lavoro.

[Link al prodotto](#)

[documentazione per i partner](#)

Splunk – Splunk Enterprise

Tipo di integrazione: ricezione

Splunk utilizza Amazon CloudWatch Events come consumatore dei risultati di Security Hub. Invia i tuoi dati a Splunk per analisi di sicurezza avanzate e SIEM.

[Link al prodotto](#)

[Documentazione dei partner](#)

Splunk – Splunk Phantom

Tipo di integrazione: ricezione

Con l'Splunk Phantom applicazione per AWS Security Hub, i risultati vengono inviati Phantom per l'arricchimento automatico del contesto con ulteriori informazioni di intelligence sulle minacce o per eseguire azioni di risposta automatiche.

[Link al prodotto](#)

[Documentazione dei partner](#)

ThreatModeler

Tipo di integrazione: ricezione

ThreatModeler è una soluzione di modellazione automatizzata delle minacce che protegge e ridimensiona il ciclo di vita del software aziendale e dello sviluppo del cloud.

[Link al prodotto](#)

[documentazione per i partner](#)

Trellix – Trellix Helix

Tipo di integrazione: ricezione

Trellix Helix è una piattaforma operativa di sicurezza ospitata nel cloud che consente alle organizzazioni di assumere il controllo di qualsiasi incidente, dall'avviso alla risoluzione.

[Link al prodotto](#)

[Documentazione dei partner](#)

Integrazioni di terze parti che inviano e ricevono risultati da Security Hub

Le seguenti integrazioni di prodotti di partner terzi inviano e ricevono i risultati da Security Hub.

Caveonix – Caveonix Cloud

Tipo di integrazione: invio e ricezione

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/caveonix/caveonix-cloud`

La piattaforma Caveonix basata sull'intelligenza artificiale automatizza la visibilità, la valutazione e la mitigazione nei cloud ibridi, coprendo servizi, VM e contenitori nativi del cloud. Integrato con AWS Security Hub, Caveonix unisce AWS dati e analisi avanzate per approfondire gli avvisi di sicurezza e la conformità.

[AWS Link al Marketplace](#)[Documentazione dei partner](#)

Cloud Custodian – Cloud Custodian

Tipo di integrazione: invio e ricezione

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/cloud-custodian/cloud-custodian`

Cloud Custodian consente agli utenti di essere ben gestiti nel cloud. Il semplice YAML DSL consente regole facilmente definite per consentire un'infrastruttura cloud ben gestita, sicura e ottimizzata in termini di costi.

[Link al prodotto](#)[Documentazione dei partner](#)

DisruptOps, Inc. – DisruptOPS

Tipo di integrazione: invio e ricezione

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/disruptops-inc/disruptops`

La DisruptOps Security Operations Platform aiuta le organizzazioni a mantenere le migliori pratiche di sicurezza nel cloud attraverso l'uso di guardrail automatizzati.

[Link al prodotto](#)

[Documentazione dei partner](#)

Kion

Tipo di integrazione: invio e ricezione

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/cloudtamerio/cloudtamerio`

Kion (precedentemente cloudtamer.io) è una soluzione completa di governance del cloud per. AWS Kion offre alle parti interessate visibilità sulle operazioni cloud e aiuta gli utenti del cloud a gestire gli account, controllare budget e costi e garantire la conformità continua.

[Link al prodotto](#)

[Documentazione dei partner](#)

Turbot – Turbot

Tipo di integrazione: invio e ricezione

ARN del prodotto: `arn:aws:securityhub:<REGION>::product/turbot/turbot`

Turbot garantisce che la tua infrastruttura cloud sia sicura, conforme, scalabile e ottimizzata in termini di costi.

[Link al prodotto](#)

[Documentazione dei partner](#)

Utilizzo di integrazioni di prodotti personalizzate per inviare i risultati a AWS Security Hub

Oltre ai risultati generati dai AWS servizi integrati e dai prodotti di terze parti, Security Hub può utilizzare i risultati generati da altri prodotti di sicurezza personalizzati.

È possibile inviare questi risultati a Security Hub manualmente utilizzando l'operazione [BatchImportFindingsAPI](#).

Quando configuri l'integrazione personalizzata, utilizza le [linee guida e le liste di controllo](#) fornite nella Security Hub Partner Integration Guide.

Requisiti e raccomandazioni per l'invio di risultati da prodotti per la sicurezza personalizzati

Prima di poter richiamare correttamente l'operazione [BatchImportFindingsAPI](#), è necessario abilitare Security Hub.

I dettagli del risultato devono essere forniti utilizzando il [the section called "Formato dei risultati"](#). Per i risultati dell'integrazione personalizzata, utilizza i seguenti requisiti e suggerimenti.

Impostazione dell'ARN del prodotto

Quando abiliti Security Hub, nel tuo account corrente viene generato un prodotto Amazon Resource Name (ARN) predefinito per Security Hub.

Questo ARN del prodotto ha il seguente formato:

```
arn:aws:securityhub:<region>:<account-id>:product/<account-id>/default.
```

Ad esempio, `arn:aws:securityhub:us-`

```
west-2:123456789012:product/123456789012/default.
```

Utilizza questo ARN del prodotto come il valore per l'attributo [ProductArn](#) quando richiami l'operazione API `BatchImportFindings`.

Definizione del nome dell'azienda e del prodotto

È possibile utilizzare `BatchImportFindings` per impostare un nome aziendale e un nome di prodotto preferiti per l'integrazione personalizzata che invia i risultati a Security Hub.

I nomi specificati sostituiscono il nome dell'azienda e il nome del prodotto preconfigurati, denominati rispettivamente nome personale e nome predefinito, e vengono visualizzati nella console Security Hub e nel codice JSON di ogni risultato. Per informazioni, consulta [Utilizzo di BatchImportFindings per creare e aggiornare i risultati](#).

Impostazione degli ID risultato

È necessario fornire, gestire e incrementare gli ID risultato, utilizzando l'attributo [Id](#).

Ogni nuovo risultato deve avere un ID di ricerca univoco. Se il prodotto personalizzato invia più risultati con lo stesso ID di ricerca, Security Hub elabora solo il primo risultato.

Impostazione dell'ID account

È necessario specificare il proprio ID account, utilizzando l'attributo [AwsAccountId](#).

Impostazione delle date di creazione e aggiornamento

È necessario fornire i propri timestamp per gli attributi [CreatedAt](#) e [UpdatedAt](#).

Aggiornamento dei risultati da prodotti personalizzati

Oltre a inviare nuovi risultati da prodotti personalizzati, puoi anche aggiornare i risultati esistenti di prodotti personalizzati utilizzando l'operazione API [BatchImportFindings](#).

Per aggiornare i risultati esistenti, utilizza l'ID risultato esistente (tramite l'attributo [Id](#)). Invia nuovamente il risultato completo con le informazioni appropriate aggiornate nella richiesta, incluso un timestamp [UpdatedAt](#) modificato.

Esempio di integrazioni personalizzate

È possibile utilizzare le integrazioni di prodotti personalizzate di esempio riportate di seguito come guida per creare la propria soluzione personalizzata.

Invio dei risultati delle Chef InSpec scansioni a Security Hub

È possibile creare un AWS CloudFormation modello che esegua una scansione di [Chef InSpec](#) conformità e quindi invii i risultati a Security Hub.

Per maggiori dettagli, consulta [Monitoraggio continuo della conformità con Chef InSpec e AWS Security Hub](#).

Invio delle vulnerabilità dei container rilevate Trivy da Security Hub

È possibile creare un AWS CloudFormation modello da utilizzare per [AquaSecurity Trivy](#) scansionare i contenitori alla ricerca di vulnerabilità e quindi inviare tali risultati di vulnerabilità a Security Hub.

Per maggiori dettagli, vedi [Come creare una pipeline CI/CD per la scansione delle vulnerabilità dei container con e Security Trivy Hub](#).AWS

Controlli e standard di AWS sicurezza in Security Hub

AWS Security Hub utilizza, aggrega e analizza i risultati di sicurezza di vari prodotti supportati AWS e di terze parti.

Security Hub genera inoltre i propri risultati eseguendo controlli di sicurezza automatici e continui rispetto alle regole. Le regole sono rappresentate dai controlli di sicurezza. I controlli possono, a loro volta, essere abilitati in uno o più standard di sicurezza. I controlli consentono di determinare se i requisiti di uno standard sono soddisfatti.

I controlli di sicurezza rispetto ai controlli generano risultati che è possibile utilizzare per monitorare il livello di sicurezza e identificare risorse specifiche Account AWS o che richiedono attenzione. Ogni controllo è correlato a un AWS servizio e a una risorsa. Ad esempio, i controlli di sicurezza rispetto al controllo [CloudTrail.4](#) determinano se è stata configurata la convalida dei file di registro nei registri. AWS CloudTrail Per ulteriori informazioni sui controlli, vedere [Visualizzazione e gestione dei controlli di sicurezza](#)

È possibile abilitare un controllo in uno o più standard Security Hub abilitati. Quando abiliti uno standard, Security Hub abilita automaticamente i controlli che si applicano allo standard. Gli standard di sicurezza consentono di concentrarsi su uno specifico framework di conformità. Security Hub definisce i controlli che si applicano a ogni standard. Per ulteriori informazioni sugli standard di sicurezza, vedere [Visualizzazione e gestione degli standard di sicurezza](#).

Sulla base dei risultati dei controlli di sicurezza, Security Hub calcola un punteggio di sicurezza complessivo e punteggi di sicurezza specifici per lo standard. Questi punteggi ti aiutano a comprendere il tuo livello di sicurezza. Per ulteriori informazioni sui punteggi, vedere [Come vengono calcolati i punteggi di sicurezza](#).

Per informazioni sui prezzi di Security Hub per i controlli di sicurezza, consulta i [prezzi di Security Hub](#).

Argomenti

- [Autorizzazioni IAM per configurare standard e controlli](#)
- [Controlli di sicurezza e punteggi di sicurezza in Security Hub](#)
- [Riferimento agli standard del Security Hub](#)
- [Visualizzazione e gestione degli standard di sicurezza](#)

- [Riferimento ai controlli del Security Hub](#)
- [Visualizzazione e gestione dei controlli di sicurezza](#)

Autorizzazioni IAM per configurare standard e controlli

Per visualizzare le informazioni sui controlli di sicurezza e abilitare e disabilitare i controlli di sicurezza negli standard, il ruolo AWS Identity and Access Management (IAM) utilizzato per accedere AWS Security Hub richiede le autorizzazioni per chiamare le seguenti azioni API. Senza aggiungere le autorizzazioni per queste azioni, non sarai in grado di chiamare queste API. Per ottenere le autorizzazioni necessarie, puoi utilizzare le [policy gestite da Security Hub](#). In alternativa, puoi aggiornare le policy IAM personalizzate per includere le autorizzazioni per queste azioni. Le policy personalizzate devono includere anche le autorizzazioni per le API [DescribeStandardsControls](#) e [UpdateStandardsControl](#).

- [BatchGetSecurityControls](#)— Restituisce informazioni su una serie di controlli di sicurezza per l'account corrente e. Regione AWS
- [ListSecurityControlDefinitions](#)— Restituisce informazioni sui controlli di sicurezza che si applicano a uno standard specifico.
- [ListStandardsControlAssociations](#)— Indica se un controllo di sicurezza è attualmente abilitato o disabilitato in ogni standard abilitato nell'account.
- [BatchGetStandardsControlAssociations](#)— Per un batch di controlli di sicurezza, indica se ogni controllo è attualmente abilitato o disabilitato in base a uno standard specifico.
- [BatchUpdateStandardsControlAssociations](#)— Utilizzato per abilitare un controllo di sicurezza negli standard che includono il controllo o per disabilitare un controllo negli standard. Si tratta di un sostituto in batch dell'[UpdateStandardsControl](#) API esistente se un amministratore non desidera consentire agli account dei membri di abilitare o disabilitare i controlli.

Oltre alle API precedenti, dovresti aggiungere l'autorizzazione alla chiamata **BatchGetControlEvaluations** al tuo ruolo IAM. Questa autorizzazione è necessaria per visualizzare lo stato di attivazione e conformità di un controllo, i risultati contano per un controllo e il punteggio di sicurezza complessivo per i controlli sulla console Security Hub. Poiché solo le chiamate alla console **BatchGetControlEvaluations**, questa autorizzazione IAM non corrisponde direttamente alle API o AWS CLI ai comandi di Security Hub documentati pubblicamente.

[Per ulteriori informazioni sulle API relative a controlli e standard, consulta l'AWS Security Hub API Reference.](#)

Controlli di sicurezza e punteggi di sicurezza in Security Hub

Per ogni controllo che abiliti, AWS Security Hub esegue controlli di sicurezza. Un controllo di sicurezza determina se le AWS risorse sono conformi alle regole incluse nel controllo.

Alcuni controlli vengono eseguiti secondo una pianificazione periodica. Altri controlli vengono eseguiti solo quando si modifica lo stato della risorsa. Per ulteriori informazioni, consulta [the section called “Pianificazione dell'esecuzione dei controlli di sicurezza”](#).

Molti controlli di sicurezza utilizzano regole AWS Config gestite o personalizzate per stabilire i requisiti di conformità. Per eseguire questi controlli, è necessario impostare AWS Config. Per ulteriori informazioni, consulta [the section called “AWS Config regole e controlli di sicurezza”](#). Altri utilizzano funzioni Lambda personalizzate, gestite da Security Hub e non visibili ai clienti.

Quando Security Hub esegue i controlli di sicurezza, genera i risultati e assegna loro uno stato di conformità. Per ulteriori informazioni sullo stato di conformità, consulta [Valori relativi allo stato di conformità di un risultato](#).

Security Hub utilizza lo stato di conformità dei risultati del controllo per determinare lo stato di controllo generale. Security Hub calcola anche un punteggio di sicurezza per tutti i controlli abilitati e per standard specifici. Per ulteriori informazioni, consulta [the section called “Stato di conformità e stato di controllo”](#) e [the section called “Definizione dei punteggi di sicurezza”](#).

Se hai attivato i risultati del controllo consolidato, Security Hub genera un singolo risultato anche quando un controllo è associato a più di uno standard. Per ulteriori informazioni, consulta [Risultati di controllo consolidati](#).

Argomenti

- [In che modo Security Hub utilizza AWS Config le regole per eseguire i controlli di sicurezza](#)
- [AWS Config risorse necessarie per generare i risultati del controllo](#)
- [Pianificazione dell'esecuzione dei controlli di sicurezza](#)
- [Generazione e aggiornamento dei risultati del controllo](#)
- [Stato di conformità e stato di controllo](#)
- [Definizione dei punteggi di sicurezza](#)

In che modo Security Hub utilizza AWS Config le regole per eseguire i controlli di sicurezza

Per eseguire i controlli di sicurezza sulle risorse del tuo ambiente, AWS Security Hub utilizza i passaggi specificati dallo standard o utilizza AWS Config regole specifiche. Alcune regole sono regole gestite, gestite da AWS Config. Altre regole sono regole personalizzate sviluppate da Security Hub.

AWS Config le regole utilizzate da Security Hub per i controlli vengono chiamate regole collegate ai servizi, poiché sono abilitate e controllate dal servizio Security Hub.

Per abilitare i controlli in base a queste AWS Config regole, devi prima abilitare AWS Config il tuo account e abilitare la registrazione delle risorse per le risorse richieste. Per informazioni su come abilitare AWS Config, vedere [Configurazione AWS Config](#). Per informazioni sulla registrazione delle risorse richieste, vedere [AWS Config risorse necessarie per generare i risultati del controllo](#)

In che modo Security Hub genera le regole collegate ai servizi

Per ogni controllo che utilizza una regola AWS Config collegata al servizio, Security Hub crea istanze delle regole richieste nell'ambiente. AWS

Queste regole collegate ai servizi sono specifiche di Security Hub. che le crea anche se esistono già altre istanze delle stesse regole. La regola collegata al servizio viene aggiunta securityhub prima del nome della regola originale e un identificatore univoco dopo il nome della regola. Ad esempio, per la regola AWS Config gestita originale `vpc-flow-logs-enabled`, il nome della regola collegata al servizio sarebbe qualcosa di simile. `securityhub-vpc-flow-logs-enabled-12345`

Esistono limiti al numero di AWS Config regole che possono essere utilizzate per valutare i controlli. AWS Config Le regole personalizzate create da Security Hub non vengono conteggiate ai fini di tale limite. Puoi abilitare uno standard di sicurezza anche se hai già raggiunto il AWS Config limite per le regole gestite nel tuo account. Per ulteriori informazioni sui limiti delle AWS Config regole, consulta [Service Limits](#) nella Guida per gli AWS Config sviluppatori.

Visualizzazione dei dettagli sulle AWS Config regole per i controlli

Per i controlli che utilizzano regole AWS Config gestite, la descrizione del controllo include un collegamento ai dettagli della AWS Config regola. Le regole personalizzate non sono collegate dalla descrizione del controllo. Per le descrizioni dei controlli, vedere [Riferimento ai controlli del Security Hub](#). Seleziona un controllo dall'elenco per visualizzarne la descrizione.

Per i risultati generati da tali controlli, i dettagli del risultato includono un collegamento alla AWS Config regola associata. Tieni presente che per accedere alla AWS Config regola partendo dai dettagli della ricerca, devi inoltre disporre di un'autorizzazione IAM nell'account selezionato a cui accedere AWS Config.

I dettagli dei risultati nella pagina Risultati, nella pagina Insights e nella pagina Integrazioni includono un collegamento alle regole ai dettagli della AWS Config regola. Per informazioni, consulta [Esame dei dettagli del ritrovamento](#).

Nella pagina dei dettagli del controllo, la colonna Indaga dell'elenco dei risultati contiene un collegamento ai dettagli della AWS Config regola. Per informazioni, consulta [Visualizzazione della AWS Config regola per una risorsa di ricerca](#).

AWS Config risorse necessarie per generare i risultati del controllo

AWS Security Hub genera risultati di controllo eseguendo controlli di sicurezza rispetto ai controlli del Security Hub. Alcuni controlli utilizzano AWS Config regole che valutano la conformità con risorse specifiche. Affinché Security Hub generi risultati per i controlli che hanno un tipo di pianificazione innescato dalla modifica, è necessario attivare la registrazione delle risorse richieste in AWS Config. Non è necessario registrare le risorse per la maggior parte dei controlli che hanno un tipo di pianificazione periodica. Tuttavia, alcuni controlli periodici richiedono la registrazione delle risorse per rilevare le modifiche alla conformità.

Questa pagina fornisce un elenco delle risorse richieste per tutti gli standard e un elenco delle risorse richieste suddivise per standard. La prima tabella elenca anche i controlli del Security Hub che utilizzano ciascuna risorsa.

Se un risultato viene generato da un controllo di sicurezza basato su una AWS Config regola, i dettagli del risultato includono un collegamento Rules alla AWS Config regola associata. Per accedere alla AWS Config regola, il tuo account deve disporre delle autorizzazioni IAM per visualizzare AWS Config le regole.

Note

Regioni AWS Se un controllo non è disponibile, la risorsa corrispondente non è disponibile in AWS Config. Per un elenco dei limiti regionali sui controlli del Security Hub, vedere [Disponibilità dei controlli per regione](#).

AWS Config risorse necessarie per tutti i controlli

Affinché Security Hub generi i risultati relativi ai controlli attivati da Security Hub abilitati alla modifica che utilizzano una AWS Config regola, è necessario registrare queste risorse in AWS Config. Questa tabella indica anche quali controlli richiedono una particolare risorsa. Un controllo può richiedere più di una risorsa.

Servizio	Risorsa richiesta	Controlli correlati
Amazon API Gateway	AWS::ApiGateway::Stage	APIGateway.1 APIGateway.2 APIGateway.3 APIGateway.4 APIGateway.5
	AWS::ApiGatewayV2::Stage	APIGateway.1 APIGateway.9
AWS AppSync	AWS::AppSync::GraphQLApi	AppSync2. AppSync4. AppSync5.
AWS Backup (AWS Backup)	AWS::Backup::RecoveryPoint	Backup.1
AWS Certificate Manager (ACM)	AWS::ACM::Certificate	ACM.1 ACM.2 ACM.3

Servizio	Risorsa richiesta	Controlli correlati
Amazon Athena	AWS::Athena::DataCatalog	Athena.2
	AWS::Athena::WorkGroup	Athena.3
AWS CloudFormation	AWS::CloudFormation::Stack	CloudFormation1. CloudFormation2.
Amazon CloudFront	AWS::CloudFront::Distribution	CloudFront1. CloudFront.3. CloudFront4. CloudFront5. CloudFront6. CloudFront.7 CloudFront8. CloudFront9. CloudFront.10 CloudFront.13 CloudFront.14
AWS CloudTrail	AWS::CloudTrail::Trail	CloudTrail9.
Amazon CloudWatch	AWS::CloudWatch::Alarm	CloudWatch.15 CloudWatch.17

Servizio	Risorsa richiesta	Controlli correlati
AWS CodeArtifact	AWS::CodeArtifact::Repository	CodeArtifact.1.
AWS CodeBuild	AWS::CodeBuild::Project	CodeBuild.1. CodeBuild2. CodeBuild3. CodeBuild4.
Amazon Detective	AWS::Detective::Graph	Detective. 1
AWS Database Migration Service (AWS DMS)	AWS::DMS::Certificate	DMS.2
	AWS::DMS::Endpoint	DMS.9 DMS.10 DMS.11 DMS.12
	AWS::DMS::EventSubscription	DMS.3
	AWS::DMS::ReplicationInstance	DMS.4 DMS.6
	AWS::DMS::ReplicationSubnetGroup	DMS.5

Servizio	Risorsa richiesta	Controlli correlati
	AWS::DMS: :ReplicationTask	DMS.7 DMS.8
Amazon DynamoDB	AWS::DynamoDB::Table	DynamoDB.2 Dynamo DB.6
Amazon Elastic Compute Cloud (EC2)	AWS::EC2: :ClientVpnEndpoint	EC 2.51
	AWS::EC2: :CustomerGateway	EC2,36
	AWS::EC2::EIP	EC2.12 EC2,37
	AWS::EC2: :FlowLog	EC2,48
	AWS::EC2: :Instance	EC2.4 EC2.8 EC2.9 EC2.17 EC2.24 EC2,38 EMR.1 SSM.1

Servizio	Risorsa richiesta	Controlli correlati
	AWS::EC2: :Internet Gateway	EC2,39
	AWS::EC2: :LaunchTe mplate	EC2.25
	AWS::EC2: :NatGateway	EC2,40
	AWS::EC2: :NetworkAc1	EC2.16 EC2.21 EC2,41
	AWS::EC2: :NetworkI nterface	EC2.22 EC2,35
	AWS::EC2: :RouteTable	EC2,42
	AWS::EC2: :SecurityGroup	EC2.2 EC2.13 EC 2.14 EC2.18 EC2.19 EC2,43

Servizio	Risorsa richiesta	Controlli correlati
	AWS::EC2: :Subnet	EC2.15 EC2,44 ElastiCache7. Lambda.5
	AWS::EC2: :TransitG ateway	EC2.23 EC2,52
	AWS::EC2: :TransitG atewayAtt achment	EC2,33
	AWS::EC2: :TransitG atewayRou teTable	EC2,34
	AWS::EC2: :Volume	EC2.3 EC2,45
	AWS::EC2::VPC	EC2,46
	AWS::EC2: :VPCEndpo intService	EC2,47
	AWS::EC2: :VPCPeeri ngConnector	EC2,49
	AWS::EC2: :VPNConnection	EC2.20

Servizio	Risorsa richiesta	Controlli correlati
	AWS::EC2: :VPNGateway	EC2,50
Dimensionamento automatico Amazon EC2	AWS::AutoScaling::AutoScalingGroup	AutoScaling1. AutoScaling2. AutoScaling6. AutoScaling9. AutoScaling.10
	AWS::AutoScaling::LaunchConfiguration	AutoScaling3. Autoscaling.5
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance	SSM.3
	AWS::SSM::ManagedInstanceInventory	SSM.1
	AWS::SSM::PatchCompliance	SSM.2
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::PublicRepository	ECR.4
	AWS::ECR::Repository	ECR.2 ECR.3

Servizio	Risorsa richiesta	Controlli correlati
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS: :Cluster	ECS.12 ECS.14
	AWS::ECS: :Service	ECS.2 ECS.10 ECS.13
	AWS::ECS: :TaskDefinition	ECS.1 ECS.3 ECS.4 ECS.5 ECS.8 ECS.9 ECS.15
Amazon Elastic File System (Amazon EFS)	AWS::EFS: :AccessPoint	EFS.3 EFS.4 EFS.5
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS: :Cluster	EKS.2 EKS.6
	AWS::EKS: :IdentityProviderConfig	EKS.7

Servizio	Risorsa richiesta	Controlli correlati
AWS Elastic Beanstalk	AWS::ElasticBeanstalk::Environment	ElasticBeanstalk1. ElasticBeanstalk2. ElasticBeanstalk3.
Sistema di bilanciamento del carico elastico	AWS::ElasticLoadBalancing::LoadBalancer	ELB.2 ELB.3 ELB.5 ELB.7 ELB.8 ELB.9 ELB.10 ELB.14
	AWS::ElasticLoadBalancingV2::LoadBalancer	ELB.4 ELB.5 ELB.6 ELB.12 ELB.13 LINEA 16

Servizio	Risorsa richiesta	Controlli correlati
ElasticSearch	AWS::Elasticsearch::Domain	ES.3 ES.4 ES.5 ES.6 ES.7 ES.8 ES.9
Amazon EventBridge	AWS::Events::EventBus	EventBridge2. EventBridge3.
	AWS::Events::Endpoint	EventBridge4.
Amazon FSx	AWS::FSx::FileSystem	FSX.1
AWS Global Accelerator	AWS::GlobalAccelerator::Accelerator	GlobalAccelerator1.
AWS Glue	AWS::Glue::Job	Colla. 1
Amazon GuardDuty	AWS::GuardDuty::Detector	GuardDuty4.
	AWS::GuardDuty::Filter	GuardDuty2.

Servizio	Risorsa richiesta	Controlli correlati
	AWS::GuardDuty::IPSet	GuardDuty3.
AWS Identity and Access Management (IAM)	AWS::IAM::Group	IAM.18 SONO 27 KMS.2
	AWS::IAM::Policy	IAM.1 IAM.21 KMS.1
	AWS::IAM::Role	IAM.18 SONO 24 SONO 27 KMS.2
	AWS::IAM::User	IAM.2 IAM.18 SONO 25 SONO 27 KMS.2
AWS Identity and Access Management Access Analyzer	AWS::AccessAnalyzer::Analyzer	IO SONO 23
AWS IoT	AWS::IoT::Authorizer	IoT 4

Servizio	Risorsa richiesta	Controlli correlati
	AWS::IoT: :Dimension	IoT.3
	AWS::IoT: :MitigationAction	IoT.2
	AWS::IoT: :Policy	IoT.6
	AWS::IoT: :RoleAlias	IoT.5
	AWS::IoT: :SecurityProfile	IoT.1
AWS Key Management Service (AWS KMS)	AWS::KMS::Key	KMS.3
Amazon Kinesis	AWS::Kinesis: :Stream	Kinesis.1 Cinesi.2
AWS Lambda	AWS::Lambda: :Function	Lambda.1 Lambda.2 Lambda.3 Lambda.5 Lambda.6
MSK Amazon	AWS::MSK: :Cluster	MSK.1 MSK.2

Servizio	Risorsa richiesta	Controlli correlati
Amazon MQ	AWS::AmazonMQ::Broker	MQ. 2 MQ. 3 MQ.4 MQ.5 MQ.6
AWS Network Firewall	AWS::NetworkFirewall::Firewall	NetworkFirewall1. NetworkFirewall.7 NetworkFirewall9.
	AWS::NetworkFirewall::FirewallPolicy	NetworkFirewall3. NetworkFirewall4. NetworkFirewall5. NetworkFirewall8.
	AWS::NetworkFirewall::RuleGroup	NetworkFirewall6.

Servizio	Risorsa richiesta	Controlli correlati
OpenSearch Servizio Amazon	AWS::OpenSearch::Domain	Opensearch.1 Opensearch.2 Opensearch.3 Opensearch.4 Opensearch.5 Opensearch.6 Opensearch.7 Opensearch.8 Ricerca aperta. 9 Ricerca aperta.10 Ricerca aperta.11

Servizio	Risorsa richiesta	Controlli correlati
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster	<p>Documento DB.1</p> <p>Documento DB.2</p> <p>Documento DB.4</p> <p>Documento DB.5</p> <p>Nettuno.1</p> <p>Nettuno.2</p> <p>Nettuno.4</p> <p>Nettuno.5</p> <p>Nettuno.7</p> <p>Nettuno.8</p> <p>Nettuno.9</p> <p>RDS.7</p> <p>RDS.12</p> <p>RDS.14</p> <p>RDS.15</p> <p>RDS.16</p> <p>RDS.24</p> <p>RIF. 27</p> <p>RIF. 28</p> <p>RIF. 34</p> <p>RIF. 35</p>

Servizio	Risorsa richiesta	Controlli correlati
	AWS::RDS: :DBClusterSnapshot	Documento DB.3 Nettuno.3 Nettuno.6 RDS.1 RDS.4 RIF. 29
	AWS::RDS: :DBInstance	RDS.2 RDS.3 RDS.5 RDS.6 RDS.8 RDS.9 RDS.10 RDS.11 RDS.13 RDS.17 RDS.18 RDS.23 RDS.25 RIF. 30

Servizio	Risorsa richiesta	Controlli correlati
	AWS::RDS: :DBSecurityGroup	RIF. 31
	AWS::RDS: :DBSnapshot	Documento DB.3 RDS.1 RDS.4 RDS.32
	AWS::RDS: :DBSubnetGroup	RIF. 33
	AWS::RDS: :EventSubscription	RDS.19 RDS.20 RDS.21 RDS.22

Servizio	Risorsa richiesta	Controlli correlati
Amazon Redshift	AWS::Redshift::Cluster	Redshift.1
		Redshift.2
		Redshift.3
		Redshift.4
		Redshift.6
		Redshift.7
		Redshift.8
		Redshift.9
		Redshift.10
		Redshift.11
	AWS::Redshift::ClusterParameterGroup	Redshift.2
	AWS::Redshift::ClusterSnapshot	Redshift 13
	AWS::Redshift::ClusterSubnetGroup	Redshift 14
	AWS::Redshift::EventSubscription	Redshift 12

Servizio	Risorsa richiesta	Controlli correlati
Amazon Route 53	AWS::Route53::HostedZone	Percorso 53.2
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccessPoint	S3.19
	AWS::S3::Bucket	S3.2
		S3.3
		S3.5
		S3.6
		S3.7
		S3.8
		S3.9
		S3.10
		S3.11
		S3.12
		S3.13
		S3.14
		S3.15
S3.17		
S3.20		

Servizio	Risorsa richiesta	Controlli correlati
AWS Secrets Manager	AWS::SecretsManager::Secret	SecretsManager1. SecretsManager2. SecretsManager5.
AWS Service Catalog	AWS::ServiceCatalog::Portfolio	ServiceCatalog1.
Amazon Simple Email Service (Amazon SES)	AWS::SES::ConfigurationSet	VEDI.2
	AWS::SES::ContactList	VEDI.1
Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))	AWS::SNS::Topic	SNS.1 SNS.3
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue	SQS.1 MQ. 2
Amazon SageMaker	AWS::SageMaker::NotebookInstance	SageMaker2. SageMaker3.
AWS Step Functions	AWS::StepFunctions::StateMachine	StepFunctions.1. StepFunctions2.
AWS Transfer Family	AWS::Transfer::Workflow	Trasferimento.1

Servizio	Risorsa richiesta	Controlli correlati
AWS WAF	AWS::WAF::Rule	WAF.6
	AWS::WAF::RuleGroup	WAF.7
	AWS::WAF::WebACL	WAF.8
	AWS::WAFRegional::Rule	WAF.2
	AWS::WAFRegional::RuleGroup	WAF.3
	AWS::WAFRegional::WebACL	WAF.4
	AWS::WAFV2::RuleGroup	GUERRA 12
	AWS::WAFV2::WebACL	WAF.10

Risorse necessarie per lo standard FSBP

Affinché Security Hub riporti in modo accurato i risultati relativi ai controlli attivati da AWS Foundational Security Best Practices (FSBP) abilitati per modificare i controlli che utilizzano una AWS Config regola, è necessario registrare queste risorse in. AWS Config Per ulteriori informazioni su questo standard, vedere. [AWS Standard FSBP \(Foundational Security Best Practices\)](#)

Servizio	Risorse obbligatorie
Amazon API Gateway	AWS::ApiGateway::Stage

Servizio	Risorse obbligatorie
	AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
AWS CodeBuild	AWS::CodeBuild::Project
AWS Database Migration Service (AWS DMS)	AWS::DMS::Endpoint AWS::DMS::ReplicationInstance AWS::DMS::ReplicationTask
Amazon DynamoDB	AWS::DynamoDB::Table
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance AWS::SSM::ManagedInstanceInventory AWS::SSM::PatchCompliance

Servizio	Risorse obbligatorie
Amazon Elastic Compute Cloud (EC2)	<p>AWS::EC2::ClientVpnEndpoint</p> <p>AWS::EC2::Instance</p> <p>AWS::EC2::LaunchTemplate</p> <p>AWS::EC2::NetworkAcl</p> <p>AWS::EC2::NetworkInterface</p> <p>AWS::EC2::SecurityGroup</p> <p>AWS::EC2::Subnet</p> <p>AWS::EC2::TransitGateway</p> <p>AWS::EC2::VPNConnection</p> <p>AWS::EC2::Volume</p>
Dimensionamento automatico Amazon EC2	<p>AWS::AutoScaling::AutoScalingGroup</p> <p>AWS::AutoScaling::LaunchConfiguration</p>
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	<p>AWS::ECS::Cluster</p> <p>AWS::ECS::Service</p> <p>AWS::ECS::TaskDefinition</p>
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint
Amazon EKS	AWS::EKS::Cluster

Servizio	Risorse obbligatorie
ElasticBeanstalk	AWS::ElasticBeanstalk::Environment
Sistema di bilanciamento del carico elastico	AWS::ElasticLoadBalancing::LoadBalancer AWS::ElasticLoadBalancingV2::LoadBalancer
ElasticSearch	AWS::Elasticsearch::Domain
Amazon FSx	AWS::FSx::FileSystem
AWS Identity and Access Management (IAM)	AWS::IAM::Group AWS::IAM::Policy AWS::IAM::Role AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Key
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
MSK Amazon	AWS::MSK::Cluster
AWS Network Firewall	AWS::NetworkFirewall::Firewall AWS::NetworkFirewall::FirewallPolicy AWS::NetworkFirewall::RuleGroup
OpenSearch Servizio Amazon	AWS::OpenSearch::Domain

Servizio	Risorse obbligatorie
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster AWS::RDS::DBClusterSnapshot AWS::RDS::DBInstance AWS::RDS::DBSnapshot AWS::RDS::EventSubscription
Amazon Redshift	AWS::Redshift::Cluster
Amazon Route 53	AWS::Route53::HostedZone
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccessPoint AWS::S3::Bucket
Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue
Amazon SageMaker	AWS::SageMaker::NotebookInstance
AWS Secrets Manager	AWS::SecretsManager::Secret
AWS Step Functions	AWS::StepFunctions::StateMachine

Servizio	Risorse obbligatorie
AWS WAF	AWS::WAF::Rule
	AWS::WAF::RuleGroup
	AWS::WAF::WebACL
	AWS::WAFRegional::Rule
	AWS::WAFRegional::RuleGroup
	AWS::WAFRegional::WebACL
	AWS::WAFv2::RuleGroup
	AWS::WAFv2::WebACL

Risorse necessarie per CIS AWS Foundations Benchmark

Per eseguire controlli di sicurezza per i controlli abilitati che si applicano al benchmark Center for Internet Security (CIS) AWS Foundations, Security Hub esegue le esatte fasi di controllo prescritte per i controlli in [Securing Amazon Web Services](#) o utilizza regole gestite specifiche AWS Config .

Per ulteriori informazioni su questo standard, consulta. [CIS AWS Foundations Benchmark](#)

Risorse necessarie per CIS v3.0.0

Affinché Security Hub riporti in modo accurato i risultati dei controlli attivati da modifiche CIS v3.0.0 abilitati che utilizzano una AWS Config regola, è necessario registrare queste risorse in. AWS Config

Servizio	Risorse obbligatorie
Amazon Elastic Compute Cloud (Amazon EC2)	AWS::EC2::Instance
	AWS::EC2::NetworkAcl
	AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Group

Servizio	Risorse obbligatorie
	AWS::IAM::User
	AWS::IAM::Role
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBInstance
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket

Risorse necessarie per CIS v1.4.0

Affinché Security Hub riporti in modo accurato i risultati dei controlli attivati da modifiche CIS v1.4.0 abilitati che utilizzano una AWS Config regola, è necessario registrare queste risorse in. AWS Config

Servizio	Risorse obbligatorie
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::NetworkAcl
	AWS::EC2::SecurityGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy
	AWS::IAM::User
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBInstance
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket

Risorse necessarie per CIS v1.2.0

Affinché Security Hub riporti in modo accurato i risultati dei controlli attivati da modifiche CIS v1.2.0 abilitati che utilizzano una AWS Config regola, è necessario registrare queste risorse in. AWS Config

Servizio	Risorse obbligatorie
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::SecurityGroup

Servizio	Risorse obbligatorie
AWS Identity and Access Management (IAM)	AWS::IAM::Policy
	AWS::IAM::User

Risorse necessarie per NIST SP 800-53 Rev. 5

Affinché Security Hub riporti in modo accurato i risultati per i controlli attivati dal National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 abilitati alla modifica che utilizzano una AWS Config regola, è necessario registrare queste risorse in AWS Config. È necessario registrare solo le risorse per i controlli che hanno attivato un tipo di modifica della pianificazione. Per ulteriori informazioni su questo standard, vedere [Istituto nazionale di standard e tecnologia \(NIST\) SP 800-53 Rev. 5](#).

Servizio	Risorse obbligatorie
Amazon API Gateway	AWS::ApiGateway::Stage
	AWS::ApiGatewayV2::Stage
AWS AppSync	AWS::AppSync::GraphQLApi
AWS Backup	AWS::Backup::RecoveryPoint
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
Amazon CloudWatch	AWS::CloudWatch::Alarm
AWS CodeBuild	AWS::CodeBuild::Project
AWS Database Migration Service (AWS DMS)	AWS::DMS::Endpoint
	AWS::DMS::ReplicationInstance
	AWS::DMS::ReplicationTask

Servizio	Risorse obbligatorie
Amazon DynamoDB	AWS::DynamoDB::Table
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::ClientVpnEndpoint AWS::EC2::EIP AWS::EC2::Instance AWS::EC2::LaunchTemplate AWS::EC2::NetworkAcl AWS::EC2::NetworkInterface AWS::EC2::SecurityGroup AWS::EC2::Subnet AWS::EC2::TransitGateway AWS::EC2::VPNConnection AWS::EC2::Volume
Dimensionamento automatico Amazon EC2	AWS::AutoScaling::AutoScalingGroup AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster AWS::ECS::Service AWS::ECS::TaskDefinition
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint

Servizio	Risorse obbligatorie
Amazon EKS	<code>AWS::EKS::Cluster</code>
ElasticBeanstalk	<code>AWS::ElasticBeanstalk::Environment</code>
Sistema di bilanciamento del carico elastico	<code>AWS::ElasticLoadBalancing::LoadBalancer</code> <code>AWS::ElasticLoadBalancingV2::LoadBalancer</code>
ElasticSearch	<code>AWS::Elasticsearch::Domain</code>
Amazon EventBridge	<code>AWS::Events::Endpoint</code> <code>AWS::Events::EventBus</code>
Amazon FSx	<code>AWS::FSx::FileSystem</code>
AWS Identity and Access Management (IAM)	<code>AWS::IAM::Group</code> <code>AWS::IAM::Policy</code> <code>AWS::IAM::Role</code> <code>AWS::IAM::User</code>
AWS Key Management Service (AWS KMS)	<code>AWS::KMS::Key</code>
Amazon Kinesis	<code>AWS::Kinesis::Stream</code>
AWS Lambda	<code>AWS::Lambda::Function</code>
MSK Amazon	<code>AWS::MSK::Cluster</code>
Amazon MQ	<code>AWS::AmazonMQ::Broker</code>

Servizio	Risorse obbligatorie
AWS Network Firewall	AWS::NetworkFirewall::Firewall AWS::NetworkFirewall::FirewallPolicy AWS::NetworkFirewall::RuleGroup
OpenSearch Servizio Amazon	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster AWS::RDS::DBClusterSnapshot AWS::RDS::DBInstance AWS::RDS::DBSnapshot AWS::RDS::EventSubscription
Amazon Redshift	AWS::Redshift::Cluster
Amazon Route 53	AWS::Route53::HostedZone
Amazon Simple Storage Service (Amazon S3)	AWS::S3::AccessPoint AWS::S3::Bucket
AWS Service Catalog	AWS::ServiceCatalog::Portfolio
Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance AWS::SSM::ManagedInstanceInventory AWS::SSM::PatchCompliance

Servizio	Risorse obbligatorie
Amazon SageMaker	AWS::SageMaker::NotebookInstance
AWS Secrets Manager	AWS::SecretsManager::Secret
AWS WAF	AWS::WAF::Rule AWS::WAF::RuleGroup AWS::WAF::WebACL AWS::WAFRegional::Rule AWS::WAFRegional::RuleGroup AWS::WAFRegional::WebACL AWS::WAFv2::RuleGroup AWS::WAFv2::WebACL

Risorse richieste per PCI DSS v3.2.1

Affinché Security Hub riporti in modo accurato i risultati dei controlli PCI DSS (Payment Card Industry Data Security Standard) abilitati che utilizzano una AWS Config regola, è necessario registrare queste risorse in. AWS Config Per ulteriori informazioni su questo standard, vedere. [Payment Card Industry Data Security Standard \(PCI DSS\)](#)

Servizio	Risorse obbligatorie
AWS CodeBuild	AWS::CodeBuild::Project
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::EIP AWS::EC2::Instance AWS::EC2::SecurityGroup

Servizio	Risorse obbligatorie
Dimensionamento automatico Amazon EC2	AWS::AutoScaling::AutoScalingGroup
AWS Identity and Access Management (IAM)	AWS::IAM::Policy AWS::IAM::User
AWS Lambda	AWS::Lambda::Function
OpenSearch Servizio Amazon	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBClusterSnapshot AWS::RDS::DBInstance AWS::RDS::DBSnapshot
Amazon Redshift	AWS::Redshift::Cluster
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance AWS::SSM::ManagedInstanceInventory AWS::SSM::PatchCompliance

Risorse necessarie per AWS Resource Tagging Standard

Tutti i controlli del AWS Resource Tagging Standard attivano modifiche e utilizzano una regola. AWS Config Affinché Security Hub riporti in modo accurato i risultati di questi controlli, è necessario registrare le seguenti risorse in AWS Config. È necessario registrare le risorse solo per i controlli che hanno attivato un tipo di modifica della pianificazione. Per ulteriori informazioni su questo standard, vedere [AWS Standard di etichettatura delle risorse](#).

Servizio	Risorse obbligatorie
AWS Certificate Manager (ACM)	AWS::ACM::Certificate
AWS AppSync	AWS::AppSync::GraphQLApi
Dimensionamento automatico Amazon EC2	AWS::AutoScaling::AutoScalingGroup
Amazon Athena	AWS::Athena::DataCatalog AWS::Athena::WorkGroup
Dimensionamento automatico Amazon EC2	AWS::AutoScaling::AutoScalingGroup
AWS CloudFormation	AWS::CloudFormation::Stack
Amazon CloudFront	AWS::CloudFront::Distribution
AWS CloudTrail	AWS::CloudTrail::Trail
AWS CodeArtifact	AWS::CodeArtifact::Repository
Amazon Detective	AWS::Detective::Graph
AWS Database Migration Service (AWS DMS)	AWS::DMS::Certificate AWS::DMS::EventSubscription AWS::DMS::ReplicationInstance AWS::DMS::ReplicationSubnetGroup
Amazon DynamoDB	AWS::DynamoDB::Trail
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::CustomerGateway AWS::EC2::EIP AWS::EC2::FlowLog

Servizio	Risorse obbligatorie
	AWS::EC2::Instance AWS::EC2::InternetGateway AWS::EC2::NatGateway AWS::EC2::NetworkAcl AWS::EC2::NetworkInterface AWS::EC2::RouteTable AWS::EC2::SecurityGroup AWS::EC2::Subnet AWS::EC2::TransitGateway AWS::EC2::TransitGatewayAttachment AWS::EC2::TransitGatewayRouteTable AWS::EC2::Volume AWS::EC2::VPC AWS::EC2::VPCEndpointService AWS::EC2::VPCPeeringConnector AWS::EC2::VPNGateway
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::PublicRepository

Servizio	Risorse obbligatorie
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster AWS::ECS::Service AWS::ECS::TaskDefinition
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint
Amazon Elastic Kubernetes Service (Amazon EKS)	AWS::EKS::Cluster AWS::EKS::IdentityProviderConfig
AWS Elastic Beanstalk (Elastic Beanstalk)	AWS::ElasticBeanstalk::Environment
ElasticSearch	AWS::Elasticsearch::Domain
Amazon EventBridge	AWS::Events::EventBus
AWS Global Accelerator	AWS::GlobalAccelerator::Accelerator
AWS Glue	AWS::Glue::Job
Amazon GuardDuty	AWS::GuardDuty::Detector AWS::GuardDuty::Filter AWS::GuardDuty::IPSet
AWS Identity and Access Management (IAM)	AWS::IAM::Role AWS::IAM::User
AWS Identity and Access Management Access Analyzer (Analizzatore di accesso IAM)	AWS::AccessAnalyzer::Analyzer

Servizio	Risorse obbligatorie
AWS IoT	AWS::IoT::Authorizer AWS::IoT::Dimension AWS::IoT::MitigationAction AWS::IoT::Policy AWS::IoT::RoleAlias AWS::IoT::SecurityProfile
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
Amazon MQ	AWS::AmazonMQ::Broker
AWS Network Firewall	AWS::NetworkFirewall::Firewall AWS::NetworkFirewall::FirewallPolicy
OpenSearch Servizio Amazon	AWS::OpenSearch::Domain
Amazon Relational Database Service	AWS::RDS::DBCluster AWS::RDS::DBClusterSnapshot AWS::RDS::DBInstance AWS::RDS::DBSecurityGroup AWS::RDS::DBSnapshot AWS::RDS::DBSubnetGroup

Servizio	Risorse obbligatorie
Amazon Redshift	AWS::Redshift::Cluster AWS::Redshift::ClusterSnapshot AWS::Redshift::ClusterSubnetGroup AWS::Redshift::EventSubscription
AWS Secrets Manager	AWS::SecretsManager::Secret
Amazon Simple Email Service (Amazon SES)	AWS::SES::ConfigurationSet AWS::SES::ContactList
Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue
AWS Step Functions	AWS::StepFunctions::Activity
AWS Transfer Family	AWS::Transfer::Workflow

Risorse richieste per Service-Managed Standard: AWS Control Tower

Affinché Security Hub riporti in modo accurato i risultati per Service-Managed Standard abilitato: AWS Control Tower modifica i controlli attivati che utilizzano una AWS Config regola, è necessario registrare le seguenti risorse in. AWS Config Per ulteriori informazioni su questo standard, vedere. [Standard di gestione dei servizi: AWS Control Tower](#)

Servizio	Risorse obbligatorie
Amazon API Gateway	AWS::ApiGateway::Stage AWS::ApiGatewayV2::Stage
AWS Certificate Manager (ACM)	AWS::ACM::Certificate

Servizio	Risorse obbligatorie
AWS CodeBuild	AWS::CodeBuild::Project
Amazon DynamoDB	AWS::DynamoDB::Table
Amazon Elastic Compute Cloud (EC2)	AWS::EC2::Instance AWS::EC2::NetworkAcl AWS::EC2::NetworkInterface AWS::EC2::SecurityGroup AWS::EC2::Subnet AWS::EC2::VPNConnection AWS::EC2::Volume
Dimensionamento automatico Amazon EC2	AWS::AutoScaling::AutoScalingGroup AWS::AutoScaling::LaunchConfiguration
Amazon Elastic Container Registry (Amazon ECR)	AWS::ECR::Repository
Amazon Elastic Container Service (Amazon ECS)	AWS::ECS::Cluster AWS::ECS::Service AWS::ECS::TaskDefinition
Amazon Elastic File System (Amazon EFS)	AWS::EFS::AccessPoint
Amazon EKS	AWS::EKS::Cluster
ElasticBeanstalk	AWS::ElasticBeanstalk::Environment

Servizio	Risorse obbligatorie
Sistema di bilanciamento del carico elastico	AWS::ElasticLoadBalancing::LoadBalancer AWS::ElasticLoadBalancingV2::LoadBalancer
ElasticSearch	AWS::Elasticsearch::Domain
AWS Identity and Access Management (IAM)	AWS::IAM::Group AWS::IAM::Policy AWS::IAM::Role AWS::IAM::User
AWS Key Management Service (AWS KMS)	AWS::KMS::Key
Amazon Kinesis	AWS::Kinesis::Stream
AWS Lambda	AWS::Lambda::Function
AWS Network Firewall	AWS::NetworkFirewall::FirewallPolicy AWS::NetworkFirewall::RuleGroup
OpenSearch Servizio Amazon	AWS::OpenSearch::Domain
Amazon Relational Database Service (Amazon RDS)	AWS::RDS::DBCluster AWS::RDS::DBClusterSnapshot AWS::RDS::DBInstance AWS::RDS::DBSnapshot AWS::RDS::EventSubscription
Amazon Redshift	AWS::Redshift::Cluster

Servizio	Risorse obbligatorie
Amazon Simple Storage Service (Amazon S3)	AWS::S3::Bucket
Servizio di notifica semplice Amazon (Amazon Simple Notification Service (Amazon SNS))	AWS::SNS::Topic
Amazon Simple Queue Service (Amazon SQS)	AWS::SQS::Queue
Amazon EC2 Systems Manager (SSM)	AWS::SSM::AssociationCompliance AWS::SSM::ManagedInstanceInventory AWS::SSM::PatchCompliance
AWS Secrets Manager	AWS::SecretsManager::Secret
AWS WAF	AWS::WAFRegional::Rule AWS::WAFRegional::RuleGroup AWS::WAFRegional::WebACL AWS::WAFv2::WebACL

Pianificazione dell'esecuzione dei controlli di sicurezza

Dopo aver abilitato uno standard di sicurezza, AWS Security Hub inizia a eseguire tutti i controlli entro due ore. La maggior parte dei controlli inizia entro 25 minuti. Security Hub esegue i controlli valutando la regola alla base di un controllo. Fino a quando un controllo non completa la prima esecuzione dei controlli, lo stato è Nessun dato.

Quando abiliti un nuovo standard, Security Hub può impiegare fino a 24 ore per generare risultati per i controlli che utilizzano la stessa regola sottostante AWS Config collegata ai servizi dei controlli abilitati di altri standard abilitati. Ad esempio, se abiliti [Lambda.1](#) nello standard AWS Foundational Security Best Practices (FSBP), Security Hub creerà la regola collegata al servizio e in genere genererà i risultati in pochi minuti. Dopodiché, se abiliti Lambda.1 nel Payment Card Industry Data

Security Standard (PCI DSS), Security Hub potrebbe impiegare fino a 24 ore per generare i risultati per questo controllo perché utilizza la stessa regola collegata ai servizi di Lambda.1.

Dopo il controllo iniziale, la pianificazione di ogni controllo può essere periodica o attivata a modifiche.

- **Controlli periodici:** questi controlli vengono eseguiti automaticamente entro 12 o 24 ore dall'esecuzione più recente. Security Hub determina la periodicità e non è possibile modificarla. I controlli periodici riflettono una valutazione al momento dell'esecuzione del controllo. Se si aggiorna lo stato del flusso di lavoro di un risultato di controllo periodico e quindi nel controllo successivo lo stato di conformità del risultato rimane lo stesso, lo stato del flusso di lavoro rimane modificato. Ad esempio, se hai una ricerca non riuscita per KMS.4, la AWS KMS key rotazione deve essere abilitata e quindi correggere il risultato, Security Hub modifica lo stato del flusso di lavoro da a. NEW RESOLVED Se disabiliti la rotazione delle chiavi KMS prima del successivo controllo periodico, lo stato del flusso di lavoro del risultato rimane invariato. RESOLVED
- **Controlli attivati da modifiche:** questi controlli vengono eseguiti quando la risorsa associata cambia stato. AWS Config consente di scegliere tra la registrazione continua delle modifiche allo stato delle risorse e la registrazione giornaliera. Se si sceglie la registrazione giornaliera, AWS Config fornisce i dati di configurazione delle risorse alla fine di ogni periodo di 24 ore in caso di cambiamenti nello stato delle risorse. Se non ci sono modifiche, non viene fornito alcun dato. Ciò può ritardare la generazione dei risultati del Security Hub fino al completamento di un periodo di 24 ore. Indipendentemente dal periodo di registrazione scelto, Security Hub verifica ogni 18 ore per assicurarsi che non sia AWS Config stato perso alcun aggiornamento delle risorse.

In generale, Security Hub utilizza regole modificate quando possibile. Affinché una risorsa utilizzi una regola attivata da una modifica, deve supportare AWS Config gli elementi di configurazione.

Per un controllo basato su una AWS Config regola gestita, la descrizione del controllo include un collegamento alla descrizione della regola nella Guida per gli AWS Config sviluppatori. Tale descrizione include se la regola è soggetta a modifiche o è periodica.

I controlli che utilizzano le funzioni Lambda personalizzate di Security Hub sono periodici.

Generazione e aggiornamento dei risultati del controllo

AWS Security Hub genera risultati eseguendo controlli rispetto ai controlli di sicurezza. Questi risultati utilizzano il AWS Security Finding Format (ASFF). Si noti che se la dimensione del risultato supera il massimo di 240 KB, l'`Resource.Details` soggetto viene rimosso. Per i controlli supportati da AWS Config risorse, è possibile visualizzare i dettagli delle risorse sulla AWS Config console.

Security Hub normalmente addebita un costo per ogni controllo di sicurezza. Tuttavia, se più controlli utilizzano la stessa AWS Config regola, Security Hub addebita una sola volta per ogni controllo rispetto alla AWS Config regola. Se attivi [i risultati del controllo consolidato](#), Security Hub genera un singolo risultato per un controllo di sicurezza anche quando il controllo è incluso in più standard abilitati.

Ad esempio, la AWS Config regola `iam-password-policy` viene utilizzata da più controlli nello standard Center for Internet Security (CIS) AWS Foundations Benchmark e nello standard Foundational Security Best Practices. Ogni volta che Security Hub esegue un controllo rispetto a tale AWS Config regola, genera un risultato separato per ogni controllo correlato, ma addebita una sola volta per il controllo.

Risultati di controllo consolidati

Quando i risultati del controllo consolidato sono attivati nel tuo account, Security Hub genera un singolo nuovo risultato o aggiornamento dei risultati per ogni controllo di sicurezza di un controllo, anche se un controllo si applica a più standard abilitati. Per visualizzare un elenco dei controlli e degli standard a cui si applicano, consulta [Riferimento ai controlli del Security Hub](#). È possibile attivare o disattivare i risultati del controllo consolidato. Ti consigliamo di accenderlo per ridurre il rumore di rilevamento.

Se hai abilitato Security Hub Account AWS prima del 23 febbraio 2023, devi attivare i risultati del controllo consolidato seguendo le istruzioni riportate più avanti in questa sezione. Se attivi Security Hub a partire dal 23 febbraio 2023, i risultati del controllo consolidato vengono automaticamente attivati nel tuo account. Tuttavia, se utilizzi [l'integrazione di Security Hub con AWS Organizations](#) o gli account dei membri invitati tramite una [procedura di invito manuale](#), i risultati del controllo consolidato vengono attivati negli account dei membri solo se sono attivati nell'account amministratore. Se la funzionalità è disattivata nell'account amministratore, è disattivata negli account dei membri. Questo comportamento si applica agli account membro nuovi ed esistenti.

Se disattivi i risultati del controllo consolidato nel tuo account, Security Hub genera un risultato separato per ogni controllo di sicurezza per ogni standard abilitato che include un controllo. Ad esempio, se quattro standard abilitati condividono un controllo con la stessa AWS Config regola sottostante, riceverai quattro risultati separati dopo un controllo di sicurezza del controllo. Se attivi i risultati del controllo consolidato, riceverai solo un risultato. Per ulteriori informazioni su come il consolidamento influisce sui risultati, consulta [Esempi di risultati del controllo](#)

Quando attivi i risultati del controllo consolidato, Security Hub crea nuovi risultati indipendenti dagli standard e archivia i risultati originali basati sugli standard. Alcuni campi e valori di ricerca dei controlli

cambieranno e potrebbero influire sui flussi di lavoro esistenti. Per ulteriori informazioni su queste modifiche, vedi [Risultati di controllo consolidati: modifiche ASFF](#).

L'attivazione dei risultati del controllo consolidato può influire anche sui risultati che le [integrazioni di terze parti](#) ricevono da Security Hub. [Automated Security Response nella versione AWS 2.0.0 supporta](#) risultati di controllo consolidati.

Attivazione dei risultati del controllo consolidato

Per attivare i risultati del controllo consolidato, è necessario accedere a un account amministratore o a un account autonomo.

Note

Dopo aver attivato i risultati del controllo consolidato, Security Hub potrebbe impiegare fino a 24 ore per generare nuovi risultati consolidati e archiviare i risultati originali basati su standard. Durante questo periodo, nel tuo account potresti visualizzare una combinazione di risultati indipendenti dagli standard e basati sugli standard.

Security Hub console

1. [Apri la console all'indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/). [AWS Security Hub](#)
2. Nel pannello di navigazione scegli Impostazioni.
3. Scegli la scheda Generale.
4. Per Controlli, attiva i risultati del controllo consolidato.
5. Selezionare Salva.

Security Hub API

1. Esegui [UpdateSecurityHubConfiguration](#).
2. Imposta `ControlFindingGenerator` uguale a `SECURITY_CONTROL`

Richiesta di esempio:

```
{
  "ControlFindingGenerator": "SECURITY_CONTROL"
}
```


AWS CLI

1. Esegui il comando [update-security-hub-configuration](#).
2. Imposta `control-finding-generator` uguale a `SECURITY_CONTROL`.

```
aws securityhub --region us-east-1 update-security-hub-configuration --control-finding-generator SECURITY_CONTROL
```

Disattivazione dei risultati del controllo consolidato

Per disattivare i risultati del controllo consolidato, è necessario accedere a un account amministratore o a un account autonomo.

Note

Dopo aver disattivato i risultati del controllo consolidato, Security Hub potrebbe impiegare fino a 24 ore per generare nuovi risultati basati su standard e archiviare i risultati consolidati. Durante questo periodo, potresti visualizzare un mix di risultati basati su standard e consolidati nel tuo account.

Security Hub console

1. [Apri la AWS Security Hub console all'indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel pannello di navigazione scegli Impostazioni.
3. Scegli la scheda Generale.
4. Per Controlli, scegli Modifica e disattiva i risultati del controllo consolidato.
5. Selezionare Salva.

Security Hub API

1. Esegui [UpdateSecurityHubConfiguration](#).
2. Imposta `ControlFindingGenerator` uguale a `STANDARD_CONTROL`.

Richiesta di esempio:

```
{
```

```
"ControlFindingGenerator": "STANDARD_CONTROL"  
}
```

AWS CLI

1. Esegui il comando [update-security-hub-configuration](#).
2. Imposta `control-finding-generator` uguale a `STANDARD_CONTROL`.

```
aws securityhub --region us-east-1 update-security-hub-configuration --control-  
finding-generator STANDARD_CONTROL
```

Compliance

dettagli relativi ai risultati del controllo

Per quanto riguarda i risultati generati dai controlli di sicurezza, il [Compliance](#) campo del AWS Security Finding Format (ASFF) contiene dettagli relativi ai risultati dei controlli. Il campo [Compliance](#) include le seguenti informazioni:

AssociatedStandards

Gli standard abilitati in cui è abilitato un controllo.

RelatedRequirements

L'elenco dei requisiti correlati per il controllo in tutti gli standard abilitati. I requisiti provengono dal framework di sicurezza di terze parti per il controllo, come il Payment Card Industry Data Security Standard (PCI DSS).

SecurityControlId

L'identificatore per il controllo degli standard di sicurezza supportati da Security Hub.

Status

Il risultato del controllo più recente eseguito da Security Hub per un determinato controllo. I risultati dei controlli precedenti vengono conservati in un stato archiviato per 90 giorni.

StatusReasons

Contiene un elenco di motivi del valore di `Compliance.Status`. Per ogni motivo, `StatusReasons` include il codice motivo e una descrizione.

La tabella seguente elenca i codici e le descrizioni dei motivi dello stato disponibili. Le fasi di correzione dipendono dal controllo che ha generato un risultato con il codice motivo. Scegli un controllo tra i seguenti [Riferimento ai controlli del Security Hub](#) per visualizzare i passaggi di riparazione relativi a quel controllo.

Codice di motivo	Compliance Status	Descrizione
CLOUDTRAIL_METRIC_FILTER_NOT_VALID	FAILED	Il CloudTrail percorso multiregionale non dispone di un filtro metrico valido.
CLOUDTRAIL_METRIC_FILTERS_NOT_PRESENT	FAILED	I filtri metrici non sono presenti per il percorso multiregionale. CloudTrail
CLOUDTRAIL_MULTIREGION_NOT_PRESENT	FAILED	L'account non dispone di un CloudTrail percorso multiregionale con la configurazione richiesta.
CLOUDTRAIL_REGION_INVALID	WARNING	I CloudTrail percorsi multiregione non si trovano nella regione attuale.
CLOUDWATCH_ALARM_ACTIONS_NOT_VALID	FAILED	Non sono presenti operazioni di allarme valide.
CLOUDWATCH_ALARMS_NOT_PRESENT	FAILED	CloudWatch gli allarmi non esistono nell'account.
CONFIG_ACCESS_DENIED	NOT_AVAILABLE AWS Config lo stato è ConfigError	AWS Config accesso negato. Verifica che AWS Config sia abilitato e che siano state concesse autorizzazioni sufficienti.
CONFIG_EVALUATIONS_EMPTY	PASSED	AWS Config ha valutato le tue risorse in base alla regola.

Codice di motivo	Compliance Status	Descrizione
		La regola non si applicava alle AWS risorse incluse nel suo ambito, le risorse specificate sono state eliminate o i risultati della valutazione sono stati eliminati.
CONFIG_RETURNS_NOT_APPLICABLE	NOT_AVAILABLE	<p>Lo stato di conformità è NOT_AVAILABLE dovuto al fatto che è stato AWS Config restituito lo stato Non applicabile.</p> <p>AWS Config non fornisce il motivo dello stato. Di seguito sono riportati alcuni possibili motivi dello stato Non applicabile:</p> <ul style="list-style-type: none"> • La risorsa è stata rimossa dall'ambito della AWS Config regola. • La AWS Config regola è stata eliminata. • La risorsa è stata eliminata. • La logica della AWS Config regola può generare lo stato Non applicabile.

Codice di motivo	Compliance Status	Descrizione
CONFIG_RULE_EVALUATION_ERROR	NOT_AVAILABLE AWS Config lo stato è ConfigError	<p>Questo codice motivo viene utilizzato per diversi tipi di errori di valutazione.</p> <p>La descrizione fornisce le informazioni sul motivo specifico.</p> <p>Il tipo di errore può essere uno dei seguenti:</p> <ul style="list-style-type: none"> • Impossibilità di eseguire la valutazione a causa della mancanza di autorizzazioni. La descrizione fornisce l'autorizzazione specifica mancante. • Valore mancante o non valido per un parametro. La descrizione fornisce il parametro e i requisiti per il valore del parametro. • Errore durante la lettura di un bucket S3. La descrizione identifica il bucket e fornisce l'errore specifico. • Un AWS abbonamento mancante. • Timeout generale sulla valutazione. • Un account sospeso.
CONFIG_RULE_NOT_FOUND	NOT_AVAILABLE AWS Config lo stato è ConfigError	<p>La AWS Config regola è in fase di creazione.</p>

Codice di motivo	Compliance Status	Descrizione
INTERNAL_SERVICE_ERROR	NOT_AVAILABLE	Si è verificato un errore sconosciuto.
LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE	Non riuscito	Security Hub non è in grado di eseguire un controllo rispetto a un runtime Lambda personalizzato.
S3_BUCKET_CROSS_ACCOUNT_CROSS_REGION	WARNING	<p>Il risultato è in uno WARNING stato, perché il bucket S3 associato a questa regola si trova in una regione o in un account diverso.</p> <p>Questa regola non supporta controlli tra regioni o account.</p> <p>È consigliabile disabilitare questo controllo in questa regione o account. Esegui solo nella regione o nell'account in cui si trova la risorsa.</p>
SNS_SUBSCRIPTION_NOT_PRESENT	FAILED	I filtri metrici CloudWatch Logs non dispongono di un abbonamento Amazon SNS valido.

Codice di motivo	Compliance Status	Descrizione
SNS_TOPIC_CROSS_ACCOUNT	WARNING	<p>Il risultato è in uno stato. WARNING</p> <p>L'argomento SNS associato a questa regola è di proprietà di un account diverso. L'account corrente non è in grado di ottenere le informazioni sull'abbonamento.</p> <p>L'account proprietario dell'argomento SNS deve concedere all'account corrente l'<code>sns:ListSubscriptionsByTopic</code> autorizzazione per l'argomento SNS.</p>
SNS_TOPIC_CROSS_ACCOUNT_CROSS_REGION	WARNING	<p>Il risultato è in uno WARNING stato in cui l'argomento SNS associato a questa regola si trova in una regione o in un account diverso.</p> <p>Questa regola non supporta controlli tra regioni o account.</p> <p>È consigliabile disabilitare questo controllo in questa regione o account. Esegui solo nella regione o nell'account in cui si trova la risorsa.</p>
SNS_TOPIC_INVALID	FAILED	L'argomento SNS associato a questa regola non è valido.
THROTTLING_ERROR	NOT_AVAILABLE	L'operazione API pertinente ha superato il limite consentito.

ProductFields dettagli relativi ai risultati del controllo

Quando Security Hub esegue controlli di sicurezza e genera risultati di controllo, l'`ProductFields` attributo in ASFF include i seguenti campi:

`ArchivalReasons:0/Description`

Descrive perché Security Hub ha archiviato i risultati esistenti.

Ad esempio, Security Hub archivia i risultati esistenti quando si disattiva un controllo o uno standard e quando si attivano o disattivano [i risultati del controllo consolidato](#).

`ArchivalReasons:0/ReasonCode`

Fornisce il motivo per cui Security Hub ha archiviato i risultati esistenti.

Ad esempio, Security Hub archivia i risultati esistenti quando si disattiva un controllo o uno standard e quando si attivano o disattivano [i risultati del controllo consolidato](#).

`StandardsGuideArn` o `StandardsArn`

L'ARN dello standard associato al controllo.

Per lo standard CIS AWS Foundations Benchmark, il campo è `StandardsGuideArn`

Per gli standard PCI DSS e AWS Foundational Security Best Practices, il campo è `StandardsArn`

Questi campi vengono rimossi a favore di `Compliance.AssociatedStandards` se si attivano i risultati di controllo [consolidati](#).

`StandardsGuideSubscriptionArn` o `StandardsSubscriptionArn`

L'ARN dell'abbonamento dell'account allo standard.

Per lo standard CIS AWS Foundations Benchmark, il campo è `StandardsGuideSubscriptionArn`

Per gli standard PCI DSS e AWS Foundational Security Best Practices, il campo è `StandardsSubscriptionArn`

Questi campi vengono rimossi se si attivano i risultati del controllo [consolidato](#).

`RuleId` o `ControlId`

L'identificatore del controllo.

Per lo standard CIS AWS Foundations Benchmark, il campo è `RuleId`

Per altri standard, il campo è `ControlId`

Questi campi vengono rimossi a favore di `Compliance.SecurityControlId` se si attivano i [risultati di controllo consolidati](#).

`RecommendationUrl`

L'URL delle informazioni di riparazione per il controllo. Questo campo viene rimosso a favore di `Remediation.Recommendation.Url` se si attivano i risultati del [controllo consolidato](#).

`RelatedAWSResources:0/name`

Il nome della risorsa associata al risultato.

`RelatedAWSResource:0/type`

Il tipo di risorsa associata al controllo.

`StandardsControlArn`

L'ARN del controllo. Questo campo viene rimosso se si attivano i [risultati del controllo consolidato](#).

`aws/securityhub/ProductName`

Per i risultati basati sul controllo, il nome del prodotto è Security Hub.

`aws/securityhub/CompanyName`

Per i risultati basati sul controllo, il nome dell'azienda è AWS

`aws/securityhub/annotation`

Una descrizione del problema rilevato dal controllo.

`aws/securityhub/FindingId`

L'identificatore del risultato. Questo campo non fa riferimento a uno standard se si attivano i risultati del [controllo consolidato](#).

Assegnazione della gravità ai risultati del controllo

La severità assegnata a un controllo Security Hub identifica l'importanza del controllo. La gravità di un controllo determina l'etichetta di gravità assegnata ai risultati del controllo.

Criteri di gravità

La gravità di un controllo è determinata sulla base di una valutazione dei seguenti criteri:

- Quanto è difficile per un autore di minacce sfruttare la debolezza della configurazione associata al controllo?

La difficoltà è determinata dal livello di sofisticazione o complessità necessario per utilizzare la vulnerabilità per realizzare uno scenario di minaccia.

- Quanto è probabile che la debolezza porti a una compromissione delle vostre Account AWS o delle vostre risorse?

Una compromissione delle vostre Account AWS risorse significa che la riservatezza, l'integrità o la disponibilità dei dati o dell' AWS infrastruttura vengono danneggiate in qualche modo.

La probabilità di compromissione indica la probabilità che lo scenario di minaccia comporti un'interruzione o una violazione dei AWS servizi o delle risorse.

Ad esempio, considera i seguenti punti deboli della configurazione:

- Le chiavi di accesso utente non vengono ruotate ogni 90 giorni.
- La chiave utente root IAM esiste.

Entrambi i punti deboli sono ugualmente difficili da sfruttare per un avversario. In entrambi i casi, l'avversario può utilizzare il furto di credenziali o qualche altro metodo per acquisire una chiave utente. Possono quindi utilizzarlo per accedere alle tue risorse in modo non autorizzato.

Tuttavia, la probabilità di una compromissione è molto più elevata se l'autore della minaccia acquisisce la chiave di accesso dell'utente root, in quanto ciò gli offre un accesso maggiore. Di conseguenza, la vulnerabilità della chiave dell'utente root ha una gravità maggiore.

La gravità non tiene conto della criticità della risorsa sottostante. La criticità è il livello di importanza delle risorse associate alla scoperta. Ad esempio, una risorsa associata a un'applicazione mission critical è più importante di una associata a test non di produzione. Per acquisire informazioni sulla criticità delle risorse, utilizzate il `Criticality` campo del AWS Security Finding Format (ASFF).

La tabella seguente associa la difficoltà di sfruttamento e la probabilità di compromissione alle etichette di sicurezza.

	Un compromesso è altamente probabile	Compromesso probabile	Compromesso improbabile	Compromesso altamente improbabile
Molto facile da sfruttare	Critico	Critico	Elevata	Media
Un po' facile da sfruttare	Critico	Elevata	Media	Media
Un po' difficile da sfruttare	Elevata	Media	Media	Bassa
Molto difficile da sfruttare	Media	Media	Bassa	Bassa

Definizioni di gravità

Le etichette di gravità sono definite come segue.

Critico: il problema deve essere risolto immediatamente per evitare che si aggravi.

Ad esempio, un bucket S3 aperto è considerato un risultato di gravità critica. Poiché così tanti autori delle minacce cercano bucket S3 aperti, è probabile che i dati contenuti nei bucket S3 esposti vengano scoperti e consultati da altri.

In generale, le risorse accessibili al pubblico sono considerate problemi di sicurezza critici. È necessario trattare i risultati critici con la massima urgenza. È inoltre necessario considerare la criticità della risorsa.

Alto: la questione deve essere affrontata come una priorità a breve termine.

Ad esempio, se un gruppo di sicurezza VPC predefinito è aperto al traffico in entrata e in uscita, viene considerato ad alta severità. È piuttosto facile per un autore di minacce compromettere un VPC utilizzando questo metodo. È anche probabile che l'autore della minaccia sia in grado di interrompere o esfiltrare le risorse una volta inserite nel VPC.

Security Hub consiglia di considerare un rilevamento di elevata gravità come una priorità a breve termine. È necessario adottare misure correttive immediate. È inoltre necessario considerare la criticità della risorsa.

Medio: la questione dovrebbe essere affrontata come priorità a medio termine.

Ad esempio, la mancanza di crittografia per i dati in transito è considerata una rilevazione di gravità media. È necessario un man-in-the-middle attacco sofisticato per sfruttare questa debolezza. In altre parole, è piuttosto difficile. È probabile che alcuni dati vengano compromessi se lo scenario di minaccia ha esito positivo.

Security Hub consiglia di esaminare la risorsa implicata il prima possibile. È inoltre necessario considerare la criticità della risorsa.

Basso: il problema non richiede di per sé un'azione.

Ad esempio, la mancata raccolta di informazioni forensi è considerata di bassa gravità. Questo controllo può aiutare a prevenire future compromessi, ma l'assenza di analisi forensi non porta direttamente a un compromesso.

Non è necessario intervenire immediatamente sui risultati di bassa gravità, ma possono fornire un contesto quando li si correla con altri problemi.

Informativo: non è stato rilevato alcun punto debole nella configurazione.

In altre parole, lo stato è PASSEDDWARNING, oNOT AVAILABLE.

Non vi è alcuna azione consigliata. I risultati informativi aiutano i clienti a dimostrare di essere conformi.

Regole per l'aggiornamento dei risultati del controllo

Un successivo controllo rispetto a una determinata regola potrebbe generare un nuovo risultato. Ad esempio, lo stato di «Evita l'uso dell'utente root» potrebbe cambiare da FAILED aPASSED. In tal caso, viene generato un nuovo risultato che contiene il risultato più recente.

Se un controllo successivo rispetto a una determinata regola genera un risultato identico a quello corrente, il risultato esistente viene aggiornato e nessun nuovo risultato viene generato.

Security Hub archivia automaticamente i risultati dei controlli se la risorsa associata viene eliminata, la risorsa non esiste o il controllo è disabilitato. Una risorsa potrebbe non esistere più perché il servizio associato non è attualmente utilizzato. I risultati vengono archiviati automaticamente in base a uno dei seguenti criteri:

- I risultati non vengono aggiornati per tre-cinque giorni (si noti che si tratta del massimo impegno e non è garantito).

- La AWS Config valutazione associata è stata restituita NOT_APPLICABLE.

Stato di conformità e stato di controllo

Il `Compliance.Status` campo del AWS Security Finding Format descrive il risultato di un risultato di controllo. Security Hub utilizza lo stato di conformità dei risultati del controllo per determinare lo stato di controllo generale. Lo stato del controllo viene visualizzato nella pagina dei dettagli di un controllo sulla console Security Hub.

Per un account amministratore, lo stato del controllo riflette lo stato del controllo nell'account amministratore e negli account dei membri. In particolare, lo stato generale di un controllo appare come Non riuscito se il controllo presenta uno o più risultati non riusciti nell'account amministratore o in uno degli account dei membri. Se è stata impostata una regione di aggregazione, lo stato di controllo nella regione di aggregazione riflette lo stato di controllo nella regione di aggregazione e nelle regioni collegate. In particolare, lo stato generale di un controllo appare come Non riuscito se il controllo presenta uno o più risultati non riusciti nella regione di aggregazione o in una delle regioni collegate.

Security Hub genera in genere lo stato di controllo iniziale entro 30 minuti dalla prima visita alla pagina di riepilogo o alla pagina degli standard di sicurezza della console Security Hub. È necessario che [la registrazione AWS Config delle risorse](#) sia configurata per visualizzare lo stato del controllo. Dopo la prima generazione degli stati di controllo, Security Hub aggiorna gli stati di controllo ogni 24 ore in base ai risultati delle 24 ore precedenti. Un timestamp nella pagina dei dettagli del controllo indica quando lo stato del controllo è stato aggiornato l'ultima volta.

Note

Possono essere necessarie fino a 24 ore dall'attivazione di un controllo per la generazione degli stati di controllo per la prima volta nelle regioni della Cina e. AWS GovCloud (US) Region

Valori relativi allo stato di conformità di un risultato

Allo stato di conformità di ogni risultato viene assegnato uno dei seguenti valori:

- PASSED— Indica che il controllo ha superato il controllo di sicurezza per questo risultato. Imposta automaticamente il Security Hub `Workflow.Status` su RESOLVED.

Se `Compliance.Status` per un risultato cambia `PASSED` da `FAILED`, o `WARNINGNOT_AVAILABLE`, ed `Workflow.Status` era uno `NOTIFIED` dei due `RESOLVED`, allora Security Hub viene `Workflow.Status` impostato automaticamente su `NEW`.

Se non disponi di risorse corrispondenti a un controllo, Security Hub produce un `PASSED` risultato a livello di account. Se hai una risorsa corrispondente a un controllo ma poi la elimini, Security Hub crea un `NOT_AVAILABLE` risultato e lo archivia immediatamente. Dopo 18 ore, riceverai un `PASSED` risultato poiché non disponi più di risorse corrispondenti al controllo.

- **FAILED**— Indica che il controllo non ha superato il controllo di sicurezza per questo risultato.
- **WARNING**— Indica che il controllo è stato completato, ma Security Hub non è in grado di determinare se la risorsa è in uno `FAILED` stato `PASSED` o.
- **NOT_AVAILABLE**— Indica che il controllo non può essere completato perché un server ha avuto un errore, la risorsa è stata eliminata o il risultato della AWS Config valutazione è `NOT_APPLICABLE`.

Se il risultato della AWS Config valutazione è stato `NOT_APPLICABLE`, Security Hub archivia automaticamente il risultato.

Valori per lo stato del controllo

Security Hub ricava uno stato di controllo generale dallo stato di conformità dei risultati del controllo. Nel determinare lo stato del controllo, Security Hub ignora i risultati con un `RecordState` di `ARCHIVED` e i risultati con un `Workflow.Status` di `SUPPRESSED`.

Allo stato del controllo viene assegnato uno dei seguenti valori:

- **Passato**: indica che tutti i risultati hanno uno stato di conformità pari a `PASSED`.
- **Non riuscito**: indica che almeno un risultato ha uno stato di conformità pari a `FAILED`.
- **Sconosciuto**: indica che almeno un risultato ha uno stato di conformità pari a `WARNING` o `NOT_AVAILABLE`. Nessun risultato ha uno stato di conformità pari a `FAILED`.
- **Nessun dato**: indica che non ci sono risultati per il controllo. Ad esempio, un controllo appena abilitato ha questo stato fino a quando Security Hub non inizia a generare i relativi risultati. Un controllo ha questo stato anche se tutti i risultati lo sono `SUPPRESSED` o se non è disponibile nella regione corrente.
- **Disabilitato**: indica che il controllo è disabilitato nell'account e nella regione correnti. Al momento non vengono eseguiti controlli di sicurezza per questo controllo nell'account e nella regione

correnti. Tuttavia, i risultati di un controllo disattivato possono avere un valore per lo stato di conformità fino a 24 ore dopo la disabilitazione.

Definizione dei punteggi di sicurezza

La pagina Riepilogo e la pagina Controlli della console Security Hub mostrano un punteggio di sicurezza riassuntivo per tutti gli standard abilitati. Nella pagina Standard di sicurezza, Security Hub mostra anche un punteggio di sicurezza compreso tra 0 e 100 per cento per ogni standard abilitato.

Quando attivi Security Hub per la prima volta, Security Hub calcola il punteggio di sicurezza riassuntivo e i punteggi di sicurezza standard entro 30 minuti dalla prima visita alla pagina di riepilogo o alla pagina degli standard di sicurezza sulla console di Security Hub. I punteggi vengono generati solo per gli standard abilitati quando visiti quelle pagine. Per visualizzare un elenco degli standard attualmente abilitati, richiama l'operazione [GetEnabledStandardsAPI](#). Inoltre, la registrazione AWS Config delle risorse deve essere configurata per visualizzare gli spartiti. Il punteggio di sicurezza riassuntivo è la media dei punteggi di sicurezza standard.

Dopo la prima generazione dei punteggi, Security Hub aggiorna i punteggi di sicurezza ogni 24 ore. Security Hub visualizza un timestamp per indicare quando un punteggio di sicurezza è stato aggiornato l'ultima volta.

Note

Potrebbero essere necessarie fino a 24 ore prima che i punteggi di sicurezza vengano generati per la prima volta nelle regioni cinesi e. AWS GovCloud (US) Region

Se attivi i [risultati del controllo consolidato](#), l'aggiornamento dei punteggi di sicurezza potrebbe richiedere fino a 24 ore. Inoltre, l'abilitazione di una nuova regione di aggregazione o l'aggiornamento delle aree collegate ripristina i punteggi di sicurezza esistenti. Security Hub potrebbe impiegare fino a 24 ore per generare nuovi punteggi di sicurezza che includono i dati delle regioni aggiornate.

Come vengono calcolati i punteggi di sicurezza

I punteggi di sicurezza rappresentano la proporzione tra controlli passati e controlli abilitati. Il punteggio viene visualizzato come percentuale arrotondata per eccesso o per difetto al numero intero più vicino.

Security Hub calcola un punteggio di sicurezza riassuntivo per tutti gli standard abilitati. Security Hub calcola anche un punteggio di sicurezza per ogni standard abilitato. Ai fini del calcolo del punteggio, i controlli abilitati includono controlli con lo stato di Passato, Non riuscito e Sconosciuto. I controlli con stato Nessun dato sono esclusi dal calcolo del punteggio.

Security Hub ignora i risultati archiviati e soppressi durante il calcolo dello stato del controllo. Ciò può influire sui punteggi di sicurezza. Ad esempio, se si eliminano tutti i risultati non riusciti di un controllo, il relativo stato diventa Passato, il che a sua volta può migliorare i punteggi di sicurezza. Per ulteriori informazioni sullo stato del controllo, vedere [Stato di conformità e stato di controllo](#).

Esempio di punteggio:

Standard	Controlli superati	Controlli falliti	Controlli sconosciuti	Punteggio standard
AWS Best practice di sicurezza di base v1.0.0	168	22	0	88%
Benchmark CIS AWS Foundations v1.4.0	8	29	0	22%
Benchmark CIS AWS Foundations v1.2.0	6	35	0	15%
Pubblicazione speciale del NIST 800-53 Revisione 5	159	56	0	74%
PCI DSS v3.2.1	28	17	0	62%

Nel calcolare il punteggio di sicurezza riassuntivo, Security Hub conta ogni controllo una sola volta tra gli standard. Ad esempio, se hai abilitato un controllo che si applica a tre standard abilitati, ai fini del punteggio viene conteggiato come un solo controllo abilitato.

In questo esempio, sebbene il numero totale di controlli abilitati tra gli standard abilitati sia 528, Security Hub conta ogni controllo univoco una sola volta ai fini del punteggio. Il numero di controlli univoci abilitati è probabilmente inferiore a 528. Se assumiamo che il numero di controlli univoci abilitati sia 515 e che il numero di controlli unici approvati sia 357, il punteggio riepilogativo è 69%. Questo punteggio viene calcolato dividendo il numero di controlli univoci passati per il numero di controlli univoci abilitati.

Potresti avere un punteggio riassuntivo diverso dal punteggio di sicurezza standard anche se hai abilitato solo uno standard nel tuo account nella regione corrente. Ciò può verificarsi se hai effettuato l'accesso a un account amministratore e negli account membro sono abilitati standard aggiuntivi o standard diversi. Ciò può verificarsi anche se stai visualizzando il punteggio della Regione di aggregazione e nelle Regioni collegate sono abilitati standard aggiuntivi o standard diversi.

Punteggi di sicurezza per gli account amministratore

Se hai effettuato l'accesso a un account amministratore, il punteggio di sicurezza riepilogativo e i punteggi standard tengono conto degli stati di controllo nell'account amministratore e in tutti gli account dei membri.

Se lo stato di un controllo è Non riuscito anche in un solo account membro, il relativo stato è Non riuscito nell'account amministratore e influisce sui punteggi dell'account amministratore.

Se hai effettuato l'accesso a un account amministratore e stai visualizzando i punteggi in una regione di aggregazione, i punteggi di sicurezza tengono conto degli stati di controllo in tutti gli account membro e in tutte le regioni collegate.

Punteggi di sicurezza se hai impostato una regione di aggregazione

Se hai impostato un'aggregazione Regione AWS, il punteggio di sicurezza riassuntivo e i punteggi standard tengono conto complessivamente degli stati di controllo Regioni collegate.

Se lo stato di un controllo è Non riuscito anche in una sola regione collegata, il relativo stato è Non riuscito nella regione di aggregazione e influisce sui punteggi della regione di aggregazione.

Se hai effettuato l'accesso a un account amministratore e stai visualizzando i punteggi in una regione di aggregazione, i punteggi di sicurezza tengono conto degli stati di controllo in tutti gli account membro e in tutte le regioni collegate.

Riferimento agli standard del Security Hub

AWS Security Hub attualmente supporta gli standard di sicurezza descritti in questa sezione.

Scegli uno standard per visualizzare maggiori dettagli su di esso e sui controlli ad esso applicabili.

Gli standard e i controlli di Security Hub non garantiscono la conformità a nessun quadro normativo o controllo. Piuttosto, i controlli forniscono un modo per monitorare lo stato attuale delle tue Account AWS risorse.

Standard supportati

- [AWS Standard FSBP \(Foundational Security Best Practices\)](#)
- [CIS AWS Foundations Benchmark](#)
- [Istituto nazionale di standard e tecnologia \(NIST\) SP 800-53 Rev. 5](#)
- [Payment Card Industry Data Security Standard \(PCI DSS\)](#)
- [AWS Standard di etichettatura delle risorse](#)
- [Standard gestiti dai servizi](#)

AWS Standard FSBP (Foundational Security Best Practices)

Lo standard AWS Foundational Security Best Practices è un insieme di controlli che rilevano quando le tue Account AWS risorse si discostano dalle migliori pratiche di sicurezza.

Lo standard ti consente di valutare continuamente tutti i tuoi Account AWS carichi di lavoro per identificare rapidamente le aree di deviazione dalle migliori pratiche. Fornisce indicazioni pratiche e prescrittive su come migliorare e mantenere il livello di sicurezza dell'organizzazione.

I controlli includono le migliori pratiche di sicurezza per risorse provenienti da più fonti. Servizi AWS A ogni controllo viene inoltre assegnata una categoria che riflette la funzione di sicurezza a cui si applica. Per ulteriori informazioni, consulta [the section called "Categorie di controllo"](#).

Controlli che si applicano allo standard FSBP

[\[Account.1\] Le informazioni di contatto di sicurezza devono essere fornite per un Account AWS](#)

[\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)

[\[ACM.2\] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit](#)

[\[ApiGateway.1\] API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati](#)

[\[ApiGateway.2\] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend](#)

[\[ApiGateway.3\] Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray](#)

[\[ApiGateway.4\] L'API Gateway deve essere associato a un ACL Web WAF](#)

[\[ApiGateway.5\] I dati della cache dell'API REST API Gateway devono essere crittografati quando sono inattivi](#)

[\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione](#)

[\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages](#)

[\[AppSync.2\] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata](#)

[\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)

[\[AutoScaling.1\] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB](#)

[\[AutoScaling.2\] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità](#)

[\[AutoScaling.3\] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 \(IMDSv2\)](#)

[\[Autoscaling.5\] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici](#)

[\[AutoScaling.6\] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità](#)

[\[AutoScaling.9\] I gruppi di Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2](#)

[\[Backup.1\] i punti di AWS Backup ripristino devono essere crittografati a riposo](#)

[\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)

[\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)

[\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)

[\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)

[\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)

[\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)

[\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)

[\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)

[\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)

[\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)

[\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)

[\[CloudTrail.1\] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura](#)

[\[CloudTrail.2\] CloudTrail dovrebbe avere la crittografia a riposo abilitata](#)

[\[CloudTrail.4\] la convalida dei file di CloudTrail registro dovrebbe essere abilitata](#)

[\[CloudTrail.5\] i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch](#)

[\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)

[\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)

[\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)

[\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)

[\[Config.1\] AWS Config dovrebbe essere abilitato](#)

[\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)

[\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)

[\[DMS.6\] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato](#)

[\[DMS.7\] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata](#)

[\[DMS.8\] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata](#)

[\[DMS.9\] Gli endpoint DMS devono utilizzare SSL](#)

[\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)

[\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)

[\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)

[\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)

[\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)

[\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)

[\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)

[\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)

[\[DynamoDB.1\] Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda](#)

[\[DynamoDB.2\] Le tabelle DynamoDB dovrebbero avere il ripristino abilitato point-in-time](#)

[\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)

[\[DynamoDB.6\] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata](#)

[\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)

[\[EC2.1\] Gli snapshot di Amazon EBS non devono essere ripristinabili pubblicamente](#)

[\[EC2.2\] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita](#)

[\[EC2.3\] I volumi Amazon EBS collegati devono essere crittografati a riposo](#)

[\[EC2.4\] Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato](#)

[\[EC2.6\] La registrazione del flusso VPC deve essere abilitata in tutti i VPC](#)

[\[EC2.7\] La crittografia predefinita di EBS deve essere abilitata](#)

[\[EC2.8\] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 \(IMDSv2\)](#)

[\[EC2.9\] Le istanze Amazon EC2 non devono avere un indirizzo IPv4 pubblico](#)

[\[EC2.10\] Amazon EC2 deve essere configurato per utilizzare endpoint VPC creati per il servizio Amazon EC2](#)

[\[EC2.15\] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici](#)

[\[EC2.16\] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse](#)

[\[EC2.17\] Le istanze Amazon EC2 non devono utilizzare più ENI](#)

[\[EC2.18\] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate](#)

[\[EC2.19\] I gruppi di sicurezza non devono consentire l'accesso illimitato alle porte ad alto rischio](#)

[\[EC2.20\] Entrambi i tunnel VPN per una connessione VPN da sito a sito devono essere AWS attivi](#)

[\[EC2.21\] Gli ACL di rete non dovrebbero consentire l'ingresso dalla porta 0.0.0.0/0 alla porta 22 o alla porta 3389](#)

[\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)

[\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)

[\[EC2.25\] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete](#)

[\[EC2.51\] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata](#)

[\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)

[\[ECR.2\] I repository privati ECR devono avere l'immutabilità dei tag configurata](#)

[\[ECR.3\] I repository ECR devono avere almeno una politica del ciclo di vita configurata](#)

[ECS.1] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.

[ECS.2] Ai servizi ECS non devono essere assegnati automaticamente indirizzi IP pubblici

[ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host

[ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati

[ECS.5] I contenitori ECS devono essere limitati all'accesso in sola lettura ai filesystem root

[ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore

[ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione

[ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate

[ECS.12] I cluster ECS devono utilizzare Container Insights

[EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS

[EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup

[EFS.3] I punti di accesso EFS devono applicare una directory principale

[EFS.4] I punti di accesso EFS devono applicare un'identità utente

[EFS.6] I target di montaggio EFS non devono essere associati a una sottorete pubblica

[EKS.1] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico

[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata

[EKS.3] I cluster EKS devono utilizzare segreti Kubernetes crittografati

[EKS.8] I cluster EKS devono avere la registrazione di controllo abilitata

[ElastiCache.1] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato

[ElastiCache.2] ElastiCache per i cluster di cache Redis dovrebbe avere l'aggiornamento automatico della versione secondaria abilitato

[\[ElastiCache.3\] ElastiCache per i gruppi di replica Redis dovrebbe avere il failover automatico abilitato](#)

[\[ElastiCache.4\] ElastiCache per i gruppi di replica Redis deve essere crittografato a riposo](#)

[\[ElastiCache.5\] ElastiCache per i gruppi di replica Redis devono essere crittografati in transito](#)

[\[ElastiCache.6\] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH](#)

[\[ElastiCache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito](#)

[\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)

[\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)

[\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)

[\[ELB.1\] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS](#)

[\[ELB.2\] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager](#)

[\[ELB.3\] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS](#)

[\[ELB.4\] L'Application Load Balancer deve essere configurato per eliminare le intestazioni http](#)

[\[ELB.5\] La registrazione delle applicazioni e dei sistemi Classic Load Balancers deve essere abilitata](#)

[\[ELB.6\] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata](#)

[\[ELB.7\] I Classic Load Balancer devono avere il drenaggio della connessione abilitato](#)

[\[ELB.8\] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita con una durata elevata AWS Config](#)

[\[ELB.9\] I Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato](#)

[\[ELB.10\] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità](#)

[\[ELB.12\] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)

[\[ELB.13\] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità](#)

[\[ELB.14\] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)

[\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)

[\[EMR.2\] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata](#)

[\[ES.1\] I domini Elasticsearch devono avere la crittografia a riposo abilitata](#)

[\[ES.2\] I domini Elasticsearch non devono essere accessibili al pubblico](#)

[\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)

[\[ES.4\] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch](#)

[\[ES.5\] I domini Elasticsearch devono avere la registrazione di controllo abilitata](#)

[\[ES.6\] I domini Elasticsearch devono avere almeno tre nodi di dati](#)

[\[ES.7\] I domini Elasticsearch devono essere configurati con almeno tre nodi master dedicati](#)

[\[ES.8\] Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)

[\[EventBridge.3\] i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata](#)

[\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)

[\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)

[\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)

[\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)

[\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)

[\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)

[\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)

[\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)

[\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)

[\[IAM.7\] Le politiche relative alle password per gli utenti IAM dovrebbero avere configurazioni solide](#)

[\[IAM.8\] Le credenziali utente IAM non utilizzate devono essere rimosse](#)

[\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)

[\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)

[\[KMS.1\] Le politiche gestite dai clienti di IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS](#)

[\[KMS.2\] I principali IAM non devono disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS](#)

[\[KMS.3\] AWS KMS keys non deve essere eliminato involontariamente](#)

[\[Lambda.1\] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico](#)

[\[Lambda.2\] Le funzioni Lambda devono utilizzare runtime supportati](#)

[\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)

[\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)

[\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato](#)

[\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)

[\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)

[\[MSK.1\] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker](#)

[\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)

[\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)

[\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)

[\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)

[\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)

[\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)

[\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)

[\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)

[\[NetworkFirewall.2\] La registrazione del Network Firewall deve essere abilitata](#)

[\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)

[\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)

[\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)

[\[NetworkFirewall.6\] Il gruppo di regole Stateless Network Firewall non deve essere vuoto](#)

[\[NetworkFirewall.9\] I firewall Network Firewall devono avere la protezione da eliminazione abilitata](#)

[I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)

[I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)

[I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)

[La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)

[I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)

[I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)

[I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)

[\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)

[Nei OpenSearch domini \[Opensearch.10\] deve essere installato l'ultimo aggiornamento software](#)

[L'autorità di certificazione AWS Private CA principale \[PCA.1\] deve essere disabilitata](#)

[\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)

[\[RDS.1\] L'istanza RDS deve essere privata](#)

[\[RDS.2\] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, in base alla durata PubliclyAccessible AWS Config](#)

[\[RDS.3\] Le istanze database RDS devono avere la crittografia dei dati inattivi abilitata](#)

[\[RDS.4\] Le istantanee dei cluster RDS e le istantanee del database devono essere crittografate quando sono inattive](#)

[\[RDS.5\] Le istanze DB RDS devono essere configurate con più zone di disponibilità](#)

[\[RDS.6\] Il monitoraggio avanzato deve essere configurato per le istanze DB RDS](#)

[\[RDS.7\] I cluster RDS devono avere la protezione da eliminazione abilitata](#)

[\[RDS.8\] Le istanze DB RDS devono avere la protezione da eliminazione abilitata](#)

[\[RDS.9\] Le istanze DB RDS devono pubblicare i log nei registri CloudWatch](#)

[\[RDS.10\] L'autenticazione IAM deve essere configurata per le istanze RDS](#)

[\[RDS.11\] Le istanze RDS devono avere i backup automatici abilitati](#)

[\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)

[\[RDS.13\] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati](#)

[\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)

[\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)

[\[RDS.16\] I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee](#)

[\[RDS.17\] Le istanze DB RDS devono essere configurate per copiare i tag nelle istantanee](#)

[\[RDS.18\] Le istanze RDS devono essere distribuite in un VPC](#)

[\[RDS.19\] Le sottoscrizioni esistenti per le notifiche di eventi RDS devono essere configurate per gli eventi critici del cluster](#)

[\[RDS.20\] Le sottoscrizioni di notifica degli eventi RDS esistenti devono essere configurate per gli eventi critici delle istanze di database](#)

[\[RDS.21\] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici del gruppo di parametri del database](#)

[\[RDS.22\] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici dei gruppi di sicurezza del database](#)

[\[RDS.23\] Le istanze RDS non devono utilizzare una porta predefinita del motore di database](#)

[\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)

[\[RDS.25\] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato](#)

[\[RDS.27\] I cluster RDS DB devono essere crittografati quando sono inattivi](#)

[\[RDS.34\] I cluster Aurora MySQL DB devono pubblicare i log di controllo nei registri CloudWatch](#)

[\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)

[\[Redshift.1\] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico](#)

[\[Redshift.2\] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito](#)

[\[Redshift.3\] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate](#)

[\[Redshift.4\] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata](#)

[\[Redshift.6\] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati](#)

[\[Redshift.7\] I cluster Redshift devono utilizzare un routing VPC avanzato](#)

[\[Redshift.8\] I cluster Amazon Redshift non devono utilizzare il nome utente predefinito di amministratore](#)

[\[Redshift.9\] I cluster Redshift non devono utilizzare il nome di database predefinito](#)

[\[Redshift.10\] I cluster Redshift devono essere crittografati a riposo](#)

[\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)

[\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)

[\[S3.2\] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura](#)

[\[S3.3\] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura](#)

[\[S3.5\] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL](#)

[\[S3.6\] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS](#)

[\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)

[\[S3.9\] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata](#)

[\[S3.12\] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3](#)

[\[S3.13\] I bucket generici S3 devono avere configurazioni del ciclo di vita](#)

[\[S3.19\] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)

[\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)

[\[SageMaker.2\] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato](#)

[\[SageMaker.3\] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook](#)

[\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)

[\[SecretsManager.1\] I segreti di Secrets Manager devono avere la rotazione automatica abilitata](#)

[\[SecretsManager.2\] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente](#)

[\[SecretsManager.3\] Rimuovi i segreti inutilizzati di Secrets Manager](#)

[\[SecretsManager.4\] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni](#)

[\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)

[\[SQS.1\] Le code di Amazon SQS devono essere crittografate quando sono inattive](#)

[\[SSM.1\] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager](#)

[\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)

[\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)

[\[SSM.4\] I documenti SSM non devono essere pubblici](#)

[\[StepFunctions.1\] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata](#)

[\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)

[\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)

[\[WAF.2\] Le regole regionali AWS WAF classiche devono avere almeno una condizione](#)

[\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)

[\[WAF.4\] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

[\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)

[\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)

[\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

[\[WAF.10\] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole](#)

[Le regole \[WAF.12\] devono avere le metriche abilitate AWS WAF CloudWatch](#)

CIS AWS Foundations Benchmark

Il benchmark Center for Internet Security (CIS) AWS Foundations funge da set di best practice per la configurazione della sicurezza per AWS. Queste best practice accettate dal settore forniscono procedure chiare di implementazione e valutazione. step-by-step Dai sistemi operativi ai servizi cloud e ai dispositivi di rete, i controlli di questo benchmark aiutano a proteggere i sistemi specifici utilizzati dall'organizzazione.

AWS Security Hub supporta CIS AWS Foundations Benchmark v3.0.0, 1.4.0 e v1.2.0.

Questa pagina elenca i controlli di sicurezza supportati da ciascuna versione e fornisce un confronto tra le versioni.

Benchmark CIS AWS Foundations v3.0.0

Security Hub supporta la versione 3.0.0 del benchmark CIS Foundations AWS .

Security Hub ha soddisfatto i requisiti della certificazione del software di sicurezza CIS e ha ottenuto la certificazione del software di sicurezza CIS per i seguenti benchmark CIS:

- Benchmark CIS per CIS Foundations Benchmark, v3.0.0, livello 1 AWS
- Benchmark CIS per CIS Foundations Benchmark, v3.0.0, livello 2 AWS

Controlli che si applicano a CIS Foundations Benchmark v3.0.0 AWS

[\[Account.1\] Le informazioni di contatto di sicurezza devono essere fornite per un Account AWS](#)

[\[CloudTrail.1\] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura](#)

[\[CloudTrail.2\] CloudTrail dovrebbe avere la crittografia a riposo abilitata](#)

[\[CloudTrail.4\] la convalida dei file di CloudTrail registro dovrebbe essere abilitata](#)

[\[CloudTrail.7\] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail](#)

[\[Config.1\] AWS Config dovrebbe essere abilitato](#)

[\[EC2.2\] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita](#)

[\[EC2.6\] La registrazione del flusso VPC deve essere abilitata in tutti i VPC](#)

[\[EC2.7\] La crittografia predefinita di EBS deve essere abilitata](#)

[\[EC2.8\] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 \(IMDSv2\)](#)

[\[EC2.21\] Gli ACL di rete non dovrebbero consentire l'ingresso dalla porta 0.0.0.0/0 alla porta 22 o alla porta 3389](#)

[\[EC2.53\] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da 0.0.0.0/0 alle porte di amministrazione remota del server](#)

[\[EC2.54\] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da :/0 alle porte di amministrazione remota del server](#)

[\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)

[\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)

[\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)

[\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)

[\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)

[\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)

[\[IAM.9\] L'MFA deve essere abilitata per l'utente root](#)

[\[IAM.15\] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14](#)

[\[IAM.16\] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password](#)

[\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)

[\[IAM.22\] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse](#)

[\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)

[\[IAM.27\] Le identità IAM non devono avere la policy allegata AWSCloudShellFullAccess](#)

[\[IAM.28\] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato](#)

[\[KMS.4\] la rotazione dei tasti dovrebbe essere abilitata AWS KMS](#)

[\[RDS.2\] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, in base alla durata PubliclyAccessible AWS Config](#)

[\[RDS.3\] Le istanze database RDS devono avere la crittografia dei dati inattivi abilitata](#)

[\[RDS.13\] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati](#)

[\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)

[\[S3.5\] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL](#)

[\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)

[\[S3.20\] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata](#)

[\[S3.22\] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto](#)

[\[S3.23\] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto](#)

Benchmark CIS Foundations v1.4.0 AWS

Security Hub supporta la versione 1.4.0 del benchmark CIS Foundations AWS .

Controlli che si applicano a CIS Foundations Benchmark v1.4.0 AWS

[\[CloudTrail.1\] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura](#)

[\[CloudTrail.2\] CloudTrail dovrebbe avere la crittografia a riposo abilitata](#)

[\[CloudTrail.4\] la convalida dei file di CloudTrail registro dovrebbe essere abilitata](#)

[\[CloudTrail.5\] i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch](#)

[\[CloudTrail.6\] Assicurati che il bucket S3 utilizzato per archiviare i log non sia accessibile al pubblico CloudTrail](#)

[\[CloudTrail.7\] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail](#)

[\[CloudWatch.1\] Dovrebbero esistere un filtro logmetrico e un allarme per l'utilizzo da parte dell'utente «root»](#)

[\[CloudWatch.4\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM](#)

[\[CloudWatch.5\] Assicurati che esistano un filtro metrico di registro e un allarme per le CloudTrail AWS Config variazioni di durata](#)

[\[CloudWatch.6\] Assicurati che esistano un filtro metrico di registro e un allarme per gli AWS Management Console errori di autenticazione](#)

[\[CloudWatch.7\] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione programmata delle chiavi gestite dal cliente](#)

[\[CloudWatch.8\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3](#)

[\[CloudWatch.9\] Assicurati che esistano un filtro metrico di log e un allarme per le AWS Config modifiche alla configurazione](#)

[\[CloudWatch.10\] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza](#)

[\[CloudWatch.11\] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete \(NACL\)](#)

[\[CloudWatch.12\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche ai gateway di rete](#)

[\[CloudWatch.13\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte](#)

[\[CloudWatch.14\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche al VPC](#)

[\[Config.1\] AWS Config dovrebbe essere abilitato](#)

[\[EC2.2\] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita](#)

[\[EC2.6\] La registrazione del flusso VPC deve essere abilitata in tutti i VPC](#)

[\[EC2.7\] La crittografia predefinita di EBS deve essere abilitata](#)

[\[EC2.21\] Gli ACL di rete non dovrebbero consentire l'ingresso dalla porta 0.0.0.0/0 alla porta 22 o alla porta 3389](#)

[\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)

[\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)

[\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)

[\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)

[\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)

[\[IAM.9\] L'MFA deve essere abilitata per l'utente root](#)

[\[IAM.15\] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14](#)

[\[IAM.16\] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password](#)

[\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)

[\[IAM.22\] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse](#)

[\[KMS.4\] la rotazione dei tasti dovrebbe essere abilitata AWS KMS](#)

[\[RDS.3\] Le istanze database RDS devono avere la crittografia dei dati inattivi abilitata](#)

[\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)

[\[S3.5\] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL](#)

[\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)

[\[S3.20\] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata](#)

Benchmark Foundations Center for Internet Security (CIS) v1.2.0 AWS

Security Hub supporta la versione 1.2.0 del benchmark CIS AWS Foundations.

Security Hub ha soddisfatto i requisiti della certificazione del software di sicurezza CIS e ha ottenuto la certificazione del software di sicurezza CIS per i seguenti benchmark CIS:

- Benchmark CIS per CIS Foundations Benchmark, v1.2.0, livello 1 AWS
- Benchmark CIS per CIS Foundations Benchmark, v1.2.0, livello 2 AWS

Controlli che si applicano a CIS Foundations Benchmark v1.2.0 AWS

[\[CloudTrail.1\] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura](#)

[\[CloudTrail.2\] CloudTrail dovrebbe avere la crittografia a riposo abilitata](#)

[\[CloudTrail.4\] la convalida dei file di CloudTrail registro dovrebbe essere abilitata](#)

[\[CloudTrail.5\] i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch](#)

[\[CloudTrail.6\] Assicurati che il bucket S3 utilizzato per archiviare i log non sia accessibile al pubblico CloudTrail](#)

[\[CloudTrail.7\] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail](#)

[\[CloudWatch.1\] Dovrebbero esistere un filtro logmetrico e un allarme per l'utilizzo da parte dell'utente «root»](#)

[\[CloudWatch.2\] Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate](#)

[\[CloudWatch.3\] Assicurarsi che esistano un filtro metrico di registro e un allarme per l'accesso alla Console di gestione senza MFA](#)

[\[CloudWatch.4\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM](#)

[\[CloudWatch.5\] Assicurati che esistano un filtro metrico di registro e un allarme per le CloudTrail AWS Config variazioni di durata](#)

[\[CloudWatch.6\] Assicurati che esistano un filtro metrico di registro e un allarme per gli AWS Management Console errori di autenticazione](#)

[\[CloudWatch.7\] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione programmata delle chiavi gestite dal cliente](#)

[\[CloudWatch.8\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3](#)

[\[CloudWatch.9\] Assicurati che esistano un filtro metrico di log e un allarme per le AWS Config modifiche alla configurazione](#)

[\[CloudWatch.10\] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza](#)

[\[CloudWatch.11\] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete \(NACL\)](#)

[\[CloudWatch.12\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche ai gateway di rete](#)

[\[CloudWatch.13\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte](#)

[\[CloudWatch.14\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche al VPC](#)

[\[Config.1\] AWS Config dovrebbe essere abilitato](#)

[\[EC2.2\] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita](#)

[\[EC2.6\] La registrazione del flusso VPC deve essere abilitata in tutti i VPC](#)

[\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22](#)

[\[EC2.14\] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389](#)

[\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)

[\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)

[\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)

[\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)

[\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)

[\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)

[\[IAM.8\] Le credenziali utente IAM non utilizzate devono essere rimosse](#)

[\[IAM.9\] L'MFA deve essere abilitata per l'utente root](#)

[\[IAM.11\] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola](#)

[\[IAM.12\] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola](#)

[\[IAM.13\] Assicurati che la politica delle password IAM richieda almeno un simbolo](#)

[\[IAM.14\] Assicurati che la politica delle password IAM richieda almeno un numero](#)

[\[IAM.15\] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14](#)

[\[IAM.16\] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password](#)

[\[IAM.17\] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno](#)

[\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)

[\[KMS.4\] la rotazione dei tasti dovrebbe essere abilitata AWS KMS](#)

Confronto delle versioni per CIS Foundations Benchmark AWS

Questa sezione riassume le differenze tra il Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0, v1.4.0 e v1.2.0.

Security Hub supporta ognuna di queste versioni del benchmark CIS AWS Foundations, ma consigliamo di utilizzare la versione 3.0.0 per rimanere aggiornati sulle migliori pratiche di sicurezza. È possibile che siano abilitate più versioni dello standard contemporaneamente. Per ulteriori informazioni, consulta [Abilitazione e disabilitazione degli standard di sicurezza](#). Se desideri eseguire l'aggiornamento alla versione 3.0.0, è meglio abilitarlo prima di disabilitare una versione precedente.

[Se utilizzi l'integrazione di Security Hub con AWS Organizations per gestire centralmente più account Account AWS e desideri abilitare in batch la v3.0.0 su tutti gli account, puoi utilizzare la configurazione centrale.](#)

Mappatura dei controlli ai requisiti CIS in ogni versione

Scopri quali controlli supporta ogni versione di CIS AWS Foundations Benchmark.

ID e titolo di controllo	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[Account.1] Le informazioni di contatto di sicurezza devono essere fornite per un Account AWS	1.2	1.2	1.18
[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura	3.1	3.1	2.1
[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura	3.1	3.1	2.1
[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata	3.5	3.7	2.7
[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata	3.2	3.2	2.2
[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch	Non supportato: il CIS ha rimosso questo requisito	3.4	2.4
[CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i log non sia accessibile al pubblico CloudTrail	Non supportato: il CIS ha rimosso questo requisito	3.3	2.3

ID e titolo di controllo	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail	3.4	3.6	2.6
[CloudWatch.1] Dovrebbero esistere un filtro logmetrico e un allarme per l'utilizzo da parte dell'utente «root»	Non supportato: controllo manuale	4.3	3.3
[CloudWatch.2] Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate	Non supportato: controllo manuale	Non supportato: controllo manuale	3.1
[CloudWatch.3] Assicurarsi che esistano un filtro metrico di registro e un allarme per l'accesso alla Console di gestione senza MFA	Non supportato: controllo manuale	Non supportato: controllo manuale	3.2
[CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM	Non supportato: controllo manuale	4.4	3.4
[CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le CloudTrail AWS Config variazioni di durata	Non supportato: controllo manuale	4.5	3.5
[CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per gli AWS Management Console errori di autenticazione	Non supportato: controllo manuale	4.6	3.6

ID e titolo di controllo	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione programmata delle chiavi gestite dal cliente	Non supportato: controllo manuale	4.7	3.7
[CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3	Non supportato: controllo manuale	4.8	3.8
[CloudWatch.9] Assicurati che esistano un filtro metrico di log e un allarme per le AWS Config modifiche alla configurazione	Non supportato: controllo manuale	4.9	3.9
[CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza	Non supportato: controllo manuale	4.10	3,10
[CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)	Non supportato: controllo manuale	4.11	3,11
[CloudWatch.12] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche ai gateway di rete	Non supportato: controllo manuale	4.12	3,12

ID e titolo di controllo	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte	Non supportato: controllo manuale	4.13	3.13
[CloudWatch.14] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche al VPC	Non supportato: controllo manuale	4.14	3,14
[Config.1] AWS Config dovrebbe essere abilitato	3.3	3.5	2.5
[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita	5.4	5.3	4.3
[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC	3.7	3.9	2.9
[EC2.7] La crittografia predefinita di EBS deve essere abilitata	2.2.1	2.2.1	Non supportato
[EC2.8] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)	5.6	Non supportato	Non supportato
[EC2.13] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22	Non supportato: sostituito dai requisiti 5.2 e 5.3	Non supportato: sostituito dai requisiti 5.2 e 5.3	4.1
[EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389	Non supportato: sostituito dai requisiti 5.2 e 5.3	Non supportato: sostituito dai requisiti 5.2 e 5.3	4.2

ID e titolo di controllo	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso dalla porta 0.0.0.0/0 alla porta 22 o alla porta 3389	5.1	5.1	Non supportato
[EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da 0.0.0.0/0 alle porte di amministrazione remota del server	5.2	Non supportato	Non supportato
[EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server	5.3	Non supportato	Non supportato
[EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS	2.4.1	Non supportato	Non supportato
[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi	Non supportato	1.16	1.22
[IAM.2] Gli utenti IAM non devono avere policy IAM allegate	1.15	Non supportato	1.16
[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno	1.14	1.14	1.4
[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere	1.4	1.4	1.12

ID e titolo di controllo	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[IAM.5] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console	1.10	1.10	1.2
[IAM.6] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root	1.6	1.6	1.14
[IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse	Non supportato, vedi invece [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse	Non supportato, vedi [IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse invece	1.3
[IAM.9] L'MFA deve essere abilitata per l'utente root	1.5	1.5	1.13
[IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	1.5
[IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	1.6
[IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	1,7
[IAM.14] Assicurati che la politica delle password IAM richieda almeno un numero	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	1.8

ID e titolo di controllo	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14	1.8	1.8	1.9
[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password	1.9	1.9	1.10
[IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	1.11
[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support	1,17	1,17	1.2
[IAM.20] Evita l'uso dell'utente root	Non supportato: il CIS ha rimosso questo requisito	Non supportato: il CIS ha rimosso questo requisito	1.1
[IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse	1.12	1.12	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[IAM.26] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi	1.19	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive

ID e titolo di controllo	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[IAM.27] Le identità IAM non devono avere la policy allegata AWSCloudShellFullAccess	1.22	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato	1.20	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[KMS.4] la rotazione dei tasti dovrebbe essere abilitata AWS KMS	3.6	3.8	2.8
[Macie.1] Amazon Macie dovrebbe essere abilitato	Non supportato: controllo manuale	Non supportato: controllo manuale	Non supportato: controllo manuale
[RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, in base alla durata PubliclyAccessible AWS Config	2.3.3	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[RDS.3] Le istanze database RDS devono avere la crittografia dei dati inattivi abilitata	2.3.1	2.3.1	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive

ID e titolo di controllo	Requisito CIS v3.0.0	Requisito CIS v1.4.0	Requisito CIS v1.2.0
[RDS.13] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati	2.3.2	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[S3.1] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate	2.1.4	2.1.5	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[S3.5] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL	2.1.1	2.1.2	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico	2.1.4	2.1.5	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive
[S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata	2.1.2	2.1.3	Non supportato: il CIS ha aggiunto questo requisito nelle versioni successive

ARN per CIS Foundations Benchmark AWS

Quando abiliti una o più versioni di CIS AWS Foundations Benchmark, inizierai a ricevere i risultati nel AWS Security Finding Format (ASFF). In ASFF, ogni versione utilizza il seguente Amazon Resource Name (ARN):

Benchmark CIS Foundations v3.0.0 AWS

```
arn:aws::securityhub::standards/cis-aws-foundations-benchmark/v/3.0.0
```

Benchmark CIS AWS Foundations v1.4.0

```
arn:aws::securityhub::standards/cis-aws-foundations-benchmark/v/1.4.0
```

Benchmark CIS Foundations v1.2.0 AWS

```
arn:aws::securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0
```

Puoi utilizzare il [GetEnabledStandards](#) funzionamento dell'API Security Hub per scoprire l'ARN di uno standard abilitato.

Note

Quando abiliti una versione di CIS AWS Foundations Benchmark, Security Hub può impiegare fino a 18 ore per generare risultati per i controlli che utilizzano la stessa regola AWS Config collegata ai servizi dei controlli abilitati in altri standard abilitati. Per ulteriori informazioni, consulta [Pianificazione dell'esecuzione dei controlli di sicurezza](#).

I campi di ricerca sono diversi se si attivano i risultati dei controlli consolidati. Per ulteriori informazioni su queste differenze, consulta [Impatto del consolidamento sui campi e sui valori ASFF](#). Per esempi di risultati di controllo, vedere [Esempi di risultati del controllo](#).

Requisiti CIS non supportati in Security Hub

Come indicato nella tabella precedente, Security Hub non supporta tutti i requisiti CIS in ogni versione del benchmark CIS Foundations AWS . Molti dei requisiti non supportati possono essere valutati solo manualmente esaminando lo stato delle risorse. AWS

Istituto nazionale di standard e tecnologia (NIST) SP 800-53 Rev. 5

NIST SP 800-53 Rev. 5 è un framework di sicurezza informatica e conformità sviluppato dal National Institute of Standards and Technology (NIST), un'agenzia che fa parte del Dipartimento del Commercio degli Stati Uniti. Questo framework di conformità consente di proteggere la disponibilità, la riservatezza e l'integrità dei sistemi informativi e delle risorse critiche. Le agenzie e gli appaltatori del governo federale degli Stati Uniti devono conformarsi al NIST SP 800-53 per proteggere i propri sistemi, ma le aziende private possono utilizzarlo volontariamente come quadro guida per ridurre i rischi di sicurezza informatica.

Security Hub fornisce controlli che supportano determinati requisiti NIST SP 800-53. Questi controlli vengono valutati tramite controlli di sicurezza automatizzati. I controlli Security Hub non supportano i requisiti NIST SP 800-53 che richiedono controlli manuali. Inoltre, i controlli Security Hub supportano solo i requisiti automatizzati NIST SP 800-53, elencati come Requisiti correlati nei dettagli di ciascun controllo. Scegli un controllo dal seguente elenco per visualizzarne i dettagli. I requisiti correlati non menzionati nei dettagli di controllo non sono attualmente supportati da Security Hub.

A differenza di altri framework, NIST SP 800-53 non è prescrittivo su come valutare i suoi requisiti. Invece, il framework fornisce linee guida e i controlli Security Hub NIST SP 800-53 ne rappresentano la comprensione da parte del servizio.

Se utilizzi l'integrazione di Security Hub con AWS Organizations per gestire centralmente più account e desideri abilitare in batch NIST SP 800-53 su tutti, puoi eseguire [uno script multi-account di Security Hub dall'account amministratore](#).

[Per ulteriori informazioni su NIST SP 800-53 Rev. 5, consultate il NIST Computer Security Resource Center.](#)

Controlli che si applicano a NIST SP 800-53 Rev. 5

[\[Account.1\] Le informazioni di contatto di sicurezza devono essere fornite per un Account AWS](#)

[\[Account.2\] Account AWS deve far parte di un'organizzazione AWS Organizations](#)

[\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)

[\[ApiGateway.1\] API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati](#)

[\[ApiGateway.2\] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend](#)

[\[ApiGateway.3\] Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray](#)

[\[ApiGateway.4\] L'API Gateway deve essere associato a un ACL Web WAF](#)

[\[ApiGateway.5\] I dati della cache dell'API REST API Gateway devono essere crittografati quando sono inattivi](#)

[\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione](#)

[\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages](#)

[\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)

[\[AutoScaling.1\] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB](#)

[\[AutoScaling.2\] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità](#)

[\[AutoScaling.3\] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 \(IMDSv2\)](#)

[\[Autoscaling.5\] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici](#)

[\[AutoScaling.6\] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità](#)

[\[AutoScaling.9\] I gruppi di Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2](#)

[\[Backup.1\] i punti di AWS Backup ripristino devono essere crittografati a riposo](#)

[\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)

[\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)

[\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)

[\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)

[\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)

[\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)

[\[CloudFront.8\] Le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)

[\[CloudFront.9\] Le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)

[\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)

[\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)

[\[CloudTrail.1\] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura](#)

[\[CloudTrail.2\] CloudTrail dovrebbe avere la crittografia a riposo abilitata](#)

[\[CloudTrail.4\] la convalida dei file di CloudTrail registro dovrebbe essere abilitata](#)

[\[CloudTrail.5\] i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch](#)

[\[CloudWatch.15\] gli CloudWatch allarmi devono avere azioni specificate configurate](#)

[\[CloudWatch.16\] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato](#)

[\[CloudWatch.17\] le azioni di CloudWatch allarme devono essere attivate](#)

[\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)

[\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)

[\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)

[\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)

[\[Config.1\] AWS Config dovrebbe essere abilitato](#)

[\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)

[\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)

[\[DMS.6\] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato](#)

[\[DMS.7\] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata](#)

[\[DMS.8\] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata](#)

[\[DMS.9\] Gli endpoint DMS devono utilizzare SSL](#)

[\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)

[\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)

[\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)

[\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)

[\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)

[\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)

[\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)

[\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)

[\[DynamoDB.1\] Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda](#)

[\[DynamoDB.2\] Le tabelle DynamoDB dovrebbero avere il ripristino abilitato point-in-time](#)

[\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)

[\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)

[\[DynamoDB.6\] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata](#)

[\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)

[\[EC2.1\] Gli snapshot di Amazon EBS non devono essere ripristinabili pubblicamente](#)

[\[EC2.2\] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita](#)

[\[EC2.3\] I volumi Amazon EBS collegati devono essere crittografati a riposo](#)

[\[EC2.4\] Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato](#)

[\[EC2.6\] La registrazione del flusso VPC deve essere abilitata in tutti i VPC](#)

[\[EC2.7\] La crittografia predefinita di EBS deve essere abilitata](#)

[\[EC2.8\] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 \(IMDSv2\)](#)

[\[EC2.9\] Le istanze Amazon EC2 non devono avere un indirizzo IPv4 pubblico](#)

[\[EC2.10\] Amazon EC2 deve essere configurato per utilizzare endpoint VPC creati per il servizio Amazon EC2](#)

[\[EC2.12\] Gli EIP Amazon EC2 non utilizzati devono essere rimossi](#)

[\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o :/0 alla porta 22](#)

[\[EC2.15\] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici](#)

[\[EC2.16\] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse](#)

[\[EC2.17\] Le istanze Amazon EC2 non devono utilizzare più ENI](#)

[\[EC2.18\] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate](#)

[\[EC2.19\] I gruppi di sicurezza non devono consentire l'accesso illimitato alle porte ad alto rischio](#)

[\[EC2.20\] Entrambi i tunnel VPN per una connessione VPN da sito a sito devono essere AWS attivi](#)

[\[EC2.21\] Gli ACL di rete non dovrebbero consentire l'ingresso dalla porta 0.0.0.0/0 alla porta 22 o alla porta 3389](#)

[\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)

[\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)

[\[EC2.25\] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete](#)

[\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)

[\[EC2.51\] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata](#)

[\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)

[\[ECR.2\] I repository privati ECR devono avere l'immutabilità dei tag configurata](#)

[\[ECR.3\] I repository ECR devono avere almeno una politica del ciclo di vita configurata](#)

[\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)

[\[ECS.2\] Ai servizi ECS non devono essere assegnati automaticamente indirizzi IP pubblici](#)

[\[ECS.3\] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host](#)

[\[ECS.4\] I contenitori ECS devono essere eseguiti come non privilegiati](#)

[\[ECS.5\] I contenitori ECS devono essere limitati all'accesso in sola lettura ai filesystem root](#)

[\[ECS.8\] I segreti non devono essere passati come variabili di ambiente del contenitore](#)

[\[ECS.9\] Le definizioni delle attività ECS devono avere una configurazione di registrazione](#)

[\[ECS.10\] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate](#)

[\[ECS.12\] I cluster ECS devono utilizzare Container Insights](#)

[\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)

[\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)

[\[EFS.3\] I punti di accesso EFS devono applicare una directory principale](#)

[\[EFS.4\] I punti di accesso EFS devono applicare un'identità utente](#)

[\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)

[\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)

[\[EKS.2\] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata](#)

[\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)

[\[EKS.8\] I cluster EKS devono avere la registrazione di controllo abilitata](#)

[\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)

[\[ElastiCache.2\] ElastiCache per i cluster di cache Redis dovrebbe avere l'aggiornamento automatico della versione secondaria abilitato](#)

[\[ElastiCache.3\] ElastiCache per i gruppi di replica Redis dovrebbe avere il failover automatico abilitato](#)

[\[ElastiCache.4\] ElastiCache per i gruppi di replica Redis deve essere crittografato a riposo](#)

[\[ElastiCache.5\] ElastiCache per i gruppi di replica Redis devono essere crittografati in transito](#)

[\[ElastiCache.6\] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH](#)

[\[ElastiCache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito](#)

[\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)

[\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)

[\[ELB.1\] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS](#)

[\[ELB.2\] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager](#)

[\[ELB.3\] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS](#)

[\[ELB.4\] L'Application Load Balancer deve essere configurato per eliminare le intestazioni http](#)

[\[ELB.5\] La registrazione delle applicazioni e dei sistemi Classic Load Balancers deve essere abilitata](#)

[\[ELB.6\] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata](#)

[\[ELB.7\] I Classic Load Balancer devono avere il drenaggio della connessione abilitato](#)

[\[ELB.8\] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita con una durata elevata AWS Config](#)

[\[ELB.9\] I Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato](#)

[\[ELB.10\] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità](#)

[\[ELB.12\] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)

[\[ELB.13\] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità](#)

[\[ELB.14\] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)

[\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF](#)

[\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)

[\[EMR.2\] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata](#)

[\[ES.1\] I domini Elasticsearch devono avere la crittografia a riposo abilitata](#)

[\[ES.2\] I domini Elasticsearch non devono essere accessibili al pubblico](#)

[\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)

[\[ES.4\] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch](#)

[\[ES.5\] I domini Elasticsearch devono avere la registrazione di controllo abilitata](#)

[\[ES.6\] I domini Elasticsearch devono avere almeno tre nodi di dati](#)

[\[ES.7\] I domini Elasticsearch devono essere configurati con almeno tre nodi master dedicati](#)

[\[ES.8\] Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)

[\[EventBridge.3\] i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata](#)

[\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)

[\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)

[\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)

[\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)

[\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)

[\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)

[\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)

[\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)

[\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)

[\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)

[\[IAM.7\] Le politiche relative alle password per gli utenti IAM dovrebbero avere configurazioni solide](#)

[\[IAM.8\] Le credenziali utente IAM non utilizzate devono essere rimosse](#)

[\[IAM.9\] L'MFA deve essere abilitata per l'utente root](#)

[\[IAM.19\] L'MFA deve essere abilitata per tutti gli utenti IAM](#)

[\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)

[\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)

[\[KMS.1\] Le politiche gestite dai clienti di IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS](#)

[\[KMS.2\] I principali IAM non devono disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS](#)

[\[KMS.3\] AWS KMS keys non deve essere eliminato involontariamente](#)

[\[KMS.4\] la rotazione dei tasti dovrebbe essere abilitata AWS KMS](#)

[\[Lambda.1\] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico](#)

[\[Lambda.2\] Le funzioni Lambda devono utilizzare runtime supportati](#)

[\[Lambda.3\] Le funzioni Lambda devono trovarsi in un VPC](#)

[\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)

[\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)

[\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato](#)

[\[MSK.1\] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker](#)

[\[MSK.2\] Per i cluster MSK dovrebbe essere configurato un monitoraggio avanzato](#)

[\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)

[\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)

[\[MQ.5\] I broker ActiveMQ devono utilizzare la modalità di distribuzione attiva/standby](#)

[\[MQ.6\] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster](#)

[\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)

[\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)

[\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)

[\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)

[\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)

[\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)

[\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)

[\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)

[\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)

[\[NetworkFirewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità](#)

[\[NetworkFirewall.2\] La registrazione del Network Firewall deve essere abilitata](#)

[\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)

[\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)

[\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)

[\[NetworkFirewall.6\] Il gruppo di regole Stateless Network Firewall non deve essere vuoto](#)

[\[NetworkFirewall.9\] I firewall Network Firewall devono avere la protezione da eliminazione abilitata](#)

[I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)

[I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)

[I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)

[La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)

[I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)

[I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)

[I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)

[\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)

[Nei OpenSearch domini \[Opensearch.10\] deve essere installato l'ultimo aggiornamento software](#)

[I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)

[L'autorità di certificazione AWS Private CA principale \[PCA.1\] deve essere disabilitata](#)

[\[RDS.1\] L'istanza RDS deve essere privata](#)

[\[RDS.2\] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, in base alla durata PubliclyAccessible AWS Config](#)

[\[RDS.3\] Le istanze database RDS devono avere la crittografia dei dati inattivi abilitata](#)

[\[RDS.4\] Le istantanee dei cluster RDS e le istantanee del database devono essere crittografate quando sono inattive](#)

[\[RDS.5\] Le istanze DB RDS devono essere configurate con più zone di disponibilità](#)

[\[RDS.6\] Il monitoraggio avanzato deve essere configurato per le istanze DB RDS](#)

[\[RDS.7\] I cluster RDS devono avere la protezione da eliminazione abilitata](#)

[\[RDS.8\] Le istanze DB RDS devono avere la protezione da eliminazione abilitata](#)

[\[RDS.9\] Le istanze DB RDS devono pubblicare i log nei registri CloudWatch](#)

[\[RDS.10\] L'autenticazione IAM deve essere configurata per le istanze RDS](#)

[\[RDS.11\] Le istanze RDS devono avere i backup automatici abilitati](#)

[\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)

[\[RDS.13\] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati](#)

[\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)

[\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)

[\[RDS.16\] I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee](#)

[\[RDS.17\] Le istanze DB RDS devono essere configurate per copiare i tag nelle istantanee](#)

[\[RDS.18\] Le istanze RDS devono essere distribuite in un VPC](#)

[\[RDS.19\] Le sottoscrizioni esistenti per le notifiche di eventi RDS devono essere configurate per gli eventi critici del cluster](#)

[\[RDS.20\] Le sottoscrizioni di notifica degli eventi RDS esistenti devono essere configurate per gli eventi critici delle istanze di database](#)

[\[RDS.21\] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici del gruppo di parametri del database](#)

[\[RDS.22\] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici dei gruppi di sicurezza del database](#)

[\[RDS.23\] Le istanze RDS non devono utilizzare una porta predefinita del motore di database](#)

[\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)

[\[RDS.25\] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato](#)

[\[RDS.26\] Le istanze DB RDS devono essere protette da un piano di backup](#)

[\[RDS.27\] I cluster RDS DB devono essere crittografati quando sono inattivi](#)

[\[RDS.34\] I cluster Aurora MySQL DB devono pubblicare i log di controllo nei registri CloudWatch](#)

[\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)

[\[Redshift.1\] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico](#)

[\[Redshift.2\] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito](#)

[\[Redshift.3\] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate](#)

[\[Redshift.4\] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata](#)

[\[Redshift.6\] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati](#)

[\[Redshift.7\] I cluster Redshift devono utilizzare un routing VPC avanzato](#)

[\[Redshift.8\] I cluster Amazon Redshift non devono utilizzare il nome utente predefinito di amministratore](#)

[\[Redshift.9\] I cluster Redshift non devono utilizzare il nome di database predefinito](#)

[\[Redshift.10\] I cluster Redshift devono essere crittografati a riposo](#)

[\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)

[\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)

[\[S3.2\] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura](#)

[\[S3.3\] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura](#)

[\[S3.5\] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL](#)

[\[S3.6\] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS](#)

[\[S3.7\] I bucket S3 per uso generico devono utilizzare la replica tra regioni](#)

[\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)

[\[S3.9\] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata](#)

[\[S3.10\] I bucket generici S3 con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita](#)

[\[S3.11\] I bucket generici S3 devono avere le notifiche degli eventi abilitate](#)

[\[S3.12\] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3](#)

[\[S3.13\] I bucket generici S3 devono avere configurazioni del ciclo di vita](#)

[\[S3.14\] I bucket generici S3 devono avere il controllo delle versioni abilitato](#)

[\[S3.15\] I bucket generici S3 devono avere Object Lock abilitato](#)

[\[S3.17\] I bucket generici S3 devono essere crittografati quando sono inattivi con AWS KMS keys](#)

[\[S3.19\] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)

[\[S3.20\] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata](#)

[\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)

[\[SageMaker.2\] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato](#)

[\[SageMaker.3\] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook](#)

[\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)

[\[SecretsManager.1\] I segreti di Secrets Manager devono avere la rotazione automatica abilitata](#)

[\[SecretsManager.2\] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente](#)

[\[SecretsManager.3\] Rimuovi i segreti inutilizzati di Secrets Manager](#)

[\[SecretsManager.4\] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni](#)

[\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)

[\[SNS.1\] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS](#)

[\[SQS.1\] Le code di Amazon SQS devono essere crittografate quando sono inattive](#)

[\[SSM.1\] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager](#)

[\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)

[\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)

[\[SSM.4\] I documenti SSM non devono essere pubblici](#)

[\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)

[\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)

[\[WAF.2\] Le regole regionali AWS WAF classiche devono avere almeno una condizione](#)

[\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)

[\[WAF.4\] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

[\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)

[\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)

[\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

[\[WAF.10\] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole](#)

[\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

[Le regole \[WAF.12\] devono avere le metriche abilitate AWS WAF CloudWatch](#)

Payment Card Industry Data Security Standard (PCI DSS)

Il Payment Card Industry Data Security Standard (PCI DSS) di Security Hub fornisce una serie di best practice di AWS sicurezza per la gestione dei dati dei titolari di carta. È possibile utilizzare questo standard per scoprire le vulnerabilità di sicurezza nelle risorse che gestiscono i dati dei titolari di carta. Security Hub attualmente analizza i controlli a livello di account. Ti consigliamo di abilitare questi controlli in tutti gli account che dispongono di risorse che archiviano, elaborano o trasmettono i dati dei titolari di carta.

Questo standard è stato convalidato da AWS Security Assurance Services LLC (AWS SAS), un team di Qualified Security Assessors (QSA) certificati per fornire linee guida PCI DSS e valutazioni dal PCI DSS Security Standards Council (PCI SSC). AWS SAS ha confermato che i controlli automatici possono aiutare il cliente a prepararsi per una valutazione PCI DSS.

Questa pagina elenca gli ID e i titoli dei controlli di sicurezza. Nelle regioni cinesi AWS GovCloud (US) Region e cinesi, vengono utilizzati ID e titoli di controllo specifici per gli standard. Per una mappatura degli ID e dei titoli dei controlli di sicurezza agli ID e ai titoli di controllo specifici degli standard, vedere. [In che modo il consolidamento influisce sugli ID e sui titoli di controllo](#)

Controlli che si applicano al PCI DSS

[\[AutoScaling.1\] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB](#)

[\[CloudTrail.2\] CloudTrail dovrebbe avere la crittografia a riposo abilitata](#)

[\[CloudTrail.3\] Almeno un trail deve essere abilitato CloudTrail](#)

[\[CloudTrail.4\] la convalida dei file di CloudTrail registro dovrebbe essere abilitata](#)

[\[CloudTrail.5\] i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch](#)

[\[CloudWatch.1\] Dovrebbero esistere un filtro logmetrico e un allarme per l'utilizzo da parte dell'utente «root»](#)

[\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)

[\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)

[\[Config.1\] AWS Config dovrebbe essere abilitato](#)

[\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)

[\[EC2.1\] Gli snapshot di Amazon EBS non devono essere ripristinabili pubblicamente](#)

[\[EC2.2\] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita](#)

[\[EC2.6\] La registrazione del flusso VPC deve essere abilitata in tutti i VPC](#)

[\[EC2.12\] Gli EIP Amazon EC2 non utilizzati devono essere rimossi](#)

[\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: /0 alla porta 22](#)

[\[ELB.1\] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS](#)

[\[ES.1\] I domini Elasticsearch devono avere la crittografia a riposo abilitata](#)

[\[ES.2\] I domini Elasticsearch non devono essere accessibili al pubblico](#)

[\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)

[\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)

[\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)

[\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)

[\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)

[\[IAM.8\] Le credenziali utente IAM non utilizzate devono essere rimosse](#)

[\[IAM.9\] L'MFA deve essere abilitata per l'utente root](#)

[\[IAM.10\] Le politiche relative alle password per gli utenti IAM dovrebbero avere durate elevate AWS Config](#)

[\[IAM.19\] L'MFA deve essere abilitata per tutti gli utenti IAM](#)

[\[KMS.4\] la rotazione dei tasti dovrebbe essere abilitata AWS KMS](#)

[\[Lambda.1\] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico](#)

[\[Lambda.3\] Le funzioni Lambda devono trovarsi in un VPC](#)

[I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)

[I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)

[\[RDS.1\] L'istanza RDS deve essere privata](#)

[\[RDS.2\] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, in base alla durata PubliclyAccessible AWS Config](#)

[\[Redshift.1\] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico](#)

[\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)

[\[S3.2\] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura](#)

[\[S3.3\] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura](#)

[\[S3.5\] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL](#)

[\[S3.7\] I bucket S3 per uso generico devono utilizzare la replica tra regioni](#)

[\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)

[\[SSM.1\] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager](#)

[\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)

[\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)

AWS Standard di etichettatura delle risorse

Questa sezione fornisce informazioni sul AWS Resource Tagging Standard.

Note

Il AWS Resource Tagging Standard non è disponibile in Canada occidentale (Calgary), Cina e. AWS GovCloud (US)

Cos'è il AWS Resource Tagging Standard?

I tag sono coppie di chiavi e valori che fungono da metadati per l'organizzazione AWS delle risorse. Con la maggior parte AWS delle risorse, hai la possibilità di aggiungere tag quando crei la risorsa o dopo la creazione. Esempi di risorse includono una CloudFront distribuzione Amazon, un'istanza Amazon Elastic Compute Cloud (Amazon EC2) o un accesso segreto. AWS Secrets Manager

Con i tag è possibile a gestire, identificare, organizzare, cercare e filtrare le risorse.

Ogni tag è costituito da due parti:

- Una chiave del tag (ad esempio, `CostCenter`, `Environment`, o `Project`). Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.
- Un valore di tag (ad esempio, `111122223333` o `Production`). Analogamente alle chiavi dei tag, i valori dei tag prevedono una distinzione tra lettere maiuscole e minuscole.

È possibile utilizzare i tag per suddividere le risorse in categorie in base allo scopo, al proprietario, all'ambiente o ad altri criteri.

Per istruzioni sull'aggiunta di tag alle AWS risorse, consulta [Come aggiungere tag alla AWS risorsa](#) nella Guida per l'utente AWS di Security Hub.

Il AWS Resource Tagging Standard, sviluppato da AWS Security Hub, ti aiuta a identificare rapidamente se in alcune delle tue AWS risorse mancano le chiavi dei tag. Puoi personalizzare il `requiredTagKeys` parametro per specificare chiavi di tag specifiche che i controlli controllano. Se non vengono forniti tag specifici, i controlli controllano semplicemente l'esistenza di almeno una chiave di tag.

Quando abiliti il AWS Resource Tagging Standard, inizierai a ricevere i risultati nel AWS Security Finding Format (ASFF).

Note

Quando abiliti AWS Resource Tagging Standard, Security Hub può impiegare fino a 18 ore per generare risultati per i controlli che utilizzano la stessa regola AWS Config collegata ai servizi dei controlli abilitati in altri standard abilitati. Per ulteriori informazioni, consulta [Pianificazione dell'esecuzione dei controlli di sicurezza](#).

Questo standard ha il seguente Amazon Resource Name (ARN):.

```
arn:aws:securityhub:region::standards/aws-resource-tagging-standard/v/1.0.0
```

Puoi anche utilizzare il [GetEnabledStandards](#) funzionamento dell'API Security Hub per scoprire l'ARN di uno standard abilitato.

Controlli del AWS Resource Tagging Standard

Il AWS Resource Tagging Standard include i seguenti controlli. Seleziona un controllo per visualizzarne una descrizione dettagliata.

- [\[ACM.3\] I certificati ACM devono essere etichettati](#)
- [\[AppSync.4\] Le API AWS AppSync GraphQL devono essere taggate](#)
- [\[Athena.2\] I cataloghi di dati Athena devono essere etichettati](#)
- [\[Athena.3\] I gruppi di lavoro Athena devono essere etichettati](#)
- [\[AutoScaling.10\] I gruppi di Auto Scaling EC2 devono essere etichettati](#)

- [\[Backup.2\] i punti di AWS Backup ripristino devono essere etichettati](#)
- [I AWS Backup vault \[Backup.3\] devono essere etichettati](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[Backup.5\] i piani di AWS Backup backup devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CloudTrail.9\] i percorsi devono essere etichettati CloudTrail](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.2\] I certificati DMS devono essere etichettati](#)
- [\[DMS.3\] Le sottoscrizioni agli eventi DMS devono essere contrassegnate](#)
- [\[DMS.4\] Le istanze di replica DMS devono essere contrassegnate](#)
- [\[DMS.5\] I sottoreti di replica DMS devono essere etichettati](#)
- [\[DynamoDB.5\] Le tabelle DynamoDB devono essere etichettate](#)
- [\[EC2.33\] Gli allegati del gateway di transito EC2 devono essere etichettati](#)
- [\[EC2.34\] Le tabelle delle rotte dei gateway di transito EC2 devono essere etichettate](#)
- [\[EC2.35\] Le interfacce di rete EC2 devono essere etichettate](#)
- [\[EC2.36\] I gateway per i clienti EC2 devono essere etichettati](#)
- [\[EC2.37\] Gli indirizzi IP elastici EC2 devono essere etichettati](#)
- [\[EC2.38\] Le istanze EC2 devono essere etichettate](#)
- [\[EC2.39\] I gateway Internet EC2 devono essere etichettati](#)
- [\[EC2.40\] I gateway NAT EC2 devono essere etichettati](#)
- [\[EC2.41\] Gli ACL di rete EC2 devono essere etichettati](#)
- [\[EC2.42\] Le tabelle di routing EC2 devono essere etichettate](#)
- [\[EC2.43\] I gruppi di sicurezza EC2 devono essere etichettati](#)
- [\[EC2.44\] Le sottoreti EC2 devono essere etichettate](#)
- [\[EC2.45\] I volumi EC2 devono essere etichettati](#)
- [\[EC2.46\] I VPC Amazon devono essere etichettati](#)
- [\[EC2.47\] I servizi endpoint Amazon VPC devono essere etichettati](#)
- [\[EC2.48\] I log di flusso di Amazon VPC devono essere etichettati](#)

- [\[EC2.49\] Le connessioni peering Amazon VPC devono essere etichettate](#)
- [\[EC2.50\] I gateway VPN EC2 devono essere etichettati](#)
- [\[EC2.52\] I gateway di transito EC2 devono essere etichettati](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.13\] I servizi ECS devono essere etichettati](#)
- [\[ECS.14\] I cluster ECS devono essere etichettati](#)
- [\[ECS.15\] Le definizioni delle attività ECS devono essere contrassegnate](#)
- [\[EFS.5\] I punti di accesso EFS devono essere etichettati](#)
- [\[EKS.6\] I cluster EKS devono essere etichettati](#)
- [\[EKS.7\] Le configurazioni dei provider di identità EKS devono essere contrassegnate](#)
- [\[ES.9\] I domini Elasticsearch devono essere etichettati](#)
- [\[EventBridge.2\] i bus EventBridge degli eventi devono essere etichettati](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[Glue.1\] i AWS Glue lavori devono essere etichettati](#)
- [\[GuardDuty.2\] GuardDuty i filtri devono essere etichettati](#)
- [\[GuardDuty.3\] Gli GuardDuty IPSet devono essere etichettati](#)
- [\[GuardDuty.4\] i GuardDuty rilevatori devono essere etichettati](#)
- [\[IAM.23\] Gli analizzatori IAM Access Analyzer devono essere etichettati](#)
- [\[IAM.24\] I ruoli IAM devono essere etichettati](#)
- [\[IAM.25\] Gli utenti IAM devono essere etichettati](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)
- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[Kinesis.2\] Gli stream Kinesis devono essere etichettati](#)
- [\[Lambda.6\] Le funzioni Lambda devono essere etichettate](#)
- [\[MQ.4\] I broker Amazon MQ devono essere etichettati](#)
- [\[NetworkFirewall.7\] I firewall Network Firewall devono essere etichettati](#)

- [\[NetworkFirewall.8\] Le politiche firewall di Network Firewall devono essere etichettate](#)
- [I OpenSearch domini \[Opensearch.9\] devono essere etichettati](#)
- [\[RDS.28\] I cluster RDS DB devono essere etichettati](#)
- [\[RDS.29\] Gli snapshot del cluster RDS DB devono essere etichettati](#)
- [\[RDS.30\] Le istanze DB RDS devono essere etichettate](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[RDS.32\] Gli snapshot RDS DB devono essere etichettati](#)
- [\[RDS.33\] I gruppi di sottoreti RDS DB devono essere etichettati](#)
- [\[Redshift.11\] I cluster Redshift devono essere etichettati](#)
- [\[Redshift.12\] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate](#)
- [\[Redshift.13\] Le istantanee del cluster Redshift devono essere etichettate](#)
- [\[Redshift.14\] I gruppi di sottoreti del cluster Redshift devono essere etichettati](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[SecretsManager.5\] I segreti di Secrets Manager devono essere etichettati](#)
- [\[SES.1\] Gli elenchi di contatti SES devono essere etichettati](#)
- [\[SES.2\] I set di configurazione SES devono essere etichettati](#)
- [\[SNS.3\] Gli argomenti SNS devono essere etichettati](#)
- [\[SQS.2\] Le code SQS devono essere etichettate](#)
- [\[StepFunctions.2\] Le attività di Step Functions devono essere etichettate](#)
- [I AWS Transfer Family flussi di lavoro \[Transfer.1\] devono essere etichettati](#)

Standard gestiti dai servizi

Uno standard gestito dai servizi è uno standard di sicurezza gestito da un altro. Servizio AWS Ad esempio, [Service-Managed Standard: AWS Control Tower è uno standard gestito](#) dai servizi che gestisce. AWS Control Tower Uno standard gestito dai servizi si differenzia da uno standard di sicurezza gestito da AWS Security Hub nei seguenti modi:

- Creazione ed eliminazione standard: è possibile creare ed eliminare uno standard gestito dal servizio con la console o l'API del servizio di gestione oppure con. AWS CLI Finché non crei lo standard nel servizio di gestione in uno di questi modi, lo standard non viene visualizzato nella console di Security Hub e non è accessibile tramite l'API Security Hub o AWS CLI.

- Nessuna attivazione automatica dei controlli: quando si crea uno standard gestito dal servizio, Security Hub e il servizio di gestione non abilitano automaticamente i controlli che si applicano allo standard. Inoltre, quando Security Hub rilascia nuovi controlli per lo standard, questi non vengono abilitati automaticamente. Si tratta di un allontanamento dagli standard gestiti da Security Hub. Per ulteriori informazioni sul modo consueto di configurare i controlli in Security Hub, vedere [Visualizzazione e gestione dei controlli di sicurezza](#).
- Abilitazione e disabilitazione dei controlli: consigliamo di abilitare e disabilitare i controlli nel servizio di gestione per evitare deviazioni.
- Disponibilità dei controlli: il servizio di gestione sceglie quali controlli sono disponibili come parte dello standard di gestione dei servizi. I controlli disponibili possono includere tutti o un sottoinsieme dei controlli esistenti del Security Hub.

Dopo che il servizio di gestione ha creato lo standard gestito dal servizio e reso disponibili i relativi controlli, è possibile accedere ai risultati del controllo, agli stati dei controlli e al punteggio di sicurezza standard nella console Security Hub, nell'API Security Hub o. AWS CLI Alcune o tutte queste informazioni potrebbero essere disponibili anche nel servizio di gestione.

Seleziona uno standard gestito dal servizio dall'elenco seguente per visualizzare ulteriori dettagli al riguardo.

Standard gestiti dai servizi

- [Standard di gestione dei servizi: AWS Control Tower](#)

Standard di gestione dei servizi: AWS Control Tower

Questa sezione fornisce informazioni su Service-Managed Standard: AWS Control Tower

Che cos'è Service-Managed Standard? AWS Control Tower

Questo standard è progettato per gli utenti di AWS Security Hub e AWS Control Tower. Ti consente di configurare i controlli proattivi AWS Control Tower insieme ai controlli di rilevamento di Security Hub nel AWS Control Tower servizio.

I controlli proattivi aiutano a garantire il Account AWS mantenimento della conformità perché segnalano le azioni che possono portare a violazioni o configurazioni errate delle politiche. I controlli investigativi rilevano la non conformità delle risorse (ad esempio, configurazioni errate) all'interno dell'azienda. Account AWS Abilitando controlli proattivi e investigativi per l' AWS ambiente, è possibile migliorare il livello di sicurezza nelle diverse fasi di sviluppo.

i Tip

Gli standard gestiti dai servizi differiscono dagli standard gestiti da AWS Security Hub. Ad esempio, è necessario creare ed eliminare uno standard gestito dai servizi nel servizio di gestione. Per ulteriori informazioni, consulta [Standard gestiti dai servizi](#).

Nella console e nell'API di Security Hub, puoi visualizzare Service-Managed Standard: AWS Control Tower insieme ad altri standard di Security Hub.

Creazione dello standard

Questo standard è disponibile solo se lo crei in AWS Control Tower. AWS Control Tower crea lo standard quando si attiva per la prima volta un controllo applicabile utilizzando uno dei seguenti metodi:

- AWS Control Tower console
- AWS Control Tower API (chiama l'[EnableControlAPI](#))
- AWS CLI (esegui il [enable-control](#) comando)

I controlli del Security Hub sono identificati nella AWS Control Tower console come SH. **ControlID** (ad esempio, SH). CodeBuild.1).

Quando crei lo standard, se non hai già abilitato Security Hub, abilita AWS Control Tower anche Security Hub per te.

Se non lo hai configurato AWS Control Tower, non puoi visualizzare o accedere a questo standard nella console Security Hub, nell'API Security Hub o AWS CLI. Anche se è stato configurato AWS Control Tower, non è possibile visualizzare o accedere a questo standard in Security Hub senza prima aver creato lo standard AWS Control Tower utilizzando uno dei metodi precedenti.

Questo standard è disponibile solo [Regioni AWS dove AWS Control Tower è disponibile](#), tra cui AWS GovCloud (US).

Abilitazione e disabilitazione dei controlli nello standard

Dopo aver creato lo standard nella AWS Control Tower console, è possibile visualizzare lo standard e i controlli disponibili in entrambi i servizi.

Dopo aver creato lo standard per la prima volta, non ci sono controlli che vengono abilitati automaticamente. Inoltre, quando Security Hub aggiunge nuovi controlli, questi non vengono abilitati automaticamente per Service-Managed Standard. È necessario abilitare e disabilitare i controlli per lo standard in AWS Control Tower utilizzando uno dei seguenti metodi:

- AWS Control Tower console
- AWS Control Tower API (chiama le [DisableControlAPI](#) [EnableControl](#)and)
- AWS CLI (esegui i [disable-control](#)comandi [enable-control](#)and)

Quando si modifica lo stato di attivazione di un controllo in AWS Control Tower, la modifica si riflette anche in Security Hub.

Tuttavia, la disabilitazione di un controllo in Security Hub che è abilitato in AWS Control Tower comporta una deriva del controllo. Lo stato del controllo in AWS Control Tower viene visualizzato come `Drifted`. È possibile risolvere questa deriva selezionando [Re-register OU](#) nella AWS Control Tower console oppure disabilitando e riabilitando il controllo AWS Control Tower utilizzando uno dei metodi precedenti.

Il completamento delle azioni di attivazione e disabilitazione in aiuta a evitare la deriva del controllo. AWS Control Tower

Quando abiliti o disabiliti i controlli in AWS Control Tower, l'azione si applica a tutti gli account e alle regioni. Se abiliti e disabiliti i controlli in Security Hub (non consigliato per questo standard), l'azione si applica solo all'account e alla regione correnti.

Note

[La configurazione centrale](#) non può essere utilizzata per gestire Service-Managed Standard. AWS Control Tower Se utilizzi la configurazione centrale, puoi utilizzare solo il AWS Control Tower servizio per abilitare e disabilitare i controlli di questo standard per un account gestito centralmente.

Visualizzazione dello stato di attivazione e dello stato di controllo

È possibile visualizzare lo stato di attivazione di un controllo utilizzando uno dei seguenti metodi:

- Console Security Hub, API Security Hub o AWS CLI
- AWS Control Tower console

- AWS Control Tower API per visualizzare un elenco di controlli abilitati (chiamata l'[ListEnabledControls](#)API)
- AWS CLI per visualizzare un elenco di controlli abilitati (esegui il [list-enabled-controls](#) comando)

Un controllo che disabiliti AWS Control Tower ha lo stato di attivazione in Security Hub Disabled a meno che non abiliti esplicitamente tale controllo in Security Hub.

Security Hub calcola lo stato del controllo in base allo stato del flusso di lavoro e allo stato di conformità dei risultati del controllo. Per ulteriori informazioni sullo stato di attivazione e sullo stato di controllo, vedere [Visualizzazione dei dettagli di un controllo](#)

In base agli stati di controllo, Security Hub calcola un [punteggio di sicurezza](#) per Service-Managed Standard. AWS Control Tower Questo punteggio è disponibile solo in Security Hub. Inoltre, puoi visualizzare i [risultati del controllo](#) solo in Security Hub. Il punteggio di sicurezza standard e i risultati del controllo non sono disponibili in AWS Control Tower.

Note

Quando abiliti i controlli per Service-Managed Standard: AWS Control Tower, Security Hub può impiegare fino a 18 ore per generare risultati per i controlli che utilizzano una regola esistente collegata al AWS Config servizio. Potresti avere regole collegate ai servizi esistenti se hai abilitato altri standard e controlli in Security Hub. Per ulteriori informazioni, consulta [Pianificazione dell'esecuzione dei controlli di sicurezza](#).

Eliminazione dello standard

È possibile eliminare questo standard disattivando tutti i controlli applicabili utilizzando uno dei seguenti metodi: AWS Control Tower

- AWS Control Tower console
- AWS Control Tower API (chiamata l'[DisableControl](#)API)
- AWS CLI (esegui il [disable-control](#) comando)

La disabilitazione di tutti i controlli elimina lo standard in tutti gli account gestiti e nelle regioni governate in. AWS Control Tower L'eliminazione dello standard in lo AWS Control Tower rimuove

dalla pagina Standard della console di Security Hub e non è più possibile accedervi utilizzando l'API Security Hub o AWS CLI.

Note

La disabilitazione di tutti i controlli dallo standard in Security Hub non disabilita o elimina lo standard.

La disabilitazione del servizio Security Hub rimuove Service-Managed Standard AWS Control Tower e tutti gli altri standard che hai abilitato.

Formato di campo di ricerca per Service-Managed Standard: AWS Control Tower

Quando crei Service-Managed Standard: AWS Control Tower e ne abiliti i controlli, inizierai a ricevere i risultati del controllo in Security Hub. Security Hub riporta i risultati del controllo in [AWS Formato ASFF \(Security Finding Format\)](#). Questi sono i valori ASFF per Amazon Resource Name (ARN) di questo standard e: GeneratorId

- ARN standard — `arn:aws:us-east-1:securityhub:::standards/service-managed-aws-control-tower/v/1.0.0`
- GeneratorId — `service-managed-aws-control-tower/v/1.0.0/CodeBuild.1`

Per un esempio di risultato per Service-Managed Standard: AWS Control Tower, vedere. [Esempi di risultati del controllo](#)

Controlli che si applicano a Service-Managed Standard: AWS Control Tower

Service-Managed Standard: AWS Control Tower supporta un sottoinsieme di controlli che fanno parte dello standard AWS Foundational Security Best Practices (FSBP). Scegliete un controllo dalla tabella seguente per visualizzarne le informazioni, inclusi i passaggi di correzione per i risultati non riusciti.

L'elenco seguente mostra i controlli disponibili per Service-Managed Standard: AWS Control Tower. I limiti regionali sui controlli corrispondono ai limiti regionali sui controlli corollari dello standard FSBP. Questo elenco mostra gli ID dei controlli di sicurezza indipendenti dagli standard. Nella AWS Control Tower console, gli ID di controllo sono formattati come SH. **ControlID** (ad esempio SH.CodeBuild.1). In Security Hub, se [i risultati del controllo consolidato](#) sono disattivati nel tuo account, il `ProductFields.ControlId` campo utilizza l'ID di controllo standard. L'ID di controllo basato su standard è formattato come CT. **ControlId** (ad esempio, CT.CodeBuild.1).

- [\[Account.1\] Le informazioni di contatto di sicurezza devono essere fornite per un Account AWS](#)
- [\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)
- [\[ACM.2\] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit](#)
- [\[ApiGateway.1\] API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati](#)
- [\[ApiGateway.2\] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend](#)
- [\[ApiGateway.3\] Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray](#)
- [\[ApiGateway.4\] L'API Gateway deve essere associato a un ACL Web WAF](#)
- [\[ApiGateway.5\] I dati della cache dell'API REST API Gateway devono essere crittografati quando sono inattivi](#)
- [\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione](#)
- [\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages](#)
- [\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)
- [\[AutoScaling.1\] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB](#)
- [\[AutoScaling.2\] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità](#)
- [\[AutoScaling.3\] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 \(IMDSv2\)](#)
- [\[Autoscaling.5\] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici](#)
- [\[AutoScaling.6\] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità](#)
- [\[AutoScaling.9\] I gruppi di Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2](#)
- [\[CloudTrail.1\] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura](#)
- [\[CloudTrail.2\] CloudTrail dovrebbe avere la crittografia a riposo abilitata](#)
- [\[CloudTrail.4\] la convalida dei file di CloudTrail registro dovrebbe essere abilitata](#)

- [\[CloudTrail.5\] i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch](#)
- [\[CloudTrail.6\] Assicurati che il bucket S3 utilizzato per archiviare i log non sia accessibile al pubblico CloudTrail](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)
- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)
- [\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)
- [\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)
- [\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)
- [\[DMS.9\] Gli endpoint DMS devono utilizzare SSL](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DynamoDB.1\] Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda](#)
- [\[DynamoDB.2\] Le tabelle DynamoDB dovrebbero avere il ripristino abilitato point-in-time](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[EC2.1\] Gli snapshot di Amazon EBS non devono essere ripristinabili pubblicamente](#)
- [\[EC2.2\] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita](#)
- [\[EC2.3\] I volumi Amazon EBS collegati devono essere crittografati a riposo](#)
- [\[EC2.4\] Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato](#)
- [\[EC2.6\] La registrazione del flusso VPC deve essere abilitata in tutti i VPC](#)
- [\[EC2.7\] La crittografia predefinita di EBS deve essere abilitata](#)
- [\[EC2.8\] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 \(IMDSv2\)](#)
- [\[EC2.9\] Le istanze Amazon EC2 non devono avere un indirizzo IPv4 pubblico](#)

- [\[EC2.10\] Amazon EC2 deve essere configurato per utilizzare endpoint VPC creati per il servizio Amazon EC2](#)
- [\[EC2.15\] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici](#)
- [\[EC2.16\] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse](#)
- [\[EC2.17\] Le istanze Amazon EC2 non devono utilizzare più ENI](#)
- [\[EC2.18\] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate](#)
- [\[EC2.19\] I gruppi di sicurezza non devono consentire l'accesso illimitato alle porte ad alto rischio](#)
- [\[EC2.20\] Entrambi i tunnel VPN per una connessione VPN da sito a sito devono essere AWS attivi](#)
- [\[EC2.21\] Gli ACL di rete non dovrebbero consentire l'ingresso dalla porta 0.0.0.0/0 alla porta 22 o alla porta 3389](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.25\] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete](#)
- [\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)
- [\[ECR.2\] I repository privati ECR devono avere l'immutabilità dei tag configurata](#)
- [\[ECR.3\] I repository ECR devono avere almeno una politica del ciclo di vita configurata](#)
- [\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)
- [\[ECS.2\] Ai servizi ECS non devono essere assegnati automaticamente indirizzi IP pubblici](#)
- [\[ECS.3\] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host](#)
- [\[ECS.4\] I contenitori ECS devono essere eseguiti come non privilegiati](#)
- [\[ECS.5\] I contenitori ECS devono essere limitati all'accesso in sola lettura ai filesystem root](#)
- [\[ECS.8\] I segreti non devono essere passati come variabili di ambiente del contenitore](#)
- [\[ECS.10\] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate](#)
- [\[ECS.12\] I cluster ECS devono utilizzare Container Insights](#)
- [\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)

- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)
- [\[EFS.3\] I punti di accesso EFS devono applicare una directory principale](#)
- [\[EFS.4\] I punti di accesso EFS devono applicare un'identità utente](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.2\] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata](#)
- [\[ElastiCache.3\] ElastiCache per i gruppi di replica Redis dovrebbe avere il failover automatico abilitato](#)
- [\[ElastiCache.4\] ElastiCache per i gruppi di replica Redis deve essere crittografato a riposo](#)
- [\[ElastiCache.5\] ElastiCache per i gruppi di replica Redis devono essere crittografati in transito](#)
- [\[ElastiCache.6\] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[ELB.1\] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS](#)
- [\[ELB.2\] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager](#)
- [\[ELB.3\] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS](#)
- [\[ELB.4\] L'Application Load Balancer deve essere configurato per eliminare le intestazioni http](#)
- [\[ELB.5\] La registrazione delle applicazioni e dei sistemi Classic Load Balancers deve essere abilitata](#)
- [\[ELB.6\] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata](#)
- [\[ELB.7\] I Classic Load Balancer devono avere il drenaggio della connessione abilitato](#)
- [\[ELB.8\] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita con una durata elevata AWS Config](#)
- [\[ELB.9\] I Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato](#)
- [\[ELB.10\] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità](#)
- [\[ELB.12\] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)

- [\[ELB.13\] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità](#)
- [\[ELB.14\] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)
- [\[ES.1\] I domini Elasticsearch devono avere la crittografia a riposo abilitata](#)
- [\[ES.2\] I domini Elasticsearch non devono essere accessibili al pubblico](#)
- [\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)
- [\[ES.4\] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch](#)
- [\[ES.5\] I domini Elasticsearch devono avere la registrazione di controllo abilitata](#)
- [\[ES.6\] I domini Elasticsearch devono avere almeno tre nodi di dati](#)
- [\[ES.7\] I domini Elasticsearch devono essere configurati con almeno tre nodi master dedicati](#)
- [\[ES.8\] Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [\[EventBridge.3\] i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata](#)
- [\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)
- [\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)
- [\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)
- [\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)
- [\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)
- [\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)
- [\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)
- [\[IAM.7\] Le politiche relative alle password per gli utenti IAM dovrebbero avere configurazioni solide](#)
- [\[IAM.8\] Le credenziali utente IAM non utilizzate devono essere rimosse](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)
- [\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)

- [\[KMS.1\] Le politiche gestite dai clienti di IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS](#)
- [\[KMS.2\] I principali IAM non devono disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS](#)
- [\[KMS.3\] AWS KMS keys non deve essere eliminato involontariamente](#)
- [\[KMS.4\] la rotazione dei tasti dovrebbe essere abilitata AWS KMS](#)
- [\[Lambda.1\] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico](#)
- [\[Lambda.2\] Le funzioni Lambda devono utilizzare runtime supportati](#)
- [\[Lambda.3\] Le funzioni Lambda devono trovarsi in un VPC](#)
- [\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)
- [\[MSK.1\] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker](#)
- [\[MQ.5\] I broker ActiveMQ devono utilizzare la modalità di distribuzione attiva/standby](#)
- [\[MQ.6\] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)
- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)
- [\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)
- [\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)
- [\[NetworkFirewall.6\] Il gruppo di regole Stateless Network Firewall non deve essere vuoto](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)
- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)

- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)
- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [\[RDS.1\] L'istanza RDS deve essere privata](#)
- [\[RDS.2\] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, in base alla durata PubliclyAccessible AWS Config](#)
- [\[RDS.3\] Le istanze database RDS devono avere la crittografia dei dati inattivi abilitata](#)
- [\[RDS.4\] Le istantanee dei cluster RDS e le istantanee del database devono essere crittografate quando sono inattive](#)
- [\[RDS.5\] Le istanze DB RDS devono essere configurate con più zone di disponibilità](#)
- [\[RDS.6\] Il monitoraggio avanzato deve essere configurato per le istanze DB RDS](#)
- [\[RDS.8\] Le istanze DB RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.9\] Le istanze DB RDS devono pubblicare i log nei registri CloudWatch](#)
- [\[RDS.10\] L'autenticazione IAM deve essere configurata per le istanze RDS](#)
- [\[RDS.11\] Le istanze RDS devono avere i backup automatici abilitati](#)
- [\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)
- [\[RDS.13\] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati](#)
- [\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)
- [\[RDS.17\] Le istanze DB RDS devono essere configurate per copiare i tag nelle istantanee](#)
- [\[RDS.18\] Le istanze RDS devono essere distribuite in un VPC](#)
- [\[RDS.19\] Le sottoscrizioni esistenti per le notifiche di eventi RDS devono essere configurate per gli eventi critici del cluster](#)
- [\[RDS.20\] Le sottoscrizioni di notifica degli eventi RDS esistenti devono essere configurate per gli eventi critici delle istanze di database](#)
- [\[RDS.21\] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici del gruppo di parametri del database](#)

- [\[RDS.22\] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici dei gruppi di sicurezza del database](#)
- [\[RDS.23\] Le istanze RDS non devono utilizzare una porta predefinita del motore di database](#)
- [\[RDS.25\] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato](#)
- [\[RDS.27\] I cluster RDS DB devono essere crittografati quando sono inattivi](#)
- [\[Redshift.1\] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico](#)
- [\[Redshift.2\] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito](#)
- [\[Redshift.4\] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata](#)
- [\[Redshift.6\] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati](#)
- [\[Redshift.7\] I cluster Redshift devono utilizzare un routing VPC avanzato](#)
- [\[Redshift.8\] I cluster Amazon Redshift non devono utilizzare il nome utente predefinito di amministratore](#)
- [\[Redshift.9\] I cluster Redshift non devono utilizzare il nome di database predefinito](#)
- [\[Redshift.10\] I cluster Redshift devono essere crittografati a riposo](#)
- [\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)
- [\[S3.2\] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura](#)
- [\[S3.3\] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura](#)
- [\[S3.5\] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL](#)
- [\[S3.6\] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS](#)
- [\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)
- [\[S3.9\] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata](#)
- [\[S3.12\] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3](#)
- [\[S3.13\] I bucket generici S3 devono avere configurazioni del ciclo di vita](#)
- [\[S3.17\] I bucket generici S3 devono essere crittografati quando sono inattivi con AWS KMS keys](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)
- [\[SageMaker.2\] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato](#)
- [\[SageMaker.3\] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook](#)

- [\[SecretsManager.1\] I segreti di Secrets Manager devono avere la rotazione automatica abilitata](#)
- [\[SecretsManager.2\] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente](#)
- [\[SecretsManager.3\] Rimuovi i segreti inutilizzati di Secrets Manager](#)
- [\[SecretsManager.4\] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni](#)
- [\[SQS.1\] Le code di Amazon SQS devono essere crittografate quando sono inattive](#)
- [\[SSM.1\] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager](#)
- [\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)
- [\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)
- [\[SSM.4\] I documenti SSM non devono essere pubblici](#)
- [\[WAF.2\] Le regole regionali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.4\] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.10\] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole](#)

Per ulteriori informazioni su questo standard, consulta i [controlli del Security Hub](#) nella Guida AWS Control Tower per l'utente.

Visualizzazione e gestione degli standard di sicurezza

Gli standard di sicurezza includono una serie di requisiti per determinare la conformità ai quadri normativi, alle migliori pratiche del settore o alle politiche aziendali. AWS Security Hub associa questi requisiti ai controlli ed esegue controlli di sicurezza sui controlli per valutare se i requisiti di uno standard sono soddisfatti. Un controllo può essere abilitato in uno o più standard. Se attivi i risultati del controllo consolidato, Security Hub genera un singolo risultato per controllo di sicurezza anche quando un controllo fa parte di più standard abilitati. Per ulteriori informazioni, consulta [Risultati di controllo consolidati](#).

Per un elenco degli standard disponibili e dei controlli ad essi applicabili, consulta [Riferimento agli standard](#). La pagina degli standard di sicurezza sulla console Security Hub mostra anche tutti gli

standard di sicurezza supportati in Security Hub e il relativo stato di abilitazione. Per ogni standard di sicurezza abilitato nel tuo account (o se utilizzi l'integrazione con AWS Organizations, in almeno un account della tua organizzazione), puoi visualizzare le seguenti informazioni:

- [Lo stato di abilitazione dello standard in diverse politiche di configurazione del Security Hub se si utilizza la configurazione centrale](#)
- Una descrizione di eventuali standard disabilitati
- Un elenco dei controlli attualmente abilitati nello standard e lo stato generale di tali controlli in base allo stato di conformità dei relativi risultati
- un elenco di controlli che si applicano allo standard ma che sono attualmente disabilitati
- Un [punteggio di sicurezza](#) per lo standard

Security Hub genera un punteggio di sicurezza per ogni standard. Gli account amministratore visualizzano i punteggi di sicurezza aggregati e gli stati di controllo dei rispettivi account membri. Se hai impostato una regione di aggregazione, i punteggi di sicurezza riflettono lo stato di conformità dei controlli in tutte le regioni collegate. Per ulteriori informazioni, consulta [Come vengono calcolati i punteggi di sicurezza](#).

Argomenti

- [Abilitazione e disabilitazione degli standard di sicurezza](#)
- [Visualizzazione dei dettagli di uno standard](#)
- [Abilitazione e disabilitazione dei controlli in standard specifici](#)

Abilitazione e disabilitazione degli standard di sicurezza

Puoi abilitare o disabilitare ogni standard di sicurezza disponibile in Security Hub.

Prima di abilitare qualsiasi standard di sicurezza, assicurati di aver abilitato AWS Config e configurato la registrazione delle risorse. In caso contrario, Security Hub potrebbe non essere in grado di generare risultati per i controlli che si applicano a uno standard. Per ulteriori informazioni, consulta [Configurazione AWS Config](#).

Note

Le istruzioni per abilitare e disabilitare gli standard variano a seconda che si utilizzi o meno la [configurazione centrale](#). Questa sezione descrive le differenze. La configurazione centrale

è disponibile per gli utenti che integrano Security Hub e AWS Organizations. Si consiglia di utilizzare la configurazione centrale per semplificare il processo di attivazione e disabilitazione degli standard in ambienti con più account e più regioni.

Abilitazione di uno standard di sicurezza

Quando si abilita uno standard di sicurezza, tutti i controlli che si applicano allo standard vengono abilitati automaticamente in esso. Security Hub inizia anche a generare risultati per i controlli che si applicano allo standard.

Puoi scegliere quali controlli abilitare e disabilitare in ogni standard. La disabilitazione di un controllo interrompe la generazione dei risultati relativi al controllo e il controllo viene ignorato durante il calcolo dei punteggi di sicurezza.

Quando abiliti Security Hub, Security Hub calcola il punteggio di sicurezza iniziale per uno standard entro 30 minuti dalla prima visita alla pagina di riepilogo o alla pagina degli standard di sicurezza sulla console di Security Hub. Possono essere necessarie fino a 24 ore prima che i punteggi di sicurezza vengano generati per la prima volta nelle regioni della Cina e. AWS GovCloud (US) Region I punteggi vengono generati solo per gli standard abilitati quando visiti quelle pagine. Inoltre, la registrazione AWS Config delle risorse deve essere configurata per visualizzare gli spartiti. Dopo la prima generazione del punteggio, Security Hub aggiorna il punteggio di sicurezza ogni 24 ore. Security Hub visualizza un timestamp per indicare quando un punteggio di sicurezza è stato aggiornato l'ultima volta. Per visualizzare un elenco degli standard attualmente abilitati nel tuo account, richiama l'API. [GetEnabledStandards](#)

Attivazione di uno standard su più account e regioni

Per abilitare uno standard di sicurezza su più account e Regioni AWS, è necessario utilizzare la [configurazione centrale](#).

Quando si utilizza la configurazione centrale, l'amministratore delegato può creare politiche di configurazione del Security Hub che abilitano uno o più standard. È quindi possibile associare la politica di configurazione a account e unità organizzative (OU) specifici o alla radice. Una politica di configurazione ha effetto nella regione di origine (chiamata anche regione di aggregazione) e in tutte le regioni collegate.

Le politiche di configurazione offrono la personalizzazione. Ad esempio, è possibile scegliere di abilitare solo AWS Foundational Security Best Practices (FSBP) in un'unità organizzativa e di abilitare

FSBP e Center for Internet Security (CIS) AWS Foundations Benchmark v1.4.0 in un'altra unità organizzativa. Per istruzioni sulla creazione di una politica di configurazione che abiliti standard specifici, vedere [Creazione e associazione dei criteri di configurazione del Security Hub](#)

Se utilizzi la configurazione centrale, Security Hub non abilita automaticamente nessuno standard negli account nuovi o esistenti. Invece, quando crea una politica di configurazione, l'amministratore delegato definisce quali standard abilitare nei diversi account. Security Hub offre una politica di configurazione consigliata in cui è abilitato solo FSBP. Per ulteriori informazioni, consulta [Tipi di politiche di configurazione](#).

Note

L'amministratore delegato può creare politiche di configurazione per abilitare qualsiasi standard tranne [Service-Managed Standard](#). AWS Control Tower È possibile abilitare questo standard solo nel servizio. AWS Control Tower Se si utilizza la configurazione centrale, è possibile abilitare e disabilitare i controlli di questo standard per un account gestito centralmente solo in AWS Control Tower.

Se desideri che alcuni account configurino i propri standard anziché l'amministratore delegato, l'amministratore delegato può designare tali account come autogestiti. Gli account autogestiti devono configurare gli standard separatamente in ciascuna regione.

Abilitazione di uno standard in un unico account e regione

Se non utilizzi la configurazione centrale o se sei un account autogestito, non puoi utilizzare i criteri di configurazione per abilitare centralmente gli standard in più account e regioni. Tuttavia, puoi utilizzare i seguenti passaggi per abilitare uno standard in un unico account e regione.

Security Hub console

Per abilitare uno standard in un account e in un'unica regione

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Conferma di utilizzare Security Hub nella regione in cui desideri abilitare lo standard.
3. Nel pannello di navigazione Security Hub, scegli Standard di sicurezza.
4. Per lo standard che si desidera abilitare, scegliere Enable (Abilita). Ciò abilita anche tutti i controlli all'interno di quello standard.

5. Ripetere l'operazione in ogni regione in cui si desidera abilitare lo standard.

Security Hub API

Per abilitare uno standard in un account e in un'unica regione

1. Invoca l'[BatchEnableStandards](#) API.
2. Fornisci l'Amazon Resource Name (ARN) dello standard che desideri abilitare. Per ottenere l'ARN standard, richiama l'API. [DescribeStandards](#)
3. Ripetere l'operazione in ogni regione in cui si desidera abilitare lo standard.

AWS CLI

Per abilitare uno standard in un account e in un'unica regione

1. Esegui il comando [batch-enable-standards](#).
2. Fornisci l'Amazon Resource Name (ARN) dello standard che desideri abilitare. Per ottenere l'ARN standard, esegui il [describe-standards](#) comando.

```
aws securityhub batch-enable-standards --standards-subscription-requests  
'{"StandardsArn": "standard ARN"}'
```

Esempio

```
aws securityhub batch-enable-standards --standards-subscription-requests  
'{"StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-  
security-best-practices/v/1.0.0"}'
```

3. Ripetere l'operazione in ogni regione in cui si desidera abilitare lo standard.

Attivazione automatica degli standard di sicurezza predefiniti

Se non utilizzi la configurazione centrale, Security Hub abilita automaticamente gli standard di sicurezza predefiniti nei nuovi account quando entrano a far parte della tua organizzazione. Inoltre, tutti i controlli che fanno parte degli standard predefiniti vengono abilitati automaticamente. Attualmente, gli standard di sicurezza predefiniti che vengono abilitati automaticamente sono AWS Foundational Security Best Practices (FSBP) e Center for Internet Security (CIS) Foundations

Benchmark v1.2.0. AWS Puoi disattivare gli standard abilitati automaticamente se preferisci abilitare manualmente gli standard nei nuovi account.

Se si utilizza la configurazione centrale, è possibile creare una politica di configurazione che abiliti gli standard predefiniti e associare questa politica alla radice. Tutti gli account e le unità organizzative dell'organizzazione ereditano questa politica di configurazione a meno che non siano associati a una politica diversa o siano gestiti automaticamente.

Disattiva gli standard abilitati automaticamente

I passaggi seguenti si applicano solo se si esegue l'integrazione con la configurazione centrale AWS Organizations ma non si utilizza. Se non utilizzi l'integrazione Organizations, puoi disattivare uno standard predefinito quando attivi Security Hub per la prima volta oppure puoi seguire i passaggi per [disabilitare uno standard](#).

Security Hub console

Per disattivare gli standard abilitati automaticamente

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
Accedi utilizzando le credenziali dell'account amministratore.
2. Nel pannello di navigazione di Security Hub, in Impostazioni, scegli Configurazione.
3. Nella sezione Account, disattiva l'attivazione automatica degli standard predefiniti.

Security Hub API

Per disattivare gli standard abilitati automaticamente

1. Richiama l'[UpdateOrganizationConfiguration](#) API dall'account amministratore di Security Hub.
2. Per disattivare gli standard abilitati automaticamente negli account dei nuovi membri, imposta `AutoEnableStandards` uguale a `NONE`.

AWS CLI

Per disattivare gli standard abilitati automaticamente

1. Esegui il comando [update-organization-configuration](#).

2. Includi il `auto-enable-standards` parametro per disattivare gli standard abilitati automaticamente negli account dei nuovi membri.

```
aws securityhub update-organization-configuration --auto-enable-standards
```

Disabilitazione di uno standard di sicurezza

Quando si disabilita uno standard di sicurezza in Security Hub, si verifica quanto segue:

- Tutti i controlli che si applicano allo standard sono inoltre disabilitati a meno che non siano associati a un altro standard.
- I controlli per i controlli disabilitati non vengono più eseguiti e non vengono generati risultati aggiuntivi per i controlli disabilitati.
- I risultati esistenti relativi ai controlli disabilitati vengono archiviati automaticamente dopo circa 3-5 giorni.
- Le AWS Config regole che Security Hub ha creato per i controlli disabilitati vengono rimosse.

Questa operazione si verifica in genere entro pochi minuti dalla disattivazione dello standard, ma potrebbe richiedere più tempo. Se la prima richiesta di eliminazione delle AWS Config regole fallisce, Security Hub riprova ogni 12 ore. Tuttavia, se hai disabilitato Security Hub o non hai abilitato nessun altro standard, Security Hub non può riprovare la richiesta, il che significa che non può eliminare le AWS Config regole. Se ciò si verifica e devi eliminare AWS Config le regole, contatta AWS Support.

Disabilitazione di uno standard su più account e regioni

Per disabilitare uno standard di sicurezza su più account e regioni, è necessario utilizzare la [configurazione centrale](#).

Quando si utilizza la configurazione centrale, l'amministratore delegato può creare politiche di configurazione che disabilitano uno o più standard. È possibile associare una politica di configurazione a account e unità organizzative specifici o alla radice. Una politica di configurazione ha effetto nella regione di origine (chiamata anche regione di aggregazione) e in tutte le regioni collegate.

Le politiche di configurazione offrono la personalizzazione. Ad esempio, è possibile scegliere di disabilitare lo standard PCI DSS (Payment Card Industry Data Security Standard) in un'unità

organizzativa e disabilitare sia PCI DSS che il National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5 in un'altra unità organizzativa. Per istruzioni sulla creazione di una politica di configurazione che disabiliti gli standard specifici, vedere. [Creazione e associazione dei criteri di configurazione del Security Hub](#)

Note

L'amministratore delegato può creare politiche di configurazione per disabilitare qualsiasi standard tranne il [Service-Managed](#) Standard. AWS Control Tower È possibile disabilitare questo standard solo nel servizio. AWS Control Tower Se si utilizza la configurazione centrale, è possibile abilitare e disabilitare i controlli di questo standard per un account gestito centralmente solo in AWS Control Tower.

Se desideri che alcuni account configurino i propri standard anziché l'amministratore delegato, l'amministratore delegato può designare tali account come autogestiti. Gli account autogestiti devono configurare gli standard separatamente in ciascuna regione.

Disabilitazione di uno standard in un unico account e regione

Se non utilizzi la configurazione centrale o sei un account autogestito, non puoi utilizzare i criteri di configurazione per disabilitare centralmente gli standard in più account e regioni. Tuttavia, puoi utilizzare i seguenti passaggi per disabilitare uno standard in un unico account e regione.

Security Hub console

Per disabilitare uno standard in un account e in una regione

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Conferma di utilizzare Security Hub nella regione in cui desideri disabilitare lo standard.
3. Nel pannello di navigazione Security Hub, scegli Standard di sicurezza.
4. Per lo standard che si desidera disabilitare, scegliere Disable (Disabilita).
5. Ripeti l'operazione in ogni regione in cui desideri disabilitare lo standard.

Security Hub API

Per disabilitare uno standard in un account e in una regione

1. Invoca l'[BatchDisableStandardsAPI](#).

2. Per ogni standard che desideri disabilitare, fornisci l'ARN dell'abbonamento standard. Per ottenere gli ARN dell'abbonamento per gli standard abilitati, richiama l'API. [GetEnabledStandards](#)
3. Ripeti l'operazione in ogni regione in cui desideri disabilitare lo standard.

AWS CLI

Per disabilitare uno standard in un account e in una regione

1. Esegui il comando [batch-disable-standards](#).
2. Per ogni standard che desideri disabilitare, fornisci l'ARN dell'abbonamento standard. Per ottenere gli ARN dell'abbonamento per gli standard abilitati, esegui il [get-enabled-standards](#) comando.

```
aws securityhub batch-disable-standards --standards-subscription-arns "standard  
subscription ARN"
```

Esempio

```
aws securityhub batch-disable-standards --standards-subscription-arns  
"arn:aws:securityhub:us-west-1:123456789012:subscription/aws-foundational-  
security-best-practices/v/1.0.0"
```

3. Ripeti l'operazione in ogni regione in cui desideri disabilitare lo standard.

Visualizzazione dei dettagli di uno standard

Sulla AWS Security Hub console, la pagina dei dettagli di uno standard include le seguenti informazioni:

- Il punteggio di sicurezza standard e un riepilogo visivo dei controlli di sicurezza per i controlli abilitati nello standard. Se si esegue l'integrazione con AWS Organizations, i controlli abilitati in almeno un account dell'organizzazione vengono considerati abilitati.
- Le impostazioni per [abilitare o disabilitare un controllo](#) che si applica allo standard.
- Un elenco di controlli che si applicano allo standard. I controlli sono suddivisi in diverse schede in base allo stato di abilitazione. Il numero di controlli nella colonna Tutti i controlli abilitati è la somma dei controlli nelle colonne Failed, Unknown, No data e Passato.

Puoi anche utilizzare l'API Security Hub e AWS CLI recuperare i dettagli di uno standard. Le sezioni seguenti spiegano come ottenere i dettagli di uno standard.

Visualizzazione della pagina dei dettagli di uno standard abilitato (console)

Dalla pagina Standard di sicurezza, è possibile visualizzare la pagina dei dettagli di uno standard abilitato.

Se hai effettuato l'accesso all'account amministratore, puoi visualizzare i dettagli di qualsiasi standard abilitato in almeno un account membro.

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel pannello di navigazione Security Hub, scegli Standard di sicurezza.
3. Per lo standard di cui desideri visualizzare i dettagli, scegli Visualizza risultati.

Punteggio di sicurezza standard e riepilogo dei controlli di sicurezza

Nella parte superiore della pagina dei dettagli dello standard è riportato il punteggio di sicurezza dello standard. Il punteggio è la percentuale di controlli superati rispetto al numero di controlli abilitati (che contengono dati) per lo standard.

Security Hub calcola in genere il punteggio di sicurezza iniziale entro 30 minuti dalla prima visita alla pagina di riepilogo o alla pagina degli standard di sicurezza sulla console di Security Hub. I punteggi vengono generati solo per gli standard abilitati quando visiti quelle pagine. Per visualizzare un elenco degli standard attualmente abilitati, utilizza l'operazione [GetEnabledStandards](#) API. Inoltre, la registrazione AWS Config delle risorse deve essere configurata per visualizzare gli spartiti. Dopo la prima generazione del punteggio, Security Hub aggiorna il punteggio di sicurezza ogni 24 ore. Security Hub visualizza un timestamp per indicare quando un punteggio di sicurezza è stato aggiornato l'ultima volta. Per ulteriori informazioni, consulta [the section called “Definizione dei punteggi di sicurezza”](#).

Note

Possono essere necessarie fino a 24 ore prima che i punteggi di sicurezza vengano generati per la prima volta nelle regioni cinesi e. AWS GovCloud (US) Region

Accanto al punteggio c'è un grafico che riassume i controlli di sicurezza per i controlli abilitati per lo standard. Il grafico mostra la percentuale di controlli di sicurezza non riusciti e superati. Quando ti fermi sul grafico, il pop-up mostra quanto segue:

- Il numero di controlli di sicurezza non riusciti per i controlli di ciascuna gravità
- Il numero di controlli di sicurezza per i controlli con stato Sconosciuto
- Il numero di controlli di sicurezza superati

Per gli account amministratore, il punteggio e il grafico standard vengono aggregati nell'account amministratore e in tutti gli account dei membri.

Tutti i dati nelle pagine dei dettagli degli standard di sicurezza sono specifici della regione corrente, a meno che non sia stata impostata una regione di aggregazione. Se hai impostato una regione di aggregazione, i punteggi di sicurezza si applicano a tutte le regioni e includono i risultati in tutte le regioni collegate. Lo stato di conformità dei controlli nelle pagine dei dettagli degli standard riflette anche i risultati delle regioni collegate e il numero di controlli di sicurezza include i risultati delle regioni collegate.

Visualizzazione dei controlli negli standard abilitati

Quando visiti la pagina dei dettagli di uno standard, puoi visualizzare un elenco di controlli di sicurezza che si applicano allo standard. Questo elenco è ordinato in base allo stato di conformità del controllo e alla gravità assegnata a ciascun controllo. Security Hub aggiorna lo stato dei controlli e il conteggio dei controlli di sicurezza ogni 24 ore. Un timestamp su ogni scheda indica quando gli stati di controllo e il conteggio dei controlli di sicurezza sono stati aggiornati più di recente. Per ulteriori informazioni, consulta [the section called “Stato di conformità e stato di controllo”](#).

Per gli account amministratore, gli stati di conformità ai controlli e il numero di controlli di sicurezza sono aggregati nell'account amministratore e in tutti gli account dei membri.

La scheda Tutti i controlli abilitati elenca tutti i controlli attualmente abilitati nello standard. Per gli account amministratore, la scheda Tutti gli account abilitati include i controlli abilitati nello standard nel rispettivo account o in almeno un account membro.

Nelle schede Operazioni non riuscite, Sconosciuto, Nessun dato e Passato, i controlli della scheda Tutti i comandi abilitati vengono filtrati in modo da includere solo i controlli abilitati con uno stato specifico.

La scheda Disabilitato contiene l'elenco dei controlli disabilitati nello standard. Per gli account amministratore, la scheda Disabilitati include i controlli disabilitati nello standard nei rispettivi account e in tutti gli account dei membri.

Per ogni controllo, le schede visualizzano le seguenti informazioni:

- Lo stato del controllo (vedere [the section called “Stato di conformità e stato di controllo”](#))
- La severità assegnata al controllo
- L'ID e il titolo del controllo
- Il numero di risultati attivi non riusciti rispetto al numero totale di risultati attivi. Se applicabile, la colonna Controlli falliti elenca anche il numero di risultati con lo stato Sconosciuto.

Oltre al filtro di ricerca in ogni scheda, puoi ordinare gli elenchi in base ai seguenti campi:

- Stato di conformità
- Gravità
- ID
- Titolo
- Controlli falliti

È possibile ordinare ogni elenco utilizzando una qualsiasi delle colonne. Per impostazione predefinita, la scheda Tutti i comandi abilitati è ordinata in modo che i controlli non riusciti siano visualizzati in cima all'elenco. In questo modo è possibile concentrarsi immediatamente sui problemi che richiedono una soluzione.

Nelle schede rimanenti, i controlli sono ordinati per impostazione predefinita in ordine decrescente per gravità. In altre parole, i controlli critici sono i primi, seguiti dai controlli di severità alta, poi media e poi bassa.

Scegli il metodo di accesso preferito e segui i passaggi per visualizzare i controlli disponibili per uno standard abilitato. Al posto di queste istruzioni, puoi anche utilizzare l'operazione [DescribeStandardsControl](#) API.

Security Hub console

1. Apri la AWS Security Hub console all'indirizzo <https://console.aws.amazon.com/securityhub/>.
2. Scegli Standard di sicurezza nel pannello di navigazione.

3. Scegli Visualizza risultati per uno standard. Nella parte inferiore della pagina sono elencati i controlli (divisi per schede) che si applicano allo standard.

Security Hub API

1. Esegui [ListSecurityControlDefinitions](#) fornisci un Amazon Resource Name (ARN) standard per ottenere un elenco di ID di controllo per quello standard. Per ottenere ARN standard, esegui [DescribeStandards](#). Se non fornisci un ARN standard, questa API restituisce tutti gli ID di controllo del Security Hub. Questa API restituisce ID di controllo di sicurezza indipendenti dallo standard, non ID di controllo specifici dello standard.

Richiesta di esempio:

```
{
  "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
  best-practices/v/1.0.0"
}
```

2. Corri [ListStandardsControlAssociations](#) a scoprire se un controllo è abilitato in ogni standard che hai abilitato nel tuo account.
3. Identifica il controllo fornendo SecurityControlId o SecurityControlArn. I parametri di impaginazione sono facoltativi.

Richiesta di esempio:

```
{
  SecurityControlId: Config.1
  NextToken: lkeyusdlk-sdlflsnd-ladfterb
  MaxResults: 5
}
```

AWS CLI

1. Esegui il [list-security-control-definitions](#) comando e fornisci uno o più ARN standard per ottenere un elenco di ID di controllo. Per ottenere ARN standard, esegui il `describe-standards` comando. Se non si fornisce un ARN standard, questo comando restituisce tutti gli ID di controllo del Security Hub. Questo comando restituisce ID di controllo di sicurezza indipendenti dallo standard, non ID di controllo specifici dello standard.

```
aws securityhub --region us-east-1 list-security-control-definitions --  
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-  
security-best-practices/v/1.0.0"
```

2. Esegui il [list-standards-control-associations](#) comando per scoprire se un controllo è abilitato in ogni standard che hai abilitato nel tuo account.
3. Identifica il controllo fornendo security-control-id o security-control-arn.

Comando di esempio:

```
aws securityhub --region us-east-1 list-standards-control-associations --  
security-control-id Config.1
```

Scaricamento dell'elenco dei controlli

È possibile scaricare la pagina corrente dell'elenco dei controlli in un .csv file.

Se hai filtrato l'elenco dei controlli, il file scaricato include solo i controlli che corrispondono alle impostazioni del filtro.

Se hai scelto un controllo specifico dall'elenco, il file scaricato include solo quel controllo.

Per scaricare la pagina corrente dell'elenco dei controlli o il controllo attualmente selezionato, scegli Scarica.

Abilitazione e disabilitazione dei controlli in standard specifici

Quando abiliti uno standard in AWS Security Hub, tutti i controlli ad esso applicabili vengono abilitati automaticamente in quello standard (ad eccezione degli standard gestiti dai servizi). È quindi possibile disabilitare e riattivare controlli specifici nello standard. Tuttavia, consigliamo di allineare lo stato di attivazione di un controllo a tutti gli standard abilitati.

Note

Se si utilizza la configurazione centrale di Security Hub, l'amministratore delegato può abilitare e disabilitare i controlli per gli account dell'organizzazione in tutti gli standard abilitati. Consigliamo questo approccio in modo che lo stato di attivazione di un controllo sia allineato a tutti gli standard. Tuttavia, l'amministratore delegato può designare gli account

come autogestiti, il che offre loro la possibilità di abilitare e disabilitare i controlli in standard specifici. Per ulteriori informazioni, consulta [Come funziona la configurazione centrale](#).

La pagina dei dettagli di uno standard contiene l'elenco dei controlli applicabili per lo standard e informazioni sui controlli attualmente abilitati e disabilitati in quello standard.

Nella pagina dei dettagli degli standard, puoi anche abilitare e disabilitare i controlli in uno standard specifico. È necessario abilitare e disabilitare i controlli separatamente in ogni Account AWS e Regione AWS. Quando abiliti o disabiliti un controllo, ciò influisce solo sull'account corrente e sulla regione.

È possibile abilitare e disabilitare i controlli in ogni regione utilizzando la console Security Hub, l'API Security Hub o AWS CLI. Se hai impostato una regione di aggregazione, vedrai i controlli di tutte le regioni collegate. Se un controllo è disponibile in una regione collegata ma non nella regione di aggregazione, non è possibile abilitare o disabilitare tale controllo dalla regione di aggregazione. Per gli script di disabilitazione del controllo multiaccount e multiregione, vedere [Disabilitazione dei controlli del Security Hub](#) in un ambiente con più account.

Abilitazione di un controllo in uno standard specifico

Per abilitare un controllo in uno standard, è necessario prima abilitare almeno uno standard a cui si applica il controllo. Per ulteriori informazioni sull'attivazione di uno standard, vedere [Abilitazione e disabilitazione degli standard di sicurezza](#). Quando si abilita un controllo in uno standard, AWS Security Hub inizia a generare risultati per quel controllo. Security Hub include lo [stato del controllo](#) nel calcolo del punteggio di sicurezza complessivo e dei punteggi di sicurezza standard. Anche se abiliti un controllo in più standard, se attivi i risultati del controllo consolidato riceverai un unico risultato per ogni controllo di sicurezza tra gli standard. Per ulteriori informazioni, consulta [Risultati dei controlli consolidati](#).

Per abilitare un controllo in uno standard, il controllo deve essere disponibile nella tua regione attuale. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

Segui questi passaggi per abilitare il controllo del Security Hub in uno standard specifico. Al posto dei seguenti passaggi, puoi anche utilizzare l'azione [UpdateStandardsControlAPI](#) per abilitare i controlli in uno standard specifico. Per istruzioni sull'attivazione di un controllo in tutti gli standard, vedere [Abilitare il controllo in tutti gli standard in un unico account e regione](#).

Security Hub console

Per abilitare un controllo in uno standard specifico

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Scegli Standard di sicurezza dal pannello di navigazione.
3. Scegli Visualizza risultati per lo standard pertinente.
4. Seleziona un controllo.
5. Scegli Abilita controllo (questa opzione non viene visualizzata per un controllo già abilitato). Conferma scegliendo Abilita.

Security Hub API

Per abilitare un controllo in uno standard specifico

1. Esegui [ListSecurityControlDefinitions](#) e fornisci un ARN standard per ottenere un elenco di controlli disponibili per uno standard specifico. Per ottenere un ARN standard, esegui [DescribeStandards](#). Questa API restituisce ID di controllo di sicurezza indipendenti dallo standard, non ID di controllo specifici dello standard.

Richiesta di esempio:

```
{
  "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
  best-practices/v/1.0.0"
}
```

2. Esegui [ListStandardsControlAssociations](#) e fornisci un ID di controllo specifico per restituire lo stato di abilitazione corrente di un controllo in ogni standard.

Richiesta di esempio:

```
{
  "SecurityControlId": "IAM.1"
}
```

3. Esegui [BatchUpdateStandardsControlAssociations](#). Fornisci l'ARN dello standard in cui desideri abilitare il controllo.
4. Imposta il AssociationStatus parametro uguale a. ENABLED

Richiesta di esempio:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}]
}
```

AWS CLI

Per abilitare un controllo in uno standard specifico

1. Esegui il [list-security-control-definitions](#) comando e fornisci un ARN standard per ottenere un elenco di controlli disponibili per uno standard specifico. Per ottenere un ARN standard, esegui `describe-standards`. Questo comando restituisce ID di controllo di sicurezza indipendenti dallo standard, non ID di controllo specifici dello standard.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Esegui il [list-standards-control-associations](#) comando e fornisci un ID di controllo specifico per restituire lo stato di abilitazione corrente di un controllo in ogni standard.

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Esegui il comando [batch-update-standards-control-associations](#). Fornisci l'ARN dello standard in cui desideri abilitare il controllo.
4. Imposta il `AssociationStatus` parametro uguale a `ENABLED`

```
aws securityhub --region us-east-1 batch-update-standards-control-associations
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
"StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0", "AssociationStatus": "ENABLED"}]'
```

Disattivazione di un controllo in uno standard specifico

Quando si disabilita un controllo in uno standard, Security Hub smette di generare risultati per il controllo. Lo stato del controllo non viene più utilizzato nel calcolo del punteggio di sicurezza per lo standard.

Un modo per disabilitare un controllo consiste nel disabilitare tutti gli standard a cui si applica il controllo. Quando si disabilita uno standard, tutti i controlli che si applicano allo standard vengono disabilitati (tuttavia, tali controlli possono rimanere abilitati in altri standard). Per informazioni sulla disabilitazione di uno standard, vedere [the section called “Abilitazione e disabilitazione degli standard”](#).

Quando si disattiva un controllo disattivando uno standard a cui si applica, si verifica quanto segue:

- I controlli di sicurezza per il controllo non vengono più eseguiti per quello standard. Ciò significa che lo stato del controllo non influirà sul punteggio di sicurezza standard (Security Hub continuerà a eseguire i controlli di sicurezza per il controllo se è abilitato in altri standard).
- Non vengono generati ulteriori risultati per tale verifica.
- I risultati esistenti vengono archiviati automaticamente dopo 3-5 giorni (tieni presente che si tratta del massimo impegno e non è garantito).
- Le AWS Config regole correlate create da Security Hub vengono rimosse.

Quando si disabilita uno standard, Security Hub non tiene traccia dei controlli disattivati. Se successivamente si abilita nuovamente lo standard, tutti i controlli ad esso applicabili vengono abilitati automaticamente. Inoltre, la disattivazione di un controllo è un'operazione che si effettua una sola volta. Supponiamo di disabilitare un controllo e quindi di abilitare uno standard precedentemente disabilitato. Se lo standard include quel controllo, sarà abilitato in quello standard. Quando abiliti uno standard in Security Hub, tutti i controlli che si applicano a quello standard vengono abilitati automaticamente.

Invece di disabilitare un controllo disattivando uno standard a cui si applica, puoi semplicemente disabilitare il controllo in uno o più standard specifici.

Per ridurre i disturbi rilevati, può essere utile disabilitare i controlli non pertinenti all'ambiente in uso. Per consigli su quali controlli disabilitare, vedi [Controlli del Security Hub che potresti voler disabilitare](#).

Segui questi passaggi per disabilitare un controllo in standard specifici. Al posto dei seguenti passaggi, puoi anche utilizzare l'azione [UpdateStandardsControl](#) API per disabilitare i controlli in

uno standard specifico. Per istruzioni sulla disabilitazione di un controllo in tutti gli standard, vedere [Abilitazione e disabilitazione dei controlli in tutti gli standard](#)

Security Hub console

Per disabilitare un controllo in uno standard specifico

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Scegli Standard di sicurezza dal pannello di navigazione. Scegli Visualizza risultati per lo standard pertinente.
3. Seleziona un controllo.
4. Scegli Disabilita controllo (questa opzione non viene visualizzata per un controllo già disabilitato).
5. Fornisci un motivo per disabilitare il controllo e conferma scegliendo Disabilita.

Security Hub API

Per disabilitare un controllo in uno standard specifico

1. Esegui [ListSecurityControlDefinitions](#) e fornisci un ARN standard per ottenere un elenco di controlli disponibili per uno standard specifico. Per ottenere un ARN standard, esegui [DescribeStandards](#). Questa API restituisce ID di controllo di sicurezza indipendenti dallo standard, non ID di controllo specifici dello standard.

Richiesta di esempio:

```
{
  "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-
  best-practices/v/1.0.0"
}
```

2. Esegui [ListStandardsControlAssociations](#) e fornisci un ID di controllo specifico per restituire lo stato di abilitazione corrente di un controllo in ogni standard.

Richiesta di esempio:

```
{
  "SecurityControlId": "IAM.1"
}
```

3. Esegui [BatchUpdateStandardsControlAssociations](#). Fornisci l'ARN dello standard in cui desideri disabilitare il controllo.
4. Imposta il `AssociationStatus` parametro uguale a `DISABLED`. Se segui questi passaggi per un controllo già disabilitato, l'API restituisce una risposta con codice di stato HTTP 200.

Richiesta di esempio:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to environment"}]
}
```

AWS CLI

Per disabilitare un controllo in uno standard specifico

1. Esegui il [list-security-control-definitions](#) comando e fornisci un ARN standard per ottenere un elenco di controlli disponibili per uno standard specifico. Per ottenere un ARN standard, esegui `describe-standards`. Questo comando restituisce ID di controllo di sicurezza indipendenti dallo standard, non ID di controllo specifici dello standard.

```
aws securityhub --region us-east-1 list-security-control-definitions --
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"
```

2. Esegui il [list-standards-control-associations](#) comando e fornisci un ID di controllo specifico per restituire lo stato di abilitazione corrente di un controllo in ogni standard.

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

3. Esegui il comando [batch-update-standards-control-associations](#). Fornisci l'ARN dello standard in cui desideri disabilitare il controllo.
4. Imposta il `AssociationStatus` parametro uguale a `DISABLED`. Se segui questi passaggi per un controllo già abilitato, il comando restituisce una risposta con il codice di stato HTTP 200.


```
aws securityhub --region us-east-1 batch-update-standards-control-associations --standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1", "StandardsArn": "arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to environment"}]'
```

Riferimento ai controlli del Security Hub

Questo riferimento ai controlli fornisce un elenco di AWS Security Hub controlli disponibili con collegamenti a ulteriori informazioni su ciascun controllo. La tabella riassuntiva mostra i controlli in ordine alfabetico in base all'ID del controllo. Qui sono inclusi solo i controlli in uso attivo da Security Hub. I controlli ritirati sono esclusi da questo elenco. La tabella fornisce le seguenti informazioni per ogni controllo:

- ID del controllo di sicurezza: questo ID si applica a tutti gli standard Servizio AWS e indica la risorsa e a cui si riferisce il controllo. La console Security Hub mostra gli ID del controllo di sicurezza, indipendentemente dal fatto che [i risultati del controllo consolidato](#) siano attivati o disattivati nell'account. Tuttavia, i risultati di Security Hub fanno riferimento agli ID di controllo di sicurezza solo se i risultati del controllo consolidato sono attivati nel tuo account. Se i risultati di controllo consolidati sono disattivati nel tuo account, alcuni ID di controllo variano in base allo standard dei risultati di controllo. Per una mappatura degli ID di controllo specifici degli standard agli ID dei controlli di sicurezza, consulta [In che modo il consolidamento influisce sugli ID e sui titoli di controllo](#)

Se desideri configurare [le automazioni](#) per i controlli di sicurezza, ti consigliamo di filtrare in base all'ID del controllo anziché al titolo o alla descrizione. Sebbene Security Hub possa occasionalmente aggiornare i titoli o le descrizioni dei controlli, gli ID di controllo rimangono invariati.



I Control ID possono ignorare i numeri. Si tratta di segnaposti per controlli futuri.





- Standard applicabili: indica a quali standard si applica un controllo. Seleziona un controllo per visualizzare i requisiti specifici dei framework di conformità di terze parti.
- Titolo del controllo di sicurezza: questo titolo si applica a tutti gli standard. La console Security Hub mostra i titoli dei controlli di sicurezza, indipendentemente dal fatto che i risultati del controllo consolidato siano attivati o disattivati nel tuo account. Tuttavia, i risultati del Security Hub fanno





riferimento ai titoli dei controlli di sicurezza solo se nel tuo account è attivato il controllo consolidato. Se i risultati di controllo consolidati sono disattivati nel tuo account, alcuni titoli di controllo variano in base allo standard dei risultati di controllo. Per una mappatura degli ID di controllo specifici degli standard agli ID dei controlli di sicurezza, consulta [In che modo il consolidamento influisce sugli ID e sui titoli di controllo](#)




- **Severità:** la severità di un controllo ne identifica l'importanza dal punto di vista della sicurezza. Per informazioni su come Security Hub determina la gravità del controllo, vedere [Assegnazione della gravità ai risultati del controllo](#).
- **Tipo di pianificazione:** indica quando viene valutato il controllo. Per ulteriori informazioni, consulta [Pianificazione dell'esecuzione dei controlli di sicurezza](#).
- **Supporta parametri personalizzati:** indica se il controllo supporta valori personalizzati per uno o più parametri. Seleziona un controllo per visualizzare i dettagli dei parametri. Per ulteriori informazioni, consulta [Parametri di controllo personalizzati](#).





Seleziona un controllo per visualizzare ulteriori dettagli. I controlli sono elencati in ordine alfabetico del nome del servizio.




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Account.1	Le informazioni di contatto relative alla sicurezza devono essere fornite per un Account AWS	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
Conto.2	Account AWS dovrebbe far parte di un'organizzazione AWS Organizations	NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Periodic (Periodico)





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ACM.1	I certificati importati ed emessi da ACM devono essere rinnovati dopo un determinato periodo di tempo	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sì	Modifica attivata e periodica
ACM.2	I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit	AWS Best practice di sicurezza di base v1.0.0	HIGH (ELEVATO)	 No	Modifica attivata
ACM.3	I certificati ACM devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
APIGateway.y.1	API Gateway REST e la registrazione dell'esecuzione delle WebSocket API devono essere abilitati	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sì	Modifica attivata
APIGateway.y.2	Le fasi dell'API REST di API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
APIGateway.y.3	Le fasi dell'API REST di API Gateway devono avere AWS X-Ray la traccia abilitata	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata
APIGateway.y.4	API Gateway deve essere associato a un ACL Web WAF	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
APIGateway.y.5	I dati della cache dell'API REST di API Gateway devono essere crittografati quando sono inattivi	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
APIGateway.y.8	Le rotte API Gateway devono specificare un tipo di autorizzazione	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 Sì	Periodic (Periodico)




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
APIGateway.9	La registrazione degli accessi deve essere configurata per API Gateway V2 Stages	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
AppSync2.	AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata	AWS Best practice di sicurezza di base v1.0.0	MEDIO	 Sì	Modifica attivata
AppSync4.	AWS AppSync Le API GraphQL devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
AppSync5.	AWS AppSync Le API GraphQL non devono essere autenticate con chiavi API	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Modifica attivata
Athena.2	I cataloghi di dati Athena devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Athena.3	I gruppi di lavoro Athena devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
AutoScaling1.	I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare e i controlli di integrità ELB	AWS Best practice di sicurezza di base, Service Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
AutoScaling2.	Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sì	Modifica attivata
AutoScaling3.	Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata
Autoscaling5	Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici.	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
AutoScaling6.	I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
AutoScaling9.	I gruppi di Auto Scaling di EC2 devono utilizzare i modelli di avvio EC2	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
AutoScaling10.	I gruppi EC2 Auto Scaling devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Backup.1	AWS Backup i punti di ripristino devono essere crittografati quando sono inattivi	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
Backup.2	AWS Backup i punti di ripristino devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Backup.3	AWS Backup le casseforti devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Backup.4	AWS Backup i piani di segnalazione devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Backup.4	AWS Backup i piani di backup devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
CloudFormation2.	CloudFormation le pile devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	 Sì	Modifica attivata
CloudFront1.	CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Modifica attivata
CloudFront3.	CloudFront le distribuzioni dovrebbero richiedere e la crittografia in transito	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
CloudFront4.	CloudFront le distribuzioni devono avere il failover di origine configurato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudFront t5.	CloudFront le distribuzioni dovrebbero avere la registrazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
CloudFront t6.	CloudFront le distribuzioni dovrebbero avere WAF abilitato	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
CloudFront t7.	CloudFront le distribuzioni devono utilizzare certificati SSL/TLS personalizzati	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
CloudFront t8.	CloudFront le distribuzioni dovrebbero utilizzare SNI per soddisfare le richieste HTTPS	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
CloudFront t9.	CloudFront le distribuzioni dovrebbero crittografare il traffico verso origini personalizzate	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudFront t.10	CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
CloudFront t1.2	CloudFront le distribuzioni non devono puntare a origini S3 inesistenti	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Periodic (Periodico)
CloudFront t1.3	CloudFront le distribuzioni dovrebbero utilizzare e il controllo dell'accesso all'origine	AWS Migliori pratiche di sicurezza di base v1.0.0	MEDIO	 No	Modifica attivata
CloudFront t1.4	CloudFront le distribuzioni devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudTrail I1.	CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura	CIS AWS Foundations Benchmark v1.2.0, CIS Foundations Benchmark v1.4.0, AWS AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Periodic (Periodico)
CloudTrail I2.	CloudTrail dovrebbe avere la crittografia a riposo abilitata	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, benchmark CIS Foundations v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	MEDIO	 No	Periodic (Periodico)
CloudTrail I3.	Almeno un CloudTrail percorso deve essere abilitato	PCI DSS v3.2.1	HIGH (ELEVATO)	 No	Periodic (Periodico)






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudTrail I4.	CloudTrail la convalida dei file di registro deve essere abilitata	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	BASSO	 No	Periodic (Periodico)
CloudTrail I5.	CloudTrail i trail devono essere integrati con Amazon CloudWatch Logs	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	BASSO	 No	Periodic (Periodico)
CloudTrail I6.	Assicurati che il bucket S3 utilizzato per archiviare i CloudTrail log non sia accessibile al pubblico	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	CRITICO	 No	Modifica attivata e periodica




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudTrail 17.	Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail	Benchmark CIS Foundations v1.2.0, benchmark CIS AWS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)
CloudTrail 19.	CloudTrail i sentieri devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
CloudWatch h1.	Dovrebbero esistere un filtro logmetrico e un allarme per l'utilizzo da parte dell'utente «root»	Benchmark CIS AWS Foundations v1.2.0, PCI DSS v3.2.1, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)
CloudWatch h2.	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle chiamate API non autorizzate	Benchmark CIS AWS Foundations v1.2.0	BASSO	 No	Periodic (Periodico)
CloudWatch h3.	Verifica se esistono un filtro e un allarme per le metriche dei log per l'accesso alla Console di gestione senza autenticazione a più fattori (MFA)	Benchmark CIS AWS Foundations v1.2.0	BASSO	 No	Periodic (Periodico)



ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudWatch h4.	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle policy IAM	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)
CloudWatch h5.	Assicurati che esistano un filtro metrico di registro e un allarme per le CloudTrail modifiche alla configurazione	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)
CloudWatch h6.	Assicurati che esistano un filtro metrico di registro e un allarme per gli AWS Management Console errori di autenticazione	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)
CloudWatch h7.	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alla disabilitazione o all'eliminazione pianificata delle chiavi gestite dal cliente (CMK) create dal cliente	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)







ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudWatch h8.	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle policy dei bucket S3	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)
CloudWatch h9.	Assicurati che esistano un filtro metrico di registro e un allarme per le AWS Config modifiche alla configurazione	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)
CloudWatch h.10	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate al gruppo di sicurezza	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)
CloudWatch h.11	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle liste di controllo degli accessi alla rete (NACL)	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudWatch h.12	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ai gateway di rete	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)
CloudWatch h.13	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle tabelle di routing	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)
CloudWatch h.14	Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate al VPC	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)
CloudWatch h.15	CloudWatch gli allarmi dovrebbero avere azioni specificate configurate	NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 Sì	Modifica attivata
CloudWatch h.16	CloudWatch i gruppi di log devono essere conservati per un periodo di tempo specificato	NIST SP 800-53 Rev. 5	MEDIO	 Sì	Periodic (Periodico)





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CloudWatch h.17	CloudWatch le azioni di allarme devono essere abilitate	NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Modifica attivata
CodeArtifact1.	CodeArtifact i repository devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	 Sì	Modifica attivata
CodeBuild 1.	CodeBuild Gli URL del repository di origine di Bitbucket non devono contenere credenziali riservate	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5 AWS Control Tower	CRITICO	 No	Modifica attivata
CodeBuild 2.	CodeBuild le variabili di ambiente del progetto non devono contenere credenziali di testo non crittografato	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, NIST SP AWS Control Tower 800-53 Rev. 5	CRITICO	 No	Modifica attivata
CodeBuild 3.	CodeBuild I log S3 devono essere crittografati	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
CodeBuild 4.	CodeBuild gli ambienti di progetto dovrebbero avere una configurazione di registrazione	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
Config.1	AWS Config dovrebbe essere abilitato	Benchmark CIS AWS Foundations v1.2.0, buone pratiche di sicurezza di base v1.0.0, PCI DSS v3.2.1, benchmark CIS AWS Foundations v1.4.0, NIST SP 800-53 Rev. 5 AWS	MEDIO	 No	Periodic (Periodico)
DataFirehose1.	I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi	AWS Migliori pratiche di sicurezza di base NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
Detective .1	I grafici del comportamento dei Detective devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
DMS.1	Le istanze di replica del Database Migration Service non devono essere pubbliche	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: , PCI DSS v3.2.1, NIST SP 800-53 AWS Control Tower Rev. 5	CRITICO	 No	Periodic (Periodico)
DMS.2	I certificati DMS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
DMS.3	Le sottoscrizioni agli eventi DMS devono essere contrassegnate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
DMS.4	Le istanze di replica DMS devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
DMS.5	I sottoreti di replica DMS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
DMS.6	L'aggiornamento automatico delle versioni secondarie delle istanze di replica DMS deve essere abilitato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
DMS.7	Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
DMS.8	Le attività di replica DMS per il database di origine devono avere la registrazione abilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
DMS.9	Gli endpoint DMS devono utilizzare SSL	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
DMS.10	Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
DMS.11	Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato	AWS Migliori pratiche di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
DMS.12	Gli endpoint DMS per Redis devono avere TLS abilitato	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Documento DB.1	I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, Service Managed Standard: AWS Control Tower	MEDIO	 No	Modifica attivata
Documento DB.2	I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, Service Managed Standard: AWS Control Tower	MEDIO	 Sì	Modifica attivata
Documento DB.3	Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	CRITICO	 No	Modifica attivata
Documento DB.4	I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
Documento DB.5	I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
DynamoDB 1	Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sì	Periodic (Periodico)
DynamoDB 2	Le tabelle DynamoDB devono avere il ripristino abilitato point-in-time	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
DynamoDB 3	I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
DynamoDB.4	Le tabelle DynamoDB devono essere presenti in un piano di backup	NIST SP 800-53 Rev. 5	MEDIO	 Sì	Periodic (Periodico)
DynamoDB.5	Le tabelle DynamoDB devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
DynamoDB.6	Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
DynamoDB.7	I cluster DynamoDB Accelerator devono essere crittografati in transito	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
EC2.1	Le istantanee EBS non devono essere ripristinabili pubblicamente	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, NIST SP 800-53 Rev. AWS Control Tower 5	CRITICO	 No	Periodic (Periodico)
EC2.2	I gruppi di sicurezza VPC predefiniti non devono consentire il traffico in entrata o in uscita	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, benchmark CIS Foundations v1.4.0, NIST SP 800-53 AWS Control Tower Rev. 5 AWS	HIGH (ELEVATO)	 No	Modifica attivata


ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.3	I volumi EBS collegati devono essere crittografati quando sono inattivi	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
EC2.4	Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sì	Periodic (Periodico)
EC2.6	La registrazione del flusso VPC deve essere abilitata in tutti i VPC	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 AWS Control Tower Rev. 5 AWS	MEDIO	 No	Periodic (Periodico)

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.7	La crittografia predefinita di EBS deve essere abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
EC2.8	Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata
EC2.9	Le istanze EC2 non devono avere un indirizzo IPv4 pubblico	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata
EC2.10	Amazon EC2 deve essere configurato per utilizzare endpoint VPC creati per il servizio Amazon EC2.	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Periodic (Periodico)



ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.12	Le EIP EC2 non utilizzate devono essere rimosse	PCI DSS versione 3.2.1, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
EC2.13	I gruppi di sicurezza non devono consentire e l'accesso da 0.0.0.0/0 o :/0 alla porta 22	Benchmark CIS AWS Foundations v1.2.0, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Modifica attivata
EC 2.14	I gruppi di sicurezza non dovrebbero consentire l'accesso da 0.0.0.0/0 o :/0 alla porta 3389	AWS Benchmark CIS Foundations v1.2.0	HIGH (ELEVATO)	 No	Modifica attivata
EC2.15	Le sottoreti EC2 non devono assegnare automaticamente indirizzi IP pubblici	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
EC2.16	Gli elenchi di controllo degli accessi alla rete non utilizzati devono essere rimossi	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.17	Le istanze EC2 non devono utilizzare più ENI	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata
EC2.18	I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 Sì	Modifica attivata
EC2.19	I gruppi di sicurezza non dovrebbero consentire l'accesso illimitato alle porte ad alto rischio	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	CRITICO	 No	Modifica attivata
EC2.20	Entrambi i tunnel VPN per una connessione VPN da AWS sito a sito dovrebbero essere attivi	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.21	Gli ACL di rete non devono consentire l'ingresso dalla porta 0.0.0.0/0 alla porta 22 o alla porta 3389	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard: , CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5 AWS Control Tower AWS	MEDIO	 No	Modifica attivata
EC2.22	I gruppi di sicurezza EC2 non utilizzati devono essere rimossi	Standard gestito dai servizi: AWS Control Tower	MEDIO	 No	Periodic (Periodico)
EC2.23	I gateway di transito EC2 non dovrebbero accettare automaticamente le richieste di allegati VPC	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Modifica attivata
EC2.24	I tipi di istanze paravirtuali EC2 non devono essere utilizzati	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
EC2.25	I modelli di lancio EC2 non devono assegnare IP pubblici alle interfacce di rete	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: , NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2,28	I volumi EBS devono essere inclusi in un piano di backup	NIST SP 800-53 Rev. 5	BASSO	 Sì	Periodic (Periodico)
EC2,33	Gli allegati del gateway di transito EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,34	Le tabelle delle rotte dei gateway di transito EC2 devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,35	Le interfacce di rete EC2 devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,36	I gateway per i clienti EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,37	Gli indirizzi IP elastici EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,38	Le istanze EC2 devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2,39	I gateway Internet EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,40	I gateway NAT EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2.41	Gli ACL di rete EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,42	Le tabelle delle rotte EC2 devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,43	I gruppi di sicurezza EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,44	Le sottoreti EC2 devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,45	I volumi EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,46	I VPC Amazon devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2,47	I servizi endpoint Amazon VPC devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,48	I log di flusso di Amazon VPC devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,49	Le connessioni peering Amazon VPC devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,50	I gateway VPN EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,51	Gli endpoint EC2 Client VPN devono avere la registrazione della connessione client abilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
EC2,52	I gateway di transito EC2 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EC2,53	I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da 0.0.0.0/0 alle porte di amministrazione remota del server	AWS Benchmark CIS Foundations v3.0.0	HIGH (ELEVATO)	 No	Periodic (Periodico)





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EC2.54	I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da :/0 alle porte di amministrazione remota del server	Benchmark CIS Foundations v3.0.0 AWS	HIGH (ELEVATO)	 No	Periodic (Periodico)
ECR.1	I repository privati ECR dovrebbero avere la scansione delle immagini configurata	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Periodic (Periodico)
ECR.2	Gli archivi privati ECR devono avere l'immutabilità dei tag configurata	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ECR.3	Gli archivi ECR devono avere almeno una politica del ciclo di vita configurata	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ECR.4	Gli archivi pubblici ECR devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata







ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ECS.1	Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata
ECS.2	Ai servizi ECS non dovrebbero essere assegnati automaticamente indirizzi IP pubblici	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata
ECS.3	Le definizioni delle attività ECS non devono condividere lo spazio dei nomi del processo dell'host	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata
ECS.4	I contenitori ECS devono essere eseguiti come non privilegiati	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ECS.5	I contenitori ECS devono essere limitati all'accesso in sola lettura ai filesystem root	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata
ECS.8	I segreti non devono essere passati come variabili di ambiente del contenitore	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Modifica attivata
ECS.9	Le definizioni delle attività ECS devono avere una configurazione di registrazione	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Modifica attivata
ECS.10	I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ECS.12	I cluster ECS devono utilizzare Container Insights	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ECS.13	I servizi ECS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
ECS.14	I cluster ECS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
ECS.15	Le definizioni delle attività ECS devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EFS.1	Elastic File System deve essere configurato per crittografare i dati dei file archiviati utilizzando AWS KMS	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Periodic (Periodico)
EFS.2	I volumi Amazon EFS devono essere inclusi nei piani di backup	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EFS.3	I punti di accesso EFS devono applicare una directory principale	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
EFS.4	I punti di accesso EFS devono applicare un'identità utente	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
EFS.5	I punti di accesso EFS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	 Sì	Modifica attivata
EFS.6	Gli obiettivi di montaggio EFS non devono essere associati a una sottorete pubblica	AWS Migliori pratiche di sicurezza di base	MEDIO	 No	Periodic (Periodico)
EKS.1	Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico	AWS Migliori pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Periodic (Periodico)





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EKS.2	I cluster EKS devono essere eseguiti su una versione di Kubernetes supportata	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata
EKS.3	I cluster EKS devono utilizzare segreti Kubernetes crittografati	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
EKS.6	I cluster EKS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EKS.7	Le configurazioni dei provider di identità EKS devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EKS.8	I cluster EKS dovrebbero avere la registrazione di controllo abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
ElastiCache1.	ElastiCache I cluster Redis devono avere il backup automatico abilitato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 Sì	Periodic (Periodico)





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ElastiCache2.	ElastiCache per i cluster di cache Redis dovrebbero essere abilitati gli aggiornamenti automatici delle versioni secondarie	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Periodic (Periodico)
ElastiCache3.	ElastiCache i gruppi di replica devono avere il failover automatico abilitato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
ElastiCache4.	ElastiCache i gruppi di replica avrebbero dovuto essere abilitati encryption-at-rest	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
ElastiCache5.	ElastiCache i gruppi di replica avrebbero dovuto essere abilitati encryption-in-transit	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
ElastiCache6.	ElastiCache i gruppi di replica delle versioni precedenti di Redis devono avere Redis AUTH abilitato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
ElastiCache7.	ElastiCache i cluster non devono utilizzare e il gruppo di sottoreti predefinito	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Periodic (Periodico)





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ElasticBeanstalk1.	Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sanitaria avanzata abilitata	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata
ElasticBeanstalk2.	Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 Sì	Modifica attivata
ElasticBeanstalk3.	Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch	AWS Migliori pratiche di sicurezza di base v1.0.0	HIGH (ELEVATO)	 Sì	Modifica attivata
ELB.1	Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, NIST SP 800-53 AWS Control Tower Rev. 5	MEDIO	 No	Periodic (Periodico)




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ELB.2	I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ELB.3	I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ELB.4	Application Load Balancer deve essere configurato per eliminare le intestazioni http	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ELB.5	La registrazione di Application e Classic Load Balancers deve essere abilitata	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ELB.6	Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata	AWS Best practice di sicurezza di base, Service Managed Standard:, NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO	 No	Modifica attivata
ELB.7	I Classic Load Balancer dovrebbero avere abilitato il drenaggio della connessione	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ELB.8	I Classic Load Balancer con listener SSL devono utilizzare e una politica di sicurezza predefinita con una configurazione avanzata	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ELB.9	I sistemi Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata



ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ELB.10	Classic Load Balancer dovrebbe estendersi su più zone di disponibilità	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sì	Modifica attivata
ELB.12	Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa.	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ELB.13	I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sì	Modifica attivata
ELB.14	Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa.	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata



ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ELB.16	Gli Application Load Balancer devono essere associati a un ACL web AWS WAF	NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
EMR.1	I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Periodic (Periodico)
EMR.2	L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	CRITICO	 No	Periodic (Periodico)
ES.1	I domini Elasticsearch devono avere la crittografia a riposo abilitata	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: AWS Control Tower, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)



ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ES.2	I domini Elasticsearch non dovrebbero essere accessibili al pubblico	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, NIST SP 800-53 Rev. AWS Control Tower 5	CRITICO	 No	Periodic (Periodico)
ES.3	I domini Elasticsearch devono crittografare i dati inviati tra i nodi	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ES.4	La registrazione degli errori del dominio Elasticsearch nei registri deve essere abilitata CloudWatch	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ES.5	I domini Elasticsearch devono avere la registrazione di controllo abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
ES.6	I domini Elasticsearch devono avere almeno tre nodi di dati	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ES.7	I domini Elasticsearch devono essere configurati con almeno tre nodi master dedicati	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ES.8	Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS	AWS Best practice di sicurezza di base, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
ES.9	I domini Elasticsearch devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
EventBridge2.	EventBridge gli event bus devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
EventBridge3.	EventBridge i bus di eventi personalizzati devono avere una politica basata sulle risorse allegata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
EventBridge4.	EventBridge gli endpoint globali dovrebbero avere la replica degli eventi abilitata	NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
FSX.1	I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi.	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
FSX.2	I file system FSx for Lustre devono essere configurati per copiare i tag nei backup.	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
Colla.1	AWS Glue i lavori devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
GlobalAccelerator1.	Gli acceleratori Global Accelerator devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
GuardDuty 1.	GuardDuty dovrebbe essere abilitato	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Periodic (Periodico)
GuardDuty 2.	GuardDuty i filtri devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
GuardDuty 3.	GuardDuty Gli IPset devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
GuardDuty 4.	GuardDuty i rilevatori devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IAM.1	Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	HIGH (ELEVATO)	 No	Modifica attivata







ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.2	Gli utenti IAM non devono avere policy IAM allegate	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard: AWS Control Tower, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
IAM.3	Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5 AWS Control Tower AWS	MEDIO	 No	Periodic (Periodico)




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.4	La chiave di accesso utente root IAM non dovrebbe esistere	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	CRITICO	 No	Periodic (Periodico)
IAM.5	L'MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password di console	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard: AWS Control Tower, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5 AWS	MEDIO	 No	Periodic (Periodico)




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.6	La MFA hardware deve essere abilitata per l'utente root	CIS AWS Foundations Benchmark v1.2.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, CIS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5 AWS	CRITICO	 No	Periodic (Periodico)
IAM.7	Le politiche relative alle password per gli utenti IAM dovrebbero avere configurazioni solide	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sì	Periodic (Periodico)
IAM.8	Le credenziali utente IAM non utilizzate e devono essere rimosse	Benchmark CIS AWS Foundations v1.2.0, AWS Foundational Security Best Practices v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Periodic (Periodico)





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.9	L'MFA deve essere abilitata per l'utente root	Benchmark CIS AWS Foundations versione 1.2.0, PCI DSS versione 3.2.1, benchmark CIS Foundations versione 1.4.0, NIST SP AWS 800-53 Rev. 5	CRITICO	 No	Periodic (Periodico)
IO SONO 10	Le politiche relative alle password per gli utenti IAM devono avere configurazioni solide	PCI DSS v3.2.1	MEDIO	 No	Periodic (Periodico)
IAM.11	Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola	Benchmark CIS Foundations v1.2.0 AWS	MEDIO	 No	Periodic (Periodico)
IAM.12	Assicurati che la politica delle password IAM richieda almeno una lettera minuscola	Benchmark CIS Foundations v1.2.0 AWS	MEDIO	 No	Periodic (Periodico)
IAM.13	Assicurati che la politica delle password IAM richieda almeno un simbolo	Benchmark CIS AWS Foundations v1.2.0	MEDIO	 No	Periodic (Periodico)






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IAM.14	Assicurati che la politica delle password IAM richieda almeno un numero	Benchmark CIS AWS Foundations v1.2.0	MEDIO	 No	Periodic (Periodico)
IAM.15	Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	MEDIO	 No	Periodic (Periodico)
IAM.16	Verifica che la policy delle password di IAM impedisca il riutilizzo delle password	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)
IAM.17	Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno	Benchmark CIS Foundations v1.2.0 AWS	BASSO	 No	Periodic (Periodico)
IAM.18	Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support	Benchmark CIS AWS Foundations v1.2.0, benchmark CIS Foundations v1.4.0 AWS	BASSO	 No	Periodic (Periodico)






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IO HO 19 ANNI	L'MFA deve essere abilitata per tutti gli utenti IAM	PCI DSS versione 3.2.1, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
IAM.21	Le policy gestite dai clienti IAM che crei non dovrebbero consentire azioni jolly per i servizi	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata
IO HO 22 ANNI	Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse	Benchmark CIS Foundations v1.4.0 AWS	MEDIO	 No	Periodic (Periodico)
IO HO 23 ANNI	Gli analizzatori IAM Access Analyzer devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	 Sì	Modifica attivata
IO HO 24 ANNI	I ruoli IAM devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	 Sì	Modifica attivata
HO 25 ANNI	Gli utenti IAM devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	 Sì	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IO HO 26 ANNI	I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi	AWS Benchmark CIS Foundations v3.0.0	MEDIO	 No	Periodic (Periodico)
IO SONO 0,27	La policy non dovrebbe essere allegata alle identità IAM AWSCloudShellFullAccess	Benchmark CIS AWS Foundations v3.0.0	MEDIO	 No	Modifica attivata
IO HO 28 ANNI	L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato	Benchmark CIS Foundations v3.0.0 AWS	HIGH (ELEVATO)	 No	Periodic (Periodico)
IoT.1	AWS IoT Core i profili di sicurezza devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoT.2	AWS IoT Core le azioni di mitigazione devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoT.3	AWS IoT Core le dimensioni devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoT 4	AWS IoT Core gli autorizzatori devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
IoT.5	AWS IoT Core gli alias di ruolo devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
IoT.6	AWS IoT Core le politiche devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Kinesis.1	Gli stream Kinesis devono essere crittografati quando sono inattivi	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
Kinesis.2	Gli stream Kinesis devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
KMS.1	Le politiche gestite dai clienti IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
KMS.2	I responsabili IAM non dovrebbero disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
KMS.3	AWS KMS keys non deve essere eliminato involontariamente	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	CRITICO	 No	Modifica attivata
KMS.4	AWS KMS key la rotazione dovrebbe essere abilitata	Benchmark CIS AWS Foundations versione 1.2.0, PCI DSS versione 3.2.1, benchmark CIS Foundations versione 1.4.0, NIST SP 800-53 Rev. 5 AWS	MEDIO	 No	Periodic (Periodico)
Lambda.1	Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, NIST SP 800-53 AWS Control Tower Rev. 5	CRITICO	 No	Modifica attivata
Lambda.2	Le funzioni Lambda devono utilizzare runtime supportati	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Lambda.3	Le funzioni Lambda devono trovarsi in un VPC	PCI DSS versione 3.2.1, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
Lambda.5	Le funzioni VPC Lambda devono funzionare in più zone di disponibilità	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sì	Modifica attivata
Lambda.6	Le funzioni Lambda devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Macie.1	Amazon Macie dovrebbe essere abilitato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
Macie.2	Il rilevamento automatico dei dati sensibili di Macie dovrebbe essere abilitato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Periodic (Periodico)
MSK.1	I cluster MSK devono essere crittografati durante il transito tra i nodi del broker	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
MSK.2	I cluster MSK dovrebbero avere un monitoraggio avanzato configurato	NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
MQ. 2	I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch	AWS Migliori pratiche di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
MQ. 3	I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
MQ.4	I broker Amazon MQ devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
MQ.5	I broker ActiveMQ devono utilizzare la modalità di distribuzione attiva/standby	NIST SP 800-53 Rev. 5, Standard di gestione dei servizi: AWS Control Tower	BASSO	 No	Modifica attivata
MQ.6	I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione cluster	NIST SP 800-53 Rev. 5, Standard di gestione dei servizi: AWS Control Tower	BASSO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Nettuno.1	I cluster Neptune DB devono essere crittografati quando sono inattivi	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, Service Managed Standard: AWS Control Tower	MEDIO	 No	Modifica attivata
Nettuno.2	I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, Service Managed Standard: AWS Control Tower	MEDIO	 No	Modifica attivata
Nettuno.3	Le istantanee del cluster Neptune DB non devono essere pubbliche	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, Service Managed Standard: AWS Control Tower	CRITICO	 No	Modifica attivata
Nettuno.4	I cluster Neptune DB devono avere la protezione da eliminazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, Service Managed Standard: AWS Control Tower	BASSO	 No	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Nettuno.5	I cluster Neptune DB devono avere i backup automatici abilitati	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, Service Managed Standard: AWS Control Tower	MEDIO	 Sì	Modifica attivata
Nettuno.6	Le istantanee del cluster Neptune DB devono essere crittografate a riposo	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, Service Managed Standard: AWS Control Tower	MEDIO	 No	Modifica attivata
Nettuno.7	I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, Service Managed Standard: AWS Control Tower	MEDIO	 No	Modifica attivata
Nettuno.8	I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, Service Managed Standard: AWS Control Tower	BASSO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Nettuno.9	I cluster Neptune DB devono essere distribuiti su più zone di disponibilità	NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
NetworkFirewall1.	I firewall Network Firewall devono essere implementati su più zone di disponibilità	NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
NetworkFirewall2.	La registrazione del Network Firewall deve essere abilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
NetworkFirewall3.	Le policy del Network Firewall devono avere almeno un gruppo di regole associato	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
NetworkFirewall4.	L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere «drop or forward» per pacchetti completi.	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
NetworkFirewall5.	L'azione stateless predefinita per le policy di Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
NetworkFirewall6.	Il gruppo di regole del firewall di rete stateless non deve essere vuoto	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
NetworkFirewall7.	I firewall Network Firewall devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
NetworkFirewall8.	Le politiche firewall del Network Firewall devono essere contrassegnate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
NetworkFirewall9.	I firewall Network Firewall devono avere la protezione da eliminazione abilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Opensearch h.1	OpenSearch i domini devono avere la crittografia a riposo abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard: , PCI DSS v3.2.1, NIST SP AWS Control Tower 800-53 Rev. 5	MEDIO	 No	Modifica attivata
Opensearch h.2	OpenSearch i domini non dovrebbero essere accessibili al pubblico	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: , PCI DSS v3.2.1, NIST SP AWS Control Tower 800-53 Rev. 5	CRITICO	 No	Modifica attivata
Opensearch h.3	OpenSearch i domini devono crittografare i dati inviati tra i nodi	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
Opensearch h.4	OpenSearch la registrazione degli errori di dominio nei CloudWatch registri dovrebbe essere abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Opensearch h.5	OpenSearch i domini devono avere la registrazione di controllo abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
Opensearch h.6	OpenSearch i domini devono avere almeno tre nodi di dati	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
Opensearch h.7	OpenSearch i domini devono avere un controllo granulare degli accessi abilitato	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata
Opensearch h.8	Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la politica di sicurezza TLS più recente	AWS Best practice di sicurezza di base, Service Managed Standard:, NIST SP 800-53 Rev. AWS Control Tower 5	MEDIO	 No	Modifica attivata
Ricerca aperta. 9	OpenSearch i domini devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Ricerca aperta. 10	OpenSearch nei domini dovrebbe essere installato l'ultimo aggiornamento software	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
Ricerca aperta. 11	OpenSearch i domini devono avere almeno tre nodi primari dedicati	NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
PCA.1	AWS Private CA l'autorità di certificazione principale deve essere disabilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	BASSO	 No	Periodic (Periodico)
RDS.1	L'istanza RDS deve essere privata	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: , PCI DSS v3.2.1, NIST SP 800-53 AWS Control Tower Rev. 5	CRITICO	 No	Modifica attivata
RDS.2	Le istanze DB RDS devono vietare l'accesso pubblico, come stabilito dalla configurazione PubliclyAccessible	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, NIST SP 800-53 Rev. AWS Control Tower 5	CRITICO	 No	Modifica attivata




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.3	Le istanze DB RDS devono avere la crittografia a riposo abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard: , CIS Foundations Benchmark v1.4.0, NIST SP 800-53 AWS Control Tower AWS Rev. 5	MEDIO	 No	Modifica attivata
RDS.4	Le istantanee del cluster RDS e le istantanee del database devono essere crittografate quando sono inattive	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
RDS.5	Le istanze DB RDS devono essere configurate con più zone di disponibilità	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
RDS.6	Il monitoraggio avanzato deve essere configurato per le istanze DB RDS	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 Sì	Modifica attivata




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.7	I cluster RDS devono avere la protezione da eliminazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
RDS.8	Le istanze DB RDS devono avere la protezione da eliminazione abilitata	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata
RDS.9	Le istanze DB RDS devono pubblicare i log in Logs CloudWatch	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
RDS.10	L'autenticazione IAM deve essere configurata per le istanze RDS	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
RDS.11	Le istanze RDS devono avere i backup automatici abilitati	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sì	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.12	L'autenticazione IAM deve essere configurata per i cluster RDS	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
RDS.13	Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata
RDS.14	I cluster Amazon Aurora dovrebbero avere il backtracking abilitato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 Sì	Modifica attivata
RDS.15	I cluster RDS DB devono essere configurati per più zone di disponibilità	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
RDS.16	I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.17	Le istanze DB RDS devono essere configurate per copiare i tag nelle istantanee	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata
RDS.18	Le istanze RDS devono essere distribuite in un VPC	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata
RDS.19	Gli abbonamenti esistenti per la notifica degli eventi RDS devono essere configurati per gli eventi critici del cluster	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata
RDS.20	Gli abbonamenti esistenti per la notifica degli eventi RDS devono essere configurati per gli eventi critici delle istanze di database	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata



ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.21	È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici del gruppo di parametri del database	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata
RDS.22	È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici dei gruppi di sicurezza del database	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata
RDS.23	Le istanze RDS non devono utilizzare una porta predefinita del motore di database	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 No	Modifica attivata
RDS.24	I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.25	Le istanze del database RDS devono utilizzare e un nome utente di amministratore personalizzato	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
RDS.26	Le istanze DB RDS devono essere protette da un piano di backup	NIST SP 800-53 Rev. 5	MEDIO	 Sì	Periodic (Periodico)
RDS.27	I cluster RDS DB devono essere crittografati quando sono inattivi	AWS Buone pratiche di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5, Service Managed Standard: AWS Control Tower	MEDIO	 No	Modifica attivata
RDS.28	I cluster DB RDS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
RDS.29	Le istantanee del cluster RDS DB devono essere contrassegnate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
RDS.30	Le istanze DB RDS devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
RDS.31	I gruppi di sicurezza RDS DB devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
RDS.32	Le istantanee RDS DB devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
RDS.33	I gruppi di sottoreti RDS DB devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
RDS.34	I cluster Aurora MySQL DB devono pubblicare i log di controllo su Logs CloudWatch	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
RDS.35	Nei cluster RDS DB dovrebbe essere abilitato l'aggiornamento automatico delle versioni secondarie	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
Redshift.1	I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, NIST SP 800-53 Rev. AWS Control Tower 5	CRITICO	 No	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Redshift. 2	Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
Redshift. 3	I cluster Amazon Redshift devono avere le istantanee automatiche abilitate	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 Sì	Modifica attivata
Redshift. 4	I cluster Amazon Redshift devono avere la registrazione di controllo abilitata	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
Redshift. 6	Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
Redshift. 7	I cluster Redshift devono utilizzare un routing VPC avanzato	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata







ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Redshift. 8	I cluster Amazon Redshift non devono utilizzare il nome utente amministratore predefinito	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
Redshift. 9	I cluster Redshift non devono utilizzare il nome di database predefinito	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
Redshift. 10	I cluster Redshift devono essere crittografati quando sono inattivi	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
Redshift. 11	I cluster Redshift devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Redshift. 12	Le notifiche di sottoscrizione agli eventi Redshift devono essere contrassegnate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Redshift 13	Le istantanee del cluster Redshift devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Redshift 14	I gruppi di sottoreti del cluster Redshift devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Redshift 15	I gruppi di sicurezza Redshift dovrebbero consentire l'accesso alla porta del cluster solo da origini limitate	AWS Le migliori pratiche di sicurezza di base	HIGH (ELEVATO)	 No	Periodic (Periodico)
Percorso 53.1	I controlli sanitari della Route 53 devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Percorso 53.2	Le zone ospitate pubbliche di Route 53 devono registrare le query DNS	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
S3.1	I bucket S3 per uso generico devono avere le impostazioni di blocco dell'accesso pubblico abilitate	AWS Best practice di sicurezza di base, Service Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5 AWS	MEDIO	 No	Periodico (Periodico)
S3.2	I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico alla lettura	AWS Best practice di sicurezza di base, Service Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	CRITICO	 No	Modifica attivata e periodica
S3.3	I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura	AWS Best practice di sicurezza di base, Service Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, NIST SP 800-53 Rev. 5	CRITICO	 No	Modifica attivata e periodica


ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
S3.5	I bucket S3 per uso generico dovrebbero richiedere l'utilizzo di SSL	AWS Best practice di sicurezza di base, Service Managed Standard:, PCI DSS v3.2.1 AWS Control Tower, CIS Foundations Benchmark v1.4.0, NIST SP 800-53 Rev. 5 AWS	MEDIO	 No	Modifica attivata
S3.6	Le policy relative ai bucket per uso generico di S3 dovrebbero limitare l'accesso ad altri Account AWS	AWS Best practice di sicurezza di base, Service Managed Standard:, NIST SP 800-53 Rev. AWS Control Tower 5	HIGH (ELEVATO)	 No	Modifica attivata
S3.7	I bucket S3 per uso generico devono utilizzare la replica tra regioni	PCI DSS versione 3.2.1, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
S3.8	I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico	AWS Best practice di sicurezza di base, Service Managed Standard:, CIS AWS Foundations Benchmark v1.4.0 AWS Control Tower, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Modifica attivata




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
S3.9	I bucket S3 per uso generico devono avere la registrazione degli accessi al server abilitata	AWS Best practice di sicurezza di base, Service Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
S3.10	I bucket S3 per uso generico con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita	NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
S3.11	I bucket S3 per uso generico devono avere le notifiche degli eventi abilitate	NIST SP 800-53 Rev. 5	MEDIO	 Sì	Modifica attivata
S3.12	Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3	AWS Best practice di sicurezza di base, Service Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
S3.13	I bucket S3 per uso generico devono avere configurazioni del ciclo di vita	AWS Best practice di sicurezza di base, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	BASSO	 Sì	Modifica attivata




ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
S3.14	I bucket S3 per uso generico devono avere il controllo delle versioni abilitato	NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
S3.15	I bucket S3 per uso generico devono avere Object Lock abilitato	NIST SP 800-53 Rev. 5	MEDIO	 Sì	Modifica attivata
S3.17	I bucket S3 per uso generico devono essere crittografati quando sono inattivi con AWS KMS keys	Standard gestito dai servizi: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
S3.19	I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate	AWS Migliori pratiche di sicurezza di base, NIST SP 800-53 Rev. 5	CRITICO	 No	Modifica attivata
S3.20	I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata	Benchmark CIS AWS Foundations v1.4.0, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
S3.22	I bucket S3 per uso generico dovrebbero registrare gli eventi di scrittura a livello di oggetto	Benchmark CIS Foundations v3.0.0 AWS	MEDIO	 No	Periodic (Periodico)





ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
S3.23	I bucket S3 per uso generico dovrebbero registrare gli eventi di lettura a livello di oggetto	Benchmark CIS Foundations v3.0.0 AWS	MEDIO	 No	Periodic (Periodico)
SageMaker 1.	Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: , PCI DSS v3.2.1, NIST SP AWS Control Tower 800-53 Rev. 5	HIGH (ELEVATO)	 No	Periodic (Periodico)
SageMaker 2.	SageMaker le istanze dei notebook devono essere avviate in un VPC personalizzato	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata
SageMaker 3.	Gli utenti non devono avere accesso root alle istanze del SageMaker notebook	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	HIGH (ELEVATO)	 No	Modifica attivata






ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SageMaker 4.	SageMaker le varianti di produzione e endpoint devono avere un numero iniziale di istanze maggiore di 1	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
SecretsManager1.	I segreti di Secrets Manager devono avere la rotazione automatica abilitata	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 Sì	Modifica attivata
SecretsManager2.	I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
SecretsManager3.	Rimuovi i segreti inutilizzati di Secrets Manager	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sì	Periodic (Periodico)



ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SecretsManager4.	I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 Sì	Periodic (Periodico)
SecretsManager5.	I segreti di Secrets Manager devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
ServiceCatalog1.	I portafogli Service Catalog devono essere condivisi solo all'interno di un' AWS organizzazione	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Periodic (Periodico)
VES.1	Gli elenchi di contatti SES devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
SES.2	I set di configurazione SES devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
SNS.1	Gli argomenti SNS devono essere crittografati a riposo utilizzando AWS KMS	NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
SNS.3	Gli argomenti SNS devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SQS.1	Le code di Amazon SQS devono essere crittografate quando sono inattive	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
SQS.2	Le code SQS devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
SSM.1	Le istanze EC2 devono essere gestite da AWS Systems Manager	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, PCI DSS v3.2.1, NIST SP 800-53 AWS Control Tower Rev. 5	MEDIO	 No	Modifica attivata
SSM.2	Le istanze EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch.	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: AWS Control Tower, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	HIGH (ELEVATO)	 No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
SSM.3	Le istanze EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard: AWS Control Tower, PCI DSS v3.2.1, NIST SP 800-53 Rev. 5	BASSO	 No	Modifica attivata
SSM.4	I documenti SSM non devono essere pubblici	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	CRITICO	 No	Periodic (Periodico)
StepFunctions1.	Le macchine a stati Step Functions dovrebbero avere la registrazione attivata	AWS Migliori pratiche di sicurezza di base	MEDIO	 Sì	Modifica attivata
StepFunctions2.	Le attività di Step Functions devono essere etichettate	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata
Trasferimento.1	I flussi di lavoro Transfer Family devono essere etichettati	AWS Standard di etichettatura delle risorse	BASSO	Sì	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
Trasferimento.2	I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint	AWS Best practice di sicurezza di base, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
WAF.1	AWS WAF La registrazione classica Global Web ACL deve essere abilitata	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Periodic (Periodico)
WAF.2	AWS WAF Le regole regionali classiche devono avere almeno una condizione	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
WAF.3	AWS WAF I gruppi di regole regionali classici devono avere almeno una regola	AWS Buone pratiche di sicurezza di base v1.0.0, Service Managed Standard: AWS Control Tower, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
WAF.4	AWS WAF Gli ACL Web regionali classici devono avere almeno una regola o un gruppo di regole	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata
WAF.6	AWS WAF Le regole globali classiche devono avere almeno una condizione	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
WAF.7	AWS WAF I gruppi di regole globali classici devono avere almeno una regola	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
WAF.8	AWS WAF Gli ACL Web globali classici devono avere almeno una regola o un gruppo di regole	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata
WAF.10	AWS WAF gli ACL web devono avere almeno una regola o un gruppo di regole	AWS Best practice di sicurezza di base v1.0.0, Service Managed Standard:, NIST SP 800-53 Rev. 5 AWS Control Tower	MEDIO	 No	Modifica attivata

ID del controllo di sicurezza	Titolo del controllo di sicurezza	Standard applicabili	Gravità	Supporta parametri personalizzati	Tipo di pianificazione
WAF.11	AWS WAF la registrazione ACL web deve essere abilitata	NIST SP 800-53 Rev. 5	BASSO	 No	Periodic (Periodico)
AF.12	AWS WAF le regole dovrebbero avere le metriche abilitate CloudWatch	AWS Best practice di sicurezza di base v1.0.0, NIST SP 800-53 Rev. 5	MEDIO	 No	Modifica attivata

Argomenti

- [Account AWS controlli](#)
- [AWS Certificate Manager controlli](#)
- [Controlli Amazon API Gateway](#)
- [AWS AppSync controlli](#)
- [Controlli Amazon Athena](#)
- [AWS Backup controlli](#)
- [AWS CloudFormation controlli](#)
- [CloudFront Controlli Amazon](#)
- [AWS CloudTrail controlli](#)
- [CloudWatch Controlli Amazon](#)
- [AWS CodeArtifact controlli](#)
- [AWS CodeBuild controlli](#)
- [AWS Config controlli](#)
- [Controlli Amazon Data Firehose](#)
- [Controlli Amazon Detective](#)
- [AWS Database Migration Service controlli](#)

- [Controlli Amazon DocumentDB](#)
- [Controlli Amazon DynamoDB](#)
- [Controlli di Amazon Elastic Container Registry](#)
- [Controlli Amazon ECS](#)
- [Controlli Amazon Elastic Compute Cloud](#)
- [Controlli di Amazon EC2 Auto Scaling](#)
- [Controlli di Amazon EC2 Systems Manager](#)
- [Controlli Amazon Elastic File System](#)
- [Controlli di Amazon Elastic Kubernetes Service](#)
- [ElastiCache Controlli Amazon](#)
- [AWS Elastic Beanstalk controlli](#)
- [Controlli Elastic Load Balancing](#)
- [Controlli Amazon EMR](#)
- [Controlli Elasticsearch](#)
- [EventBridge Controlli Amazon](#)
- [Controlli Amazon FSx](#)
- [AWS Global Accelerator controlli](#)
- [AWS Glue controlli](#)
- [GuardDuty Controlli Amazon](#)
- [AWS Identity and Access Management controlli](#)
- [AWS IoT controlli](#)
- [Controlli Amazon Kinesis](#)
- [AWS Key Management Service controlli](#)
- [AWS Lambda controlli](#)
- [Controlli Amazon Macie](#)
- [Controlli Amazon MSK](#)
- [Controlli Amazon MQ](#)
- [Controlli Amazon Neptune](#)
- [AWS Network Firewall controlli](#)
- [Controlli OpenSearch di Amazon Service](#)

- [AWS Private Certificate Authority controlli](#)
- [Controlli di Amazon Relational Database Service](#)
- [Controlli Amazon Redshift](#)
- [Controlli Amazon Route 53](#)
- [Controlli di Amazon Simple Storage Service](#)
- [SageMaker Controlli Amazon](#)
- [AWS Secrets Manager controlli](#)
- [AWS Service Catalog controlli](#)
- [Controlli di Amazon Simple Email Service](#)
- [Controlli di Amazon Simple Notification Service](#)
- [Controlli di Amazon Simple Queue Service](#)
- [AWS Step Functions controlli](#)
- [AWS Transfer Family controlli](#)
- [AWS WAF controlli](#)

Account AWS controlli

Questi controlli sono correlati a Account AWS.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[Account.1] Le informazioni di contatto di sicurezza devono essere fornite per un Account AWS

Requisiti correlati: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificazione > Configurazione delle risorse

Gravità: media

Tipo di risorsa: AWS:::Account

Regola AWS Config : [security-account-information-provided](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un account Amazon Web Services (AWS) dispone di informazioni di contatto di sicurezza. Il controllo fallisce se non vengono fornite informazioni di contatto di sicurezza per l'account.

I contatti di sicurezza alternativi consentono di contattare un'altra persona in merito AWS a problemi relativi al tuo account nel caso in cui tu non sia disponibile. Le notifiche possono provenire da AWS Support o da altri Servizio AWS team su argomenti relativi alla sicurezza associati al tuo utilizzo.

Account AWS

Correzione

Per aggiungere un contatto alternativo come contatto di sicurezza al tuo Account AWS, consulta [Aggiungere, modificare o rimuovere contatti alternativi](#) nella AWS Billing and Cost Management User Guide.

[Account.2] Account AWS deve far parte di un'organizzazione AWS Organizations

Categoria: Protezione > Gestione sicura degli accessi > Controllo degli accessi

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Gravità: alta

Tipo di risorsa: AWS :: Account

Regola AWS Config : [account-part-of-organizations](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un Account AWS fa parte di un'organizzazione gestita tramite AWS Organizations. Il controllo ha esito negativo se l'account non fa parte di un'organizzazione.

Organizations ti aiuta a gestire centralmente il tuo ambiente man mano che ridimensioni i carichi di lavoro. AWS È possibile utilizzarne più Account AWS di uno per isolare i carichi di lavoro con requisiti di sicurezza specifici o per conformarsi a framework come HIPAA o PCI. Creando un'organizzazione, puoi amministrare più account come una singola unità e gestirne centralmente l'accesso, le risorse e le regioni. Servizi AWS

Correzione

Per creare una nuova organizzazione e Account AWS aggiungerla automaticamente, consulta [Creazione di un'organizzazione](#) nella Guida per l'AWS Organizations utente. Per aggiungere account a un'organizzazione esistente, vedi [Invitare un utente Account AWS a entrare a far parte della tua organizzazione](#) nella Guida per l'AWS Organizations utente.

AWS Certificate Manager controlli

Questi controlli sono correlati alle risorse ACM.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[ACM.1] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato

Requisiti correlati: NIST.800-53.r5 SC-28 (3), NIST.800-53.r5 SC-7 (16)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: AWS::ACM::Certificate

Regola AWS Config : [acm-certificate-expiration-check](#)

Tipo di pianificazione: modifica attivata e periodica

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
daysToExpiration	Numero di giorni entro i quali il certificato ACM deve essere rinnovato	Numero intero	14 Da a 365	30

Questo controllo verifica se un certificato AWS Certificate Manager (ACM) viene rinnovato entro il periodo di tempo specificato. Controlla sia i certificati importati che i certificati forniti da ACM. Il

controllo fallisce se il certificato non viene rinnovato entro il periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di rinnovo, Security Hub utilizza un valore predefinito di 30 giorni.

ACM può rinnovare automaticamente i certificati che utilizzano la convalida DNS. Per i certificati che utilizzano la convalida e-mail, è necessario rispondere a un'e-mail di convalida del dominio. ACM non rinnova automaticamente i certificati importati. È necessario rinnovare manualmente i certificati importati.

Correzione

ACM fornisce il rinnovo gestito per i tuoi certificati SSL/TLS emessi da Amazon. Ciò significa che ACM rinnova i certificati automaticamente (se utilizzi la convalida DNS) oppure ti invia notifiche via e-mail quando si avvicina la scadenza del certificato. Questi servizi sono forniti sia per i certificati ACM pubblici che privati.

Per i domini convalidati tramite e-mail

Quando mancano 45 giorni alla scadenza di un certificato, ACM invia al proprietario del dominio un'e-mail per ogni nome di dominio. Per convalidare i domini e completare il rinnovo, devi rispondere alle notifiche e-mail.

Per ulteriori informazioni, consulta [Rinnovo per domini convalidati tramite e-mail](#) nella Guida per l'utente AWS Certificate Manager.

Per i domini convalidati dal DNS

ACM rinnova automaticamente i certificati che utilizzano la convalida DNS. 60 giorni prima della scadenza, ACM verifica che il certificato possa essere rinnovato.

Se non è in grado di convalidare un nome di dominio, ACM invia una notifica indicante che è necessaria la convalida manuale. Invia queste notifiche 45 giorni, 30 giorni, 7 giorni e 1 giorno prima della scadenza.

Per ulteriori informazioni, consulta [Rinnovo per i domini convalidati dal DNS](#) nella Guida per l'AWS Certificate Manager utente.

[ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit

Categoria: Identifica > Inventario > Servizi di inventario

Gravità: alta

Tipo di risorsa: AWS::ACM::Certificate

Regola AWS Config : [acm-certificate-rsa-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i certificati RSA gestiti da AWS Certificate Manager utilizzano una lunghezza di chiave di almeno 2.048 bit. Il controllo ha esito negativo se la lunghezza della chiave è inferiore a 2.048 bit.

La forza della crittografia è direttamente correlata alla dimensione della chiave. Consigliamo una lunghezza delle chiavi di almeno 2.048 bit per proteggere AWS le risorse in quanto la potenza di calcolo diventa meno costosa e i server diventano più avanzati.

Correzione

La lunghezza minima delle chiavi per i certificati RSA emessi da ACM è già di 2.048 bit. Per istruzioni sull'emissione di nuovi certificati RSA con ACM, consulta [Emissione e gestione dei certificati nella Guida per l'utente.AWS Certificate Manager](#)

Sebbene ACM consenta di importare certificati con chiavi di lunghezza inferiore, è necessario utilizzare chiavi di almeno 2.048 bit per passare questo controllo. Non è possibile modificare la lunghezza della chiave dopo aver importato un certificato. È invece necessario eliminare i certificati con una lunghezza di chiave inferiore a 2.048 bit. Per ulteriori informazioni sull'importazione di certificati in ACM, consulta [Prerequisiti per l'importazione dei certificati nella Guida per l'utente.AWS Certificate Manager](#)

[ACM.3] I certificati ACM devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::ACM::Certificate

AWS Config regola: tagged-acm-certificate (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un certificato AWS Certificate Manager (ACM) contiene tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo ha esito negativo se il certificato non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il certificato non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un certificato ACM, consulta [Taggare i AWS Certificate Manager certificati](#) nella Guida per l'utente.AWS Certificate Manager

Controlli Amazon API Gateway

Questi controlli sono correlati alle risorse API Gateway.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[ApiGateway.1] API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati

Requisiti correlati: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 R5 CA-7, NIST. 800-53.R5 SC-7 (9), NIST. 800-53.5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa:AWS::ApiGateway::Stage, AWS::ApiGatewayV2::Stage

Regola AWS Config : [api-gw-execution-logging-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
loggingLevel	Livello di logging	Enum	ERROR, INFO	No default value

Questo controllo verifica se la registrazione è abilitata in tutte le fasi di un'API o REST di Amazon WebSocket API Gateway. Il controllo fallisce se `loggingLevel` non lo è `ERROR` o `INFO` per tutte le fasi dell'API. A meno che non si forniscano valori di parametri personalizzati per indicare che un tipo di registro specifico deve essere abilitato, Security Hub produce un risultato positivo se il livello di registrazione è uno `ERROR` o `INFO` l'altro.

API Gateway WebSocket REST o le fasi API devono avere i log pertinenti abilitati. La registrazione REST e l'esecuzione delle WebSocket API di API Gateway forniscono registrazioni dettagliate delle richieste effettuate alle fasi REST e API di WebSocket API Gateway. Le fasi includono le risposte di backend di integrazione delle API, le risposte di autorizzazione Lambda e gli endpoint per `requestId` l'AWS integrazione.

Correzione

Per abilitare la registrazione per le operazioni WebSocket REST e API, consulta [Configurare la registrazione delle CloudWatch API utilizzando la console API Gateway nella API Gateway Developer Guide](#).

[ApiGateway.2] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend

Requisiti correlati: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoria: Proteggi > Protezione dei dati

Gravità: media

Tipo di risorsa: AWS::ApiGateway::Stage

Regola AWS Config : [api-gw-ssl-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le fasi API REST di Amazon API Gateway hanno certificati SSL configurati. I sistemi di backend utilizzano questi certificati per autenticare che le richieste in entrata provengano da API Gateway.

Le fasi API REST di API Gateway devono essere configurate con certificati SSL per consentire ai sistemi di backend di autenticare che le richieste provengono da API Gateway.

Correzione

Per istruzioni dettagliate su come generare e configurare i certificati SSL API REST API Gateway, consulta [Generare e configurare un certificato SSL per l'autenticazione di backend nella Guida per sviluppatori di API Gateway](#).

[ApiGateway.3] Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray

Requisiti correlati: NIST.800-53.r5 CA-7

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa: AWS::ApiGateway::Stage

Regola AWS Config : [api-gw-xray-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il tracciamento AWS X-Ray attivo è abilitato per le fasi dell'API REST di Amazon API Gateway.

Il tracciamento attivo a raggi X consente una risposta più rapida ai cambiamenti delle prestazioni nell'infrastruttura sottostante. Le variazioni delle prestazioni potrebbero comportare una mancanza di disponibilità dell'API. Il tracciamento attivo di X-Ray fornisce metriche in tempo reale delle richieste degli utenti che fluiscono attraverso le operazioni dell'API REST dell'API Gateway e i servizi connessi.

Correzione

Per istruzioni dettagliate su come abilitare il tracciamento attivo a raggi X per le operazioni dell'API REST di API Gateway, consulta il [supporto per il tracciamento attivo di Amazon API Gateway AWS X-Ray](#) nella Developer Guide.AWS X-Ray

[ApiGateway.4] L'API Gateway deve essere associato a un ACL Web WAF

Requisiti correlati: NIST.800-53.r5 AC-4 (21)

Categoria: Proteggi > Servizi di protezione

Gravità: media

Tipo di risorsa: AWS::ApiGateway::Stage

Regola AWS Config : [api-gw-associated-with-waf](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una fase API Gateway utilizza una lista di controllo degli accessi AWS WAF Web (ACL). Questo controllo ha esito negativo se un ACL AWS WAF Web non è collegato a uno stadio REST API Gateway.

AWS WAF è un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web e le API dagli attacchi. Consente di configurare un ACL, ovvero un insieme di regole che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili definite dall'utente. Assicurati che la fase API Gateway sia associata a un ACL AWS WAF Web per proteggerla da attacchi dannosi.

Correzione

Per informazioni su come utilizzare la console API Gateway per associare un ACL web AWS WAF regionale a una fase API Gateway API esistente, consulta [Using AWS WAF to protect your API nella API Gateway Developer Guide](#).

[ApiGateway.5] I dati della cache dell'API REST API Gateway devono essere crittografati quando sono inattivi

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::ApiGateway::Stage

AWS Config regola: `api-gw-cache-encrypted` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se tutti i metodi nelle fasi API REST di API Gateway con cache abilitata sono crittografati. Il controllo ha esito negativo se un metodo in una fase API REST API Gateway è configurato per la cache e la cache non è crittografata. Security Hub valuta la crittografia di un particolare metodo solo quando la memorizzazione nella cache è abilitata per quel metodo.

La crittografia dei dati inattivi riduce il rischio di accesso ai dati archiviati su disco da parte di un utente non autenticato. AWS Aggiunge un altro set di controlli di accesso per limitare la capacità degli utenti non autorizzati di accedere ai dati. Ad esempio, sono necessarie le autorizzazioni API per decrittografare i dati prima che possano essere letti.

Le cache delle API REST di API Gateway devono essere crittografate quando sono inattive per un ulteriore livello di sicurezza.

Correzione

Per configurare la memorizzazione nella cache delle API per una fase, consulta [Enable Amazon API Gateway caching](#) nella API Gateway Developer Guide. In Impostazioni cache, scegli Crittografa i dati della cache.

[ApiGateway.8] Le rotte API Gateway devono specificare un tipo di autorizzazione

Requisiti correlati: NIST.800-53.r5 AC-3, NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Protezione > Gestione sicura degli accessi

Gravità: media

Tipo di risorsa: AWS::ApiGatewayV2::Route

AWS Config regola: [api-gwv2-authorization-type-configured](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
authorizationType	Tipo di autorizzazione dei percorsi API	Enum	AWS_IAM, CUSTOM, JWT	Nessun valore predefinito

Questo controllo verifica se le route Amazon API Gateway hanno un tipo di autorizzazione. Il controllo fallisce se la route API Gateway non ha alcun tipo di autorizzazione. Facoltativamente, puoi fornire un valore di parametro personalizzato se desideri che il controllo passi solo se la route utilizza il tipo di autorizzazione specificato nel `authorizationType` parametro.

API Gateway supporta più meccanismi per controllare e gestire l'accesso all'API. Specificando un tipo di autorizzazione, puoi limitare l'accesso all'API solo agli utenti o ai processi autorizzati.

Correzione

Per impostare un tipo di autorizzazione per le API HTTP, consulta [Controllare e gestire l'accesso a un'API HTTP in API Gateway nella API Gateway Developer Guide](#). Per impostare un tipo di autorizzazione per le WebSocket API, consulta [Controllare e gestire l'accesso a un' WebSocket API in API Gateway nella API Gateway Developer Guide](#).

[ApiGateway.9] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages

Requisiti correlati: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (4) R5 CA-7, NIST. 800-53.R5 SC-7 (9), NIST. 800-53.5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::ApiGatewayV2::Stage

AWS Config regola: [api-gwv2-access-logs-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se nelle fasi di Amazon API Gateway V2 è configurata la registrazione degli accessi. Questo controllo fallisce se le impostazioni del log di accesso non sono definite.

I log di accesso all'API Gateway forniscono informazioni dettagliate su chi ha effettuato l'accesso all'API e su come il chiamante ha effettuato l'accesso all'API. Questi log sono utili per applicazioni quali audit di sicurezza e accesso e indagini forensi. Abilita questi log di accesso per analizzare i modelli di traffico e risolvere i problemi.

Per ulteriori best practices, consulta [Monitoring REST API nella API Gateway Developer Guide](#).

Correzione

Per configurare la registrazione degli accessi, consulta [Configurare la registrazione delle CloudWatch API utilizzando la console API Gateway](#) nella Guida per sviluppatori di API Gateway.

AWS AppSync controlli

Questi controlli sono correlati alle AWS AppSync risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::AppSync::GraphQLApi

Regola AWS Config : [appsync-logging-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>fieldLoggingLevel</code>	Livello di registrazione del campo	Enum	ERROR, ALL	No default value

Questo controllo verifica se un' AWS AppSync API ha attivato la registrazione a livello di campo. Il controllo fallisce se il livello di registro del resolver del campo è impostato su Nessuno. A meno che non si forniscano valori di parametri personalizzati per indicare che un tipo di registro specifico deve essere abilitato, Security Hub produce un risultato valido se il campo resolver log level è oERROR. ALL

Puoi usare il logging e i parametri per identificare e ottimizzare le query GraphQL, oltre che per risolvere i relativi problemi. L'attivazione della registrazione per AWS AppSync GraphQL consente di ottenere informazioni dettagliate sulle richieste e le risposte delle API, identificare e rispondere ai problemi e rispettare i requisiti normativi.

Correzione

Per attivare la registrazione per AWS AppSync, consulta [Setup and configuration](#) nella Developer Guide.AWS AppSync

[AppSync.4] Le API AWS AppSync GraphQL devono essere taggate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::AppSync::GraphQLApi

AWS Config regola: `tagged-appsync-graphqlapi` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un'API AWS AppSync GraphQL ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'API GraphQL non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se l'API GraphQL non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'API AWS AppSync GraphQL, consulta l'[AWS AppSync API TagResourceReference](#).

[AppSync.5] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: alta

Tipo di risorsa: AWS::AppSync::GraphQLApi

Regola AWS Config : [appsync-authorization-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

- AllowedAuthorizationTypes: AWS_LAMBDA, AWS_IAM, OPENID_CONNECT, AMAZON_COGNITO_USER_POOLS (non personalizzabile)

Questo controllo verifica se l'applicazione utilizza una chiave API per interagire con un'API AWS AppSync GraphQL. Il controllo fallisce se un'API AWS AppSync GraphQL è autenticata con una chiave API.

Una chiave API è un valore codificato nell'applicazione che viene generato dal AWS AppSync servizio quando si crea un endpoint GraphQL non autenticato. Se questa chiave API è compromessa, l'endpoint è vulnerabile agli accessi involontari. A meno che tu non supporti un'applicazione o un sito Web accessibili al pubblico, non consigliamo di utilizzare una chiave API per l'autenticazione.

Correzione

Per impostare un'opzione di autorizzazione per l'API AWS AppSync GraphQL, consulta [Autorizzazione e autenticazione nella Guida](#) per gli AWS AppSync sviluppatori.

Controlli Amazon Athena

Questi controlli sono correlati alle risorse di Athena.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[Athena.1] I gruppi di lavoro Athena devono essere crittografati quando sono inattivi

Important

Security Hub ha ritirato questo controllo nell'aprile 2024. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Gravità: media

Tipo di risorsa: AWS::Athena::WorkGroup

Regola AWS Config : [athena-workgroup-encrypted-at-rest](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo di lavoro Athena è crittografato a riposo. Il controllo fallisce se un gruppo di lavoro Athena non è crittografato a riposo.

In Athena, puoi creare gruppi di lavoro per eseguire query per team, applicazioni o carichi di lavoro diversi. Ogni gruppo di lavoro dispone di un'impostazione per abilitare la crittografia su tutte le query. Hai la possibilità di utilizzare la crittografia lato server con le chiavi gestite di Amazon Simple Storage Service (Amazon S3), la crittografia lato server AWS Key Management Service con AWS KMS() chiavi o la crittografia lato client con chiavi KMS gestite dal cliente. I dati inattivi si riferiscono a tutti i dati archiviati in uno storage persistente e non volatile per qualsiasi durata. La crittografia aiuta

a proteggere la riservatezza di tali dati, riducendo il rischio che un utente non autorizzato possa accedervi.

Correzione

Per abilitare la crittografia a riposo per i gruppi di lavoro Athena, consulta [Modificare un gruppo di lavoro](#) nella Amazon Athena User Guide. Nella sezione Configurazione dei risultati della query, seleziona Crittografia i risultati delle query.

[Athena.2] I cataloghi di dati Athena devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::Athena::DataCatalog

AWS Config regola: tagged-athena-datacatalog (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un catalogo dati Amazon Athena contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il catalogo dati non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e

fallisce se il catalogo dati non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing. Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in [Riferimenti generali di AWS](#)

Correzione

Per aggiungere tag a un catalogo di dati Athena, consulta [Tagging Athena resources nella Amazon Athena User Guide](#).

[Athena.3] I gruppi di lavoro Athena devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Athena::WorkGroup`

AWS Config regola: `tagged-athena-workgroup` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un gruppo di lavoro Amazon Athena dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gruppo di lavoro non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di lavoro non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gruppo di lavoro Athena, consulta [Aggiungere ed eliminare tag su un singolo gruppo di lavoro nella Amazon Athena User Guide](#).

AWS Backup controlli

Questi controlli sono correlati alle AWS Backup risorse.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[Backup.1] i punti di AWS Backup ripristino devono essere crittografati a riposo

Requisiti correlati: NIST.800-53.r5 CP-9 (8), NIST.800-53.r5 SI-12

Categoria: Protezione > Protezione dei dati > Crittografia di data-at-rest

Gravità: media

Tipo di risorsa: AWS::Backup::RecoveryPoint

Regola AWS Config : [backup-recovery-point-encrypted](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un punto di AWS Backup ripristino è crittografato quando è inattivo. Il controllo fallisce se il punto di ripristino non è crittografato a riposo.

Un punto di AWS Backup ripristino si riferisce a una copia o istantanea specifica dei dati creata come parte di un processo di backup. Rappresenta un momento particolare in cui è stato eseguito il backup dei dati e funge da punto di ripristino nel caso in cui i dati originali vengano persi, danneggiati o inaccessibili. La crittografia dei punti di ripristino del backup aggiunge un ulteriore livello di protezione contro l'accesso non autorizzato. La crittografia è una procedura ottimale per proteggere la riservatezza, l'integrità e la sicurezza dei dati di backup.

Correzione

Per crittografare un punto di AWS Backup ripristino, consulta [Encryption for backup AWS Backup nella AWS Backup Developer Guide](#).

[Backup.2] i punti di AWS Backup ripristino devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::Backup::RecoveryPoint

AWS Config regola: tagged-backup-recoverypoint (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un punto di AWS Backup ripristino dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il punto di ripristino non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il punto di ripristino non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un punto di ripristino AWS Backup

1. Apri la AWS Backup console all'[indirizzo https://console.aws.amazon.com/backup](https://console.aws.amazon.com/backup).
2. Nel riquadro di navigazione scegliere Backup plans (Piani di backup).
3. Seleziona un piano di backup dall'elenco.
4. Nella sezione Tag del piano di Backup, scegli Gestisci tag.
5. Immettere una chiave e un valore per il tag. Scegli Aggiungi nuovo tag per ulteriori coppie chiave-valore.
6. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

I AWS Backup vault [Backup.3] devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::Backup::BackupVault

AWS Config regola: tagged-backup-backupvault (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un AWS Backup vault ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il punto di ripristino non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il punto di ripristino non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un archivio AWS Backup

1. Apri la AWS Backup console all'indirizzo <https://console.aws.amazon.com/backup>.
2. Nel riquadro di navigazione scegliere Backup vaults (Vault di backup).
3. Seleziona un archivio di backup dall'elenco.
4. Nella sezione Backup vault tags, scegli Gestisci tag.
5. Immettere una chiave e un valore per il tag. Scegli Aggiungi nuovo tag per ulteriori coppie chiave-valore.
6. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

[Backup.4] i piani di AWS Backup report devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::Backup::ReportPlan

AWS Config regola: tagged-backup-reportplan (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un piano di AWS Backup report contiene tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il piano di report non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se al piano di report non è associata alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un piano di report AWS Backup

1. Apri la AWS Backup console all'[indirizzo https://console.aws.amazon.com/backup](https://console.aws.amazon.com/backup).
2. Nel riquadro di navigazione scegliere Backup vaults (Vault di backup).
3. Seleziona un archivio di backup dall'elenco.
4. Nella sezione Backup vault tags, scegli Gestisci tag.
5. Scegli Aggiungi nuovo tag. Immettere una chiave e un valore per il tag. Ripetere l'operazione per ulteriori coppie chiave-valore.
6. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

[Backup.5] i piani di AWS Backup backup devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::Backup::BackupPlan

AWS Config regola: tagged-backup-backupplan (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un piano di AWS Backup backup dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il piano di backup non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il piano di backup non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un piano di backup AWS Backup

1. Apri la AWS Backup console all'[indirizzo https://console.aws.amazon.com/backup](https://console.aws.amazon.com/backup).
2. Nel riquadro di navigazione scegliere Backup vaults (Vault di backup).
3. Seleziona un archivio di backup dall'elenco.
4. Nella sezione Backup vault tags, scegli Gestisci tag.
5. Scegli Aggiungi nuovo tag. Immettere una chiave e un valore per il tag. Ripetere l'operazione per ulteriori coppie chiave-valore.
6. Una volta completata l'aggiunta di tag, scegliere Save (Salva).

AWS CloudFormation controlli

Questi controlli sono correlati alle CloudFormation risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[CloudFormation.1] gli CloudFormation stack devono essere integrati con Simple Notification Service (SNS)

Important

Security Hub ha ritirato questo controllo nell'aprile 2024. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: NIST.800-53.r5 SI-4 (12), NIST.800-53.r5 SI-4 (5)

Categoria: Rileva > Servizi di rilevamento > Monitoraggio delle applicazioni

Gravità: bassa

Tipo di risorsa: AWS::CloudFormation::Stack

Regola AWS Config : [cloudformation-stack-notification-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una notifica di Amazon Simple Notification Service è integrata con uno AWS CloudFormation stack. Il controllo fallisce per uno CloudFormation stack se non è associata alcuna notifica SNS.

La configurazione di una notifica SNS con lo CloudFormation stack consente di notificare immediatamente alle parti interessate eventuali eventi o modifiche che si verificano nello stack.

Correzione

Per integrare uno CloudFormation stack e un argomento SNS, consulta [Aggiornamento](#) degli stack direttamente nella Guida per l'utente.AWS CloudFormation

[CloudFormation.2] CloudFormation gli stack devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::CloudFormation::Stack

AWS Config regola: tagged-cloudformation-stack (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se uno AWS CloudFormation stack contiene tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se lo stack non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se lo stack non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a uno CloudFormation stack, consulta l'AWS CloudFormation API [CreateStackReference](#).

CloudFront Controlli Amazon

Questi controlli sono correlati alle CloudFront risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato

Requisiti correlati: NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16)

Categoria: Protezione > Gestione sicura degli accessi > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: AWS::CloudFront::Distribution

Regola AWS Config : [cloudfront-default-root-object-configured](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una CloudFront distribuzione Amazon è configurata per restituire un oggetto specifico che è l'oggetto root predefinito. Il controllo fallisce se nella CloudFront distribuzione non è configurato un oggetto root predefinito.

A volte un utente può richiedere l'URL principale della distribuzione anziché un oggetto nella distribuzione. In tal caso, la specifica di un oggetto root predefinito può contribuire a evitare l'esposizione dei contenuti della distribuzione Web.

Correzione

Per configurare un oggetto radice predefinito per una CloudFront distribuzione, consulta [Come specificare un oggetto radice predefinito](#) nella Amazon CloudFront Developer Guide.

[CloudFront.3] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito

Requisiti correlati: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: AWS::CloudFront::Distribution

Regola AWS Config : [cloudfront-viewer-policy-https](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una CloudFront distribuzione Amazon richiede agli spettatori di utilizzare direttamente HTTPS o se utilizza il reindirizzamento. Il controllo fallisce se `ViewerProtocolPolicy` è impostato su `allow-all` for `defaultCacheBehavior` o `for.cacheBehaviors`

HTTPS (TLS) può essere utilizzato per impedire a potenziali aggressori di utilizzare person-in-the-middle o attacchi simili per intercettare o manipolare il traffico di rete. Devono essere consentite solo le connessioni crittografate tramite HTTPS (TLS). La crittografia dei dati in transito può influire sulle prestazioni. È consigliabile testare l'applicazione con questa funzionalità per comprendere il profilo delle prestazioni e l'impatto del TLS.

Correzione

Per crittografare una CloudFront distribuzione in transito, consulta la sezione [Richiedere HTTPS per la comunicazione tra gli spettatori e CloudFront](#) nella Amazon CloudFront Developer Guide.

[CloudFront.4] le CloudFront distribuzioni devono avere configurato il failover di origine

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: bassa

Tipo di risorsa: AWS::CloudFront::Distribution

Regola AWS Config : [cloudfront-origin-failover-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una CloudFront distribuzione Amazon è configurata con un gruppo di origine che ha due o più origini.

CloudFront il failover di origine può aumentare la disponibilità. Il failover di origine reindirizza automaticamente il traffico verso un'origine secondaria se l'origine principale non è disponibile o se restituisce codici di stato di risposta HTTP specifici.

Correzione

Per configurare il failover di origine per una CloudFront distribuzione, consulta [Creating an origin group](#) nella Amazon CloudFront Developer Guide.

[CloudFront.5] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIS.800-53.R 5 SI-4 (20), NID 800-53.R 5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::CloudFront::Distribution

Regola AWS Config : [cloudfront-accesslogs-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la registrazione degli accessi al server è abilitata sulle CloudFront distribuzioni. Il controllo ha esito negativo se la registrazione dei log di accesso non è abilitata per una distribuzione.

CloudFront i registri di accesso forniscono informazioni dettagliate su ogni richiesta utente ricevuta. CloudFront Ogni log contiene informazioni come la data e l'ora di ricezione della richiesta, l'indirizzo IP del visualizzatore che ha effettuato la richiesta, l'origine della richiesta e il numero di porta della richiesta del visualizzatore.

Questi log sono utili per applicazioni quali audit di sicurezza e accesso e indagini forensi. Per ulteriori indicazioni su come analizzare i log di accesso, consulta la sezione [Interrogazione dei CloudFront log di Amazon](#) nella Amazon Athena User Guide.

Correzione

Per configurare la registrazione degli accessi per una CloudFront distribuzione, consulta [Configurazione e utilizzo dei log standard \(log di accesso\) nella Amazon Developer Guide](#).

CloudFront

[CloudFront.6] CloudFront le distribuzioni devono avere WAF abilitato

Requisiti correlati: NIST.800-53.R5 AC-4 (21)

Categoria: Proteggi > Servizi di protezione

Gravità: media

Tipo di risorsa: AWS::CloudFront::Distribution

Regola AWS Config : [cloudfront-associated-with-waf](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se CloudFront le distribuzioni sono associate agli ACL AWS WAF classici o AWS WAF Web. Il controllo ha esito negativo se la distribuzione non è associata a un ACL web.

AWS WAF è un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web e le API dagli attacchi. Consente di configurare un set di regole denominato lista di controllo degli accessi Web (ACL web) per consentire, bloccare o contare le richieste Web in base a condizioni e regole di sicurezza Web personalizzabili definite dall'utente. Assicurati che la tua CloudFront distribuzione sia associata a un ACL AWS WAF web per proteggerla da attacchi dannosi.

Correzione

Per associare un ACL AWS WAF Web a una CloudFront distribuzione, consulta [Using AWS WAF to control access to your content](#) nella Amazon CloudFront Developer Guide.

[CloudFront.7] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati

Requisiti correlati: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia di data-in-transit

Gravità: media

Tipo di risorsa: AWS::CloudFront::Distribution

Regola AWS Config : [cloudfront-custom-ssl-certificate](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se CloudFront le distribuzioni utilizzano i certificati SSL/TLS predefiniti forniti dal certificato SSL/TLS. CloudFront Questo controllo passa se la CloudFront distribuzione utilizza un certificato SSL/TLS personalizzato. Questo controllo ha esito negativo se la CloudFront distribuzione utilizza il certificato SSL/TLS predefinito.

Il protocollo SSL/TLS personalizzato consente agli utenti di accedere ai contenuti utilizzando nomi di dominio alternativi. Puoi archiviare certificati personalizzati in AWS Certificate Manager (consigliato) o in IAM.

Correzione

Per aggiungere un nome di dominio alternativo per una CloudFront distribuzione utilizzando un certificato SSL/TLS personalizzato, consulta [Aggiungere un nome di dominio alternativo nella Amazon Developer Guide](#). CloudFront

[CloudFront.8] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Configurazione di rete protetta

Gravità: bassa

Tipo di risorsa: AWS::CloudFront::Distribution

Regola AWS Config : [cloudfront-sni-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se CloudFront le distribuzioni Amazon utilizzano un certificato SSL/TLS personalizzato e sono configurate per utilizzare SNI per soddisfare le richieste HTTPS. Questo controllo fallisce se è associato un certificato SSL/TLS personalizzato ma il metodo di supporto SSL/TLS è un indirizzo IP dedicato.

Server Name Indication (SNI) è un'estensione del protocollo TLS supportato da browser e client rilasciati dopo il 2010. Se configuri CloudFront per servire le richieste HTTPS utilizzando SNI, CloudFront associa il nome di dominio alternativo a un indirizzo IP per ogni edge location. Quando un visualizzatore invia una richiesta HTTPS per i tuoi contenuti, il DNS instrada la richiesta all'indirizzo IP per la edge location corretta. L'indirizzo IP per il nome di dominio è determinato durante la negoziazione handshake SSL/TLS (l'indirizzo IP non è dedicato alla tua distribuzione).

Correzione

Per configurare una CloudFront distribuzione per utilizzare SNI per soddisfare le richieste HTTPS, consulta [Using SNI to Serve HTTPS Requests \(funziona per la maggior parte dei client\)](#) nella Developer Guide. CloudFront

[CloudFront.9] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate

Requisiti correlati: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia di data-in-transit

Gravità: media

Tipo di risorsa: AWS::CloudFront::Distribution

Regola AWS Config : [cloudfront-traffic-to-origin-encrypted](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se CloudFront le distribuzioni Amazon stanno crittografando il traffico verso origini personalizzate. Questo controllo non riesce per una CloudFront distribuzione la cui politica del protocollo di origine consente «solo http». Questo controllo fallisce anche se la politica del protocollo di origine della distribuzione è «match-viewer» mentre la politica del protocollo del visualizzatore è «allow-all».

HTTPS (TLS) può essere utilizzato per impedire l'intercettazione o la manipolazione del traffico di rete. Devono essere consentite solo le connessioni crittografate tramite HTTPS (TLS).

Correzione

Per aggiornare la politica del protocollo di origine per richiedere la crittografia per una CloudFront connessione, consulta [Richiedere HTTPS per la comunicazione tra CloudFront e la tua origine personalizzata](#) nella Amazon CloudFront Developer Guide.

[CloudFront.10] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate

Requisiti correlati: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-7 (4), nIST IST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia di data-in-transit

Gravità: media

Tipo di risorsa: AWS::CloudFront::Distribution

Regola AWS Config : [cloudfront-no-deprecated-ssl-protocols](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se CloudFront le distribuzioni Amazon utilizzano protocolli SSL obsoleti per la comunicazione HTTPS tra le CloudFront edge location e le tue origini personalizzate. Questo controllo fallisce se una CloudFront distribuzione include un `where include. CustomOriginConfig OriginSslProtocols SSLv3`

Nel 2015, l'Internet Engineering Task Force (IETF) ha annunciato ufficialmente che SSL 3.0 dovrebbe essere obsoleto a causa della scarsa sicurezza del protocollo. Si consiglia di utilizzare TLSv1.2 o versioni successive per la comunicazione HTTPS con le origini personalizzate.

Correzione

Per aggiornare i protocolli SSL di origine per una CloudFront distribuzione, consulta [Richiedere HTTPS per la comunicazione tra CloudFront e la tua origine personalizzata](#) nella Amazon CloudFront Developer Guide.

[CloudFront.12] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti

Requisiti correlati: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificazione > Configurazione delle risorse

Gravità: alta

Tipo di risorsa: AWS::CloudFront::Distribution

Regola AWS Config : [cloudfront-s3-origin-non-existent-bucket](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se CloudFront le distribuzioni Amazon puntano a origini Amazon S3 inesistenti. Il controllo fallisce per una CloudFront distribuzione se l'origine è configurata in modo da puntare a un bucket inesistente. Questo controllo si applica solo alle CloudFront distribuzioni in cui un bucket S3 senza hosting di siti Web statici è l'origine di S3.

Quando una CloudFront distribuzione nel tuo account è configurata in modo che punti a un bucket inesistente, una terza parte malintenzionata può creare il bucket di riferimento e pubblicare i propri contenuti tramite la tua distribuzione. Ti consigliamo di controllare tutte le origini indipendentemente dal comportamento di routing per assicurarti che le distribuzioni puntino alle origini appropriate.

Correzione

Per modificare una CloudFront distribuzione in modo che punti a una nuova origine, consulta la sezione [Aggiornamento di una distribuzione](#) nell'Amazon CloudFront Developer Guide.

[CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine

Categoria: Protezione > Gestione sicura degli accessi > Configurazione della politica delle risorse

Gravità: media

Tipo di risorsa: AWS::CloudFront::Distribution

Regola AWS Config : [cloudfront-s3-origin-access-control-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una CloudFront distribuzione Amazon con un'origine Amazon S3 ha configurato il controllo dell'accesso all'origine (OAC). Il controllo fallisce se OAC non è configurato per la distribuzione. CloudFront

Quando usi un bucket S3 come origine per la tua CloudFront distribuzione, puoi abilitare OAC. Ciò consente l'accesso al contenuto del bucket solo tramite la CloudFront distribuzione specificata e proibisce l'accesso diretto dal bucket o da un'altra distribuzione. Sebbene CloudFront supporti Origin Access Identity (OAI), OAC offre funzionalità aggiuntive e le distribuzioni che utilizzano OAI possono migrare verso OAC. Sebbene OAI fornisca un modo sicuro per accedere alle origini di S3, presenta delle limitazioni, come la mancanza di supporto per le configurazioni granulari delle policy e per le richieste HTTP/HTTPS che utilizzano il metodo POST in quanto richiedono la versione

4 della firma (SigV4). Regioni AWS AWS OAI inoltre non supporta la crittografia con. AWS Key Management Service OAC si basa su una AWS best practice di utilizzo dei principali di servizio IAM per l'autenticazione con le origini S3.

Correzione

Per configurare OAC per una CloudFront distribuzione con origini S3, consulta [Restricting access to an Amazon S3 origin nella Amazon Developer Guide](#). CloudFront

[CloudFront.14] le distribuzioni devono essere etichettate CloudFront

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::CloudFront::Distribution

AWS Config regola: tagged-cloudfront-distribution (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se una CloudFront distribuzione Amazon ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se la distribuzione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la distribuzione non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una CloudFront distribuzione, consulta [Tagging Amazon CloudFront distribution](#) nella Amazon CloudFront Developer Guide.

AWS CloudTrail controlli

Questi controlli sono correlati alle CloudTrail risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura

Requisiti correlati: benchmark CIS AWS Foundations v1.2.0/2.1, benchmark CIS Foundations v1.4.0/3.1, benchmark CIS AWS Foundations v3.0.0/3.1, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 3.r5 AU-12, NIT.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4),

NIST.800-53.R5 AU-14 (1), NIST.800-53.R5 CA-7, NIST.800-53.R5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-7 (8), NIST.800-53.r5 SA-8 (22) AWS

Categoria: Identificazione > Registrazione

Gravità: alta

Tipo di risorsa: AWS:::Account

Regola AWS Config : [multi-region-cloudtrail-enabled](#)

Tipo di pianificazione: periodica

Parametri:

- `readWriteType`: ALL (non personalizzabile)
- `includeManagementEvents`: true (non personalizzabile)

Questo controllo verifica se esiste almeno un AWS CloudTrail percorso multiregionale che acquisisce gli eventi di gestione di lettura e scrittura. Il controllo fallisce se CloudTrail è disabilitato o se non esiste almeno una CloudTrail traccia che acquisisca gli eventi di gestione di lettura e scrittura.

AWS CloudTrail registra le chiamate AWS API per il tuo account e ti invia i file di registro. Le informazioni registrate includono le seguenti informazioni:

- Identità del chiamante API
- Ora della chiamata API
- Indirizzo IP di origine del chiamante API
- Parametri della richiesta
- Elementi di risposta restituiti da Servizio AWS

CloudTrail fornisce una cronologia delle chiamate AWS API per un account, incluse le chiamate API effettuate dagli AWS Management Console strumenti a riga di comando AWS SDK. La cronologia include anche le chiamate API di livello superiore Servizi AWS come. AWS CloudFormation

La cronologia delle chiamate AWS API prodotta da CloudTrail consente l'analisi della sicurezza, il monitoraggio delle modifiche alle risorse e il controllo della conformità. I trail basati su più regioni offrono anche i seguenti vantaggi.

- Un trail basato su più regioni aiuta a rilevare le attività impreviste che si verificano in regioni altrimenti inutilizzate.
- Un trail basato su più regioni garantisce che la registrazione dei servizi globali sia abilitata per un trail per impostazione predefinita. La registrazione degli eventi di servizio globale registra gli eventi generati dai servizi AWS globali.
- Per un percorso multiregionale, gli eventi di gestione per tutte le operazioni di lettura e scrittura assicurano che le operazioni di gestione dei CloudTrail record su tutte le risorse in un unico file. Account AWS

Per impostazione predefinita, i CloudTrail percorsi creati utilizzando i percorsi AWS Management Console sono multiregionali.

Correzione

Per creare un nuovo percorso multiregionale in CloudTrail, vedi [Creazione di un percorso nella Guida](#) per l'AWS CloudTrail utente. Utilizzare i seguenti valori:

Campo	Valore
Impostazioni aggiuntive, Convalida del file di registro	Abilitato
Scegli gli eventi di registro, gli eventi di gestione, l'attività delle API	Leggi e scrivi. Deseleziona le caselle di controllo per le esclusioni.

Per aggiornare un percorso esistente, vedi [Aggiornamento di un percorso](#) nella Guida per l'AWS CloudTrail utente. In Management events, per l'attività dell'API, scegli Leggi e scrivi.

[CloudTrail.2] CloudTrail dovrebbe avere la crittografia a riposo abilitata

Requisiti correlati: PCI DSS versione 3.2.1/3.4, benchmark CIS Foundations versione 1.2.0/2.7, benchmark CIS AWS Foundations versione 1.4.0/3.7, benchmark CIS AWS Foundations versione 3.0.0/3.5, NIST.800-53.r5 AU-9, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 AWS CM-3 (6), NIST.800-53.r5 SC-13, NIS.800-53.r5 SC-28, NIT.800-53.r5 SC-28 (1), NIT.800-53.r5 SC-7 (10), NIT.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::CloudTrail::Trail

Regola AWS Config : [cloud-trail-encryption-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se CloudTrail è configurato per utilizzare la crittografia lato server (SSE). AWS KMS key Il controllo fallisce se non KmsKeyId è definito.

Per un ulteriore livello di sicurezza per i file di CloudTrail registro sensibili, è consigliabile utilizzare la [crittografia lato server con AWS KMS keys \(SSE-KMS\)](#) per i file di CloudTrail registro per la crittografia a riposo. Tieni presente che, per impostazione predefinita, i file di log forniti dai CloudTrail tuoi bucket sono crittografati mediante crittografia [lato server di Amazon con chiavi di crittografia gestite da Amazon S3 \(SSE-S3\)](#).

Correzione

Per abilitare la crittografia SSE-KMS per i file di CloudTrail registro, consulta [Aggiornare un percorso per utilizzare una](#) chiave KMS nella Guida per l'utente.AWS CloudTrail

[CloudTrail.3] Almeno un trail deve essere abilitato CloudTrail

Requisiti correlati: PCI DSS versione 3.2.1/10.1, PCI DSS versione 3.2.1/10.2.1, PCI DSS versione 3.2.1/10.2.2, PCI DSS versione 3.2.1/10.2.3, PCI DSS versione 3.2.1/10.2.4, PCI DSS versione 3.2.1/10.2.5, PCI DSS versione 3.2.1/10.2.6, PCI DSS versione 3.2.1/10.2.7, PCI DSS versione 3.2.1/10.2.7 versione 3.2.1/10.3.1, PCI DSS versione 3.2.1/10.3.2, PCI DSS versione 3.2.1/10.3.3, PCI DSS versione 3.2.1/10.3.4, PCI DSS versione 3.2.1/10.3.5, PCI DSS versione 3.2.1/10.3.6

Categoria: Identificazione > Registrazione

Gravità: alta

Tipo di risorsa: AWS:::Account

Regola AWS Config : [cloudtrail-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un AWS CloudTrail percorso è abilitato nel tuo Account AWS. Il controllo fallisce se il tuo account non ha almeno un CloudTrail trail abilitato.

Tuttavia, alcuni AWS servizi non consentono la registrazione di tutte le API e gli eventi. È necessario implementare eventuali percorsi di controllo aggiuntivi diversi da quelli indicati nella sezione [Servizi CloudTrail e integrazioni CloudTrail supportati](#) e consultare la documentazione relativa a ciascun servizio.

Correzione

Per iniziare CloudTrail e creare un percorso, consulta il [AWS CloudTrail tutorial Guida introduttiva](#) nella Guida per l'AWS CloudTrail utente.

[CloudTrail.4] la convalida dei file di CloudTrail registro dovrebbe essere abilitata

Requisiti correlati: PCI DSS versione 3.2.1/10.5.2, PCI DSS versione 3.2.1/10.5.5, benchmark CIS Foundations versione 1.2.0/2.2, benchmark CIS Foundations v1.4.0/3.2, benchmark CIS AWS Foundations v3.0.0/3.2, NIST.800-53.r5 AU-9, NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-7 (), NIT AWS 800-53.r5 SI-7 (3), NIT 800-53.r5 SI-7 (7) AWS

Categoria: Protezione dei dati > Integrità dei dati

Gravità: bassa

Tipo di risorsa: AWS::CloudTrail::Trail

Regola AWS Config : [cloud-trail-log-file-validation-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la convalida dell'integrità dei file di registro è abilitata su una CloudTrail traccia.

CloudTrail la convalida dei file di registro crea un file digest con firma digitale che contiene un hash di ogni log che scrive CloudTrail su Amazon S3. Puoi utilizzare questi file digest per determinare se un file di registro è stato modificato, eliminato o è rimasto invariato dopo la consegna del log. CloudTrail

Security Hub consiglia di abilitare la convalida dei file su tutti i percorsi. La convalida dei file di registro fornisce ulteriori controlli di integrità dei CloudTrail registri.

Correzione

Per abilitare la convalida dei file di CloudTrail registro, vedere [Attivazione della convalida dell'integrità dei file di registro CloudTrail nella Guida per l'utente.AWS CloudTrail](#)

[CloudTrail.5] i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch

Requisiti correlati: PCI DSS versione 3.2.1/10.5.3, benchmark CIS Foundations versione 1.2.0/2.4, benchmark CIS AWS Foundations versione 1.4.0/3.4, NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 -53R5 AU-12, NIT.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (1), NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-6 (5), NIST.800-53.R5 AU-7 (1), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-20, NIST.800-53.R5 SI-3 (8), NIST.800-53.r5 SI-4 (20), NIST.800-53.r5 SI-4 (AWS 5), NIST.800-53R5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: bassa

Tipo di risorsa: AWS::CloudTrail::Trail

Regola AWS Config : [cloud-trail-cloud-watch-logs-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se i CloudTrail trail sono configurati per inviare log a CloudWatch Logs. Il controllo fallisce se la `CloudWatchLogsLogGroupArn` proprietà del percorso è vuota.

CloudTrail registra le chiamate AWS API effettuate in un determinato account. Le informazioni registrate includono quanto segue:

- L'identità del chiamante dell'API
- L'ora della chiamata API
- L'indirizzo IP di origine del chiamante API

- I parametri della richiesta
- Gli elementi di risposta restituiti da Servizio AWS

CloudTrail utilizza Amazon S3 per l'archiviazione e la distribuzione dei file di registro. Puoi acquisire CloudTrail i log in un bucket S3 specificato per analisi a lungo termine. Per eseguire analisi in tempo reale, puoi configurare l'invio dei log CloudTrail a Logs. CloudWatch

Per un percorso abilitato in tutte le regioni di un account, CloudTrail invia i file di registro da tutte le regioni a un gruppo di log dei CloudWatch registri.

Security Hub consiglia di inviare i log a CloudTrail CloudWatch Logs. Tieni presente che questa raccomandazione ha lo scopo di garantire che l'attività dell'account venga rilevata, monitorata e attivata in modo appropriato. Puoi usare CloudWatch Logs per configurarlo con il tuo. Servizi AWS Questa raccomandazione non preclude l'uso di una soluzione diversa.

L'invio di CloudTrail log a CloudWatch Logs facilita la registrazione storica e in tempo reale delle attività in base a utente, API, risorsa e indirizzo IP. È possibile utilizzare questo approccio per stabilire allarmi e notifiche per attività anomale o riservate dell'account.

Correzione

Per l'integrazione CloudTrail con CloudWatch i registri, consulta [Invio di eventi ai CloudWatch registri nella Guida per l'utente.AWS CloudTrail](#)

[CloudTrail.6] Assicurati che il bucket S3 utilizzato per archiviare i log non sia accessibile al pubblico CloudTrail

Requisiti correlati: CIS Foundations Benchmark v1.2.0/2.3, CIS AWS Foundations Benchmark v1.4.0/3.3 AWS

Categoria: Identificazione > Registrazione

Severità: critica

Tipo di risorsa: AWS::S3::Bucket

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica e con attivazione di modifiche

Parametri: nessuno

CloudTrail registra un record di ogni chiamata API effettuata nel tuo account. Questi file di log sono archiviati in un bucket S3. Il CIS consiglia di applicare la policy del bucket S3, o lista di controllo degli accessi (ACL), al bucket S3 che CloudTrail registra per impedire l'accesso pubblico ai log. CloudTrail consentire l'accesso pubblico ai contenuti dei CloudTrail log potrebbe aiutare un avversario a identificare i punti deboli nell'uso o nella configurazione dell'account interessato.

Per eseguire questo controllo, Security Hub utilizza innanzitutto una logica personalizzata per cercare il bucket S3 in cui sono CloudTrail archiviati i log. Utilizza quindi le regole AWS Config gestite per verificare che il bucket sia accessibile pubblicamente.

Se aggregate i log in un unico bucket S3 centralizzato, Security Hub esegue il controllo solo rispetto all'account e alla regione in cui si trova il bucket S3 centralizzato. Per altri account e regioni, lo stato del controllo è Nessun dato.

Se il bucket è accessibile pubblicamente, il controllo genera un risultato non riuscito.

Correzione

Per bloccare l'accesso pubblico al tuo bucket CloudTrail S3, consulta [Configurazione delle impostazioni di blocco dell'accesso pubblico per i tuoi bucket S3 nella Guida per l'utente di Amazon Simple Storage Service](#). Seleziona tutte e quattro le impostazioni di accesso pubblico a blocchi di Amazon S3.

[CloudTrail.7] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail

Requisiti correlati: CIS Foundations Benchmark v1.2.0/2.6, CIS AWS Foundations Benchmark v1.4.0/3.6, CIS Foundations Benchmark v3.0.0/3.4 AWS AWS

Categoria: Identificazione > Registrazione

Gravità: bassa

Tipo di risorsa: AWS::S3::Bucket

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

La registrazione degli accessi al bucket S3 genera un registro che contiene i record di accesso per ogni richiesta effettuata al bucket S3. Un record dei log di accesso contiene dettagli sulla richiesta, ad esempio il tipo di richiesta, le risorse specificate nella richiesta e l'ora e la data di elaborazione della richiesta.

Il CIS consiglia di abilitare la registrazione degli accessi ai bucket sul bucket S3. CloudTrail

L'abilitazione della registrazione di bucket S3 su bucket S3 di destinazione consente di acquisire tutti gli eventi che potrebbero influenzare gli oggetti in un bucket di destinazione. La configurazione dei log da inserire in un bucket separato consente l'accesso alle informazioni di log, che possono essere utili nei flussi di lavoro di risposta a sicurezza ed errori.

Per eseguire questo controllo, Security Hub utilizza innanzitutto una logica personalizzata per cercare il bucket in cui sono archiviati CloudTrail i log e quindi utilizza la regola AWS Config gestita per verificare se la registrazione è abilitata.

Se CloudTrail invia file di log da più bucket Amazon S3 di destinazione Account AWS in un unico bucket Amazon S3, Security Hub valuta questo controllo solo rispetto al bucket di destinazione nella regione in cui si trova. Questo semplifica le tue scoperte. Tuttavia, dovresti attivare CloudTrail tutti gli account che inviano i log al bucket di destinazione. Per tutti gli account tranne quello che contiene il bucket di destinazione, lo stato del controllo è Nessun dato.

Se il bucket è accessibile pubblicamente, il controllo genera un risultato non riuscito.

Correzione

Per abilitare la registrazione dell'accesso al server per il tuo bucket CloudTrail S3, consulta [Enabling Amazon S3 server access logging nella Amazon Simple Storage Service User Guide](#).

[CloudTrail.9] i percorsi devono essere etichettati CloudTrail

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::CloudTrail::Trail

AWS Config regola: tagged-cloudtrail-trail (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un AWS CloudTrail percorso contiene tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il percorso non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il percorso non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un CloudTrail percorso, consulta la sezione AWS CloudTrail API [AddTagsReference](#).

CloudWatch Controlli Amazon

Questi controlli sono correlati alle CloudWatch risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[CloudWatch.1] Dovrebbero esistere un filtro logmetrico e un allarme per l'utilizzo da parte dell'utente «root»

Requisiti correlati: PCI DSS v3.2.1/7.2.1, CIS Foundations Benchmark v1.2.0/1.1, CIS Foundations Benchmark v1.2.0/3.3, CIS AWS Foundations Benchmark v1.4.0/1.7, CIS Foundations Benchmark v1.4.0/4.3 AWS AWS AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

AWS::Logs::MetricFilter**AWS::CloudWatch::Alarm**Tipo **AWS::CloudTrail::Trail** di risorsa:,,, **AWS::SNS::Topic**

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

L'utente root ha accesso illimitato a tutti i servizi e le risorse in un file. Account AWS Si consiglia vivamente di evitare di utilizzare l'utente root per le attività quotidiane. La riduzione al minimo dell'uso dell'utente root e l'adozione del principio del privilegio minimo per la gestione degli accessi riducono il rischio di modifiche accidentali e di divulgazione involontaria di credenziali altamente privilegiate.

È consigliabile utilizzare le credenziali dell'utente root solo quando necessario per eseguire attività di gestione degli account e dei servizi. Applica le policy AWS Identity and Access Management (IAM) direttamente ai gruppi e ai ruoli ma non agli utenti. Per un tutorial su come configurare un amministratore per l'uso quotidiano, consulta [Creazione del primo utente e gruppo di amministratori IAM](#) nella Guida per l'utente IAM

Per eseguire questo controllo, Security Hub utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 1.7 nel [CIS AWS Foundations Benchmark v1.4.0](#). Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà FAILED risultati nei seguenti casi:

- Nessun percorso è configurato.
- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà del conto corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono

generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

ListSubscriptionsByTopic Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<code>{\$.userIdentity.type="Root" && \$.userIdentity.invokedBy NOT EXISTS && \$.eventType != "AwsServiceEvent"}</code>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è...	Maggiore/Uguale
rispetto a...	1

[CloudWatch.2] Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate

Requisiti correlati: CIS AWS Foundations Benchmark v1.2.0/3.1

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:,,, AWS::Logs::MetricFilter AWS::CloudWatch::Alarm
AWS::CloudTrail::Trail AWS::SNS::Topic

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e di avvisare le chiamate API non autorizzate. Il monitoraggio delle chiamate API non autorizzate consente di rilevare errori dell'applicazione e ridurre il tempo necessario per individuare attività malevola.

Per eseguire questo controllo, Security Hub utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 3.1 nel [CIS AWS Foundations Benchmark v1.2](#).

Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà FAILED risultati nei seguenti casi:

- Nessun percorso è configurato.
- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà del conto corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

`ListSubscriptionsByTopic` Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<code>{{\$.errorCode="*UnauthorizedOperation" (\$.errorCode="AccessDenied*")}}</code>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è...	Maggiore/Uguale
rispetto a...	1

[CloudWatch.3] Assicurarsi che esistano un filtro metrico di registro e un allarme per l'accesso alla Console di gestione senza MFA

Requisiti correlati: CIS Foundations Benchmark v1.2.0/3.2 AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa:,,, AWS::Logs::MetricFilter AWS::CloudWatch::Alarm
AWS::CloudTrail::Trail AWS::SNS::Topic

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e accessi alla console di allarme non protetti da MFA. Il monitoraggio per accessi alla console a singolo fattore incrementa la visibilità negli account che non sono protetti da MFA.

Per eseguire questo controllo, Security Hub utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 3.2 nel [CIS AWS Foundations Benchmark v1.2](#). Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà luogo a FAILED risultati nei seguenti casi:

- Nessun percorso è configurato.
- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà del conto corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

ListSubscriptionsByTopic Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<pre>{ (\$.eventName = "ConsoleLogin") && (\$.additionalEventData.MFAUsed != "Yes") && (\$.userIdentity.type = "IAMUser") && (\$.responseElements.ConsoleLogin = "Success") }</pre>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è...	Maggiore/Uguale
rispetto a...	1

[CloudWatch.4] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM

Requisiti correlati: CIS Foundations Benchmark v1.2.0/3.4, CIS AWS Foundations Benchmark v1.4.0/4.4 AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo AWS::Logs::MetricFilter AWS::CloudWatch::Alarm di AWS::CloudTrail::Trail
risorsa:,, AWS::SNS::Topic

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se monitorate le chiamate API in tempo reale indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche apportate alle politiche IAM. Il monitoraggio di queste modifiche garantisce che i controlli di autenticazione e autorizzazione rimangano invariati.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà luogo a FAILED risultati nei seguenti casi:

- Nessun percorso è configurato.
- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà del conto corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione

predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

ListSubscriptionsByTopic Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Note

Lo schema di filtro consigliato in queste fasi di riparazione è diverso dal modello di filtro indicato nelle linee guida CIS. I nostri filtri consigliati hanno come target solo gli eventi provenienti dalle chiamate API IAM.

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<pre>{(\$.eventSource=iam.amazonaws.com) && ((\$.eventName>DeleteGroupPolicy) (\$.eventName>DeleteRolePolicy) (\$.eventName>DeleteUserPolicy) (\$.eventName=PutGroupPolicy) (\$.eventName=PutRolePolicy) (\$.eventName=PutUserPolicy) (\$.eventName>CreatePolicy) (\$.eventName>DeletePolicy) (\$.eventName>CreatePolicyVersion) (\$.eventName>DeletePolicyVersion) (\$.eventName=AttachRolePolicy) (\$.eventName=DetachRolePolicy) (\$.eventName=AttachUserPolicy) (\$.eventName=DetachUserPolicy) (\$.eventName=AttachGroupPolicy) (\$.eventName=DetachGroupPolicy))}</pre>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è... rispetto a...	Maggiore/Uguale 1

[CloudWatch.5] Assicurati che esistano un filtro metrico di registro e un allarme per le CloudTrail AWS Config variazioni di durata

Requisiti correlati: CIS Foundations Benchmark v1.2.0/3.5, CIS AWS Foundations Benchmark v1.4.0/4.5 AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo `AWS::Logs::MetricFilter` `AWS::CloudWatch::Alarm` di `AWS::CloudTrail::Trail`
risorsa:,,, `AWS::SNS::Topic`

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche alle impostazioni di configurazione. CloudTrail Il monitoraggio di queste modifiche garantisce visibilità sostenuta per attività dell'account.

Per eseguire questo controllo, Security Hub utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 4.5 nel [CIS AWS Foundations Benchmark v1.4.0](#). Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà luogo a FAILED risultati nei seguenti casi:

- Nessun percorso è configurato.
- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

`ListSubscriptionsByTopic` Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	{(\$.eventName=CreateTrail) (\$.eventName=UpdateTrail) (\$.eventName>DeleteTrail) (\$.eventName=StartLogging) (\$.eventName=StopLogging)}
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico

Campo	Valore
Ogni volta che <i>your-metric-name</i> è...	Maggiore/Uguale
rispetto a...	1

[CloudWatch.6] Assicurati che esistano un filtro metrico di registro e un allarme per gli AWS Management Console errori di autenticazione

Requisiti correlati: CIS Foundations Benchmark v1.2.0/3.6, CIS AWS Foundations Benchmark v1.4.0/4.6 AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo AWS::Logs::MetricFilter AWS::CloudWatch::Alarm di AWS::CloudTrail::Trail
risorsa:,,, AWS::SNS::Topic

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per i tentativi di autenticazione della console non riusciti. Il monitoraggio degli accessi alla console non riusciti potrebbe ridurre il lead time per rilevare un tentativo di attacco di forza bruta a una credenziale, che potrebbe fornire un indicatore, ad esempio IP di origine, utilizzabile in altre correlazioni eventi.

Per eseguire questo controllo, Security Hub utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 4.6 nel [CIS AWS Foundations Benchmark v1.4.0](#). Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà luogo a FAILED risultati nei seguenti casi:

- Nessun percorso è configurato.
- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

`ListSubscriptionsByTopic` Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<code>{{\$.eventName=ConsoleLogin) && (\$.errorMessage="Failed authentication")}}</code>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è...	Maggiore/Uguale
rispetto a...	1

[CloudWatch.7] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione programmata delle chiavi gestite dal cliente

Requisiti correlati: CIS Foundations Benchmark v1.2.0/3.7, CIS AWS Foundations Benchmark v1.4.0/4.7 AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo AWS::Logs::MetricFilter AWS::CloudWatch::Alarm di AWS::CloudTrail::Trail
risorsa:,, AWS::SNS::Topic

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per le chiavi gestite dai clienti che hanno cambiato stato in eliminazione disattivata o pianificata. I dati crittografati con chiavi disabilite o eliminate non sono più accessibili.

Per eseguire questo controllo, Security Hub utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 4.7 nel [CIS AWS Foundations Benchmark v1.4.0](#). Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri. Il controllo fallisce anche se contiene. ExcludeManagementEventSources kms.amazonaws.com

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà luogo a FAILED risultati nei seguenti casi:

- Nessun percorso è configurato.

- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

ListSubscriptionsByTopic Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<code>{{\$.eventSource=kms.amazonaws.com) && (\$.eventName=DisableKey) (\$.eventName=ScheduleKeyDeletion)}}</code>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è...	Maggiore/Uguale
rispetto a...	1

[CloudWatch.8] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3

Requisiti correlati: CIS Foundations Benchmark v1.2.0/3.8, CIS AWS Foundations Benchmark v1.4.0/4.8 AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo AWS::Logs::MetricFilter AWS::CloudWatch::Alarm di AWS::CloudTrail::Trail
risorsa:,, AWS::SNS::Topic

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche alle politiche dei bucket S3. Il monitoraggio di queste modifiche potrebbe ridurre il tempo necessario per rilevare e correggere policy permissive su bucket S3 sensibili.

Per eseguire questo controllo, Security Hub utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 4.8 nel [CIS AWS Foundations Benchmark v1.4.0](#). Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà luogo a FAILED risultati nei seguenti casi:

- Nessun percorso è configurato.
- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.

- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

ListSubscriptionsByTopic Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<pre>{ (\$.eventSource=s3.amazonaws.com) && ((\$.eventName=PutBucketAcl) (\$.eventName=PutBucketPolicy) (\$.eventName=PutBucketCors) (\$.eventName=PutBucketLifecycle) (\$.eventName=PutBucketReplication) (\$.eventName>DeleteBucketPolicy) (\$.eventName>DeleteBucketCors) (\$.eventName>DeleteBucketLifecycle) (\$.eventName>DeleteBucketReplication)) }</pre>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è...	Maggiore/Uguale
rispetto a...	1

[CloudWatch.9] Assicurati che esistano un filtro metrico di log e un allarme per le AWS Config modifiche alla configurazione

Requisiti correlati: CIS Foundations Benchmark v1.2.0/3.9, CIS AWS Foundations Benchmark v1.4.0/4.9 AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo AWS::Logs::MetricFilter AWS::CloudWatch::Alarm di AWS::CloudTrail::Trail
risorsa:,,, AWS::SNS::Topic

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche alle impostazioni di configurazione. AWS Config Il monitoraggio di queste modifiche garantisce visibilità sostenuta per elementi di configurazione nell'account.

Per eseguire questo controllo, Security Hub utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 4.9 nel [CIS AWS Foundations Benchmark v1.4.0](#). Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà luogo a FAILED risultati nei seguenti casi:

- Nessun percorso è configurato.

- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

ListSubscriptionsByTopic Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<code>{(\$.eventSource=config.amazonaws.com) && (\$.eventName=StopConfigurationRecorder) (\$.eventName>DeleteDeliveryChannel) (\$.eventName=PutDeliveryChannel) (\$.eventName=PutConfigurationRecorder)}</code>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è...	Maggiore/Uguale
rispetto a...	1

[CloudWatch.10] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza

Requisiti correlati: CIS Foundations Benchmark v1.2.0/3.10, CIS AWS Foundations Benchmark v1.4.0/4.10 AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo AWS::Logs::MetricFilter AWS::CloudWatch::Alarm di AWS::CloudTrail::Trail
risorsa:,, AWS::SNS::Topic

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti. I gruppi di sicurezza sono un filtro dei pacchetti stateful che controlla il traffico in entrata e in uscita in un VPC.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche ai gruppi di sicurezza. Il monitoraggio di tali modifiche garantisce che le risorse e i servizi non vengano involontariamente esposti.

Per eseguire questo controllo, Security Hub utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 4.10 nel [CIS AWS Foundations Benchmark v1.4.0](#). Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà luogo a FAILED risultati nei seguenti casi:

- Nessun percorso è configurato.

- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

ListSubscriptionsByTopic Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<code>{(\$.eventName=AuthorizeSecurityGroupIngress) (\$.eventName=AuthorizeSecurityGroupEgress) (\$.eventName=RevokeSecurityGroupIngress) (\$.eventName=RevokeSecurityGroupEgress) (\$.eventName=CreateSecurityGroup) (\$.eventName>DeleteSecurityGroup)}</code>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è...	Maggiore/Uguale
rispetto a...	1

[CloudWatch.11] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete (NACL)

Requisiti correlati: CIS Foundations Benchmark v1.2.0/3.11, CIS AWS Foundations Benchmark v1.4.0/4.11 AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo AWS::Logs::MetricFilter AWS::CloudWatch::Alarm di AWS::CloudTrail::Trail
risorsa:,,, AWS::SNS::Topic

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti. NACL vengono utilizzate come filtro dei pacchetti stateless per controllare il traffico in entrata e in uscita per sottoreti in un VPC.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche ai NACL. Il monitoraggio di queste modifiche aiuta a garantire che AWS risorse e servizi non vengano esposti involontariamente.

Per eseguire questo controllo, Security Hub utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 4.11 nel [CIS AWS Foundations Benchmark v1.4.0](#). Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà luogo a FAILED risultati nei seguenti casi:

- Nessun percorso è configurato.

- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà dell'account corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

ListSubscriptionsByTopic Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso valido per tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<pre>{(\$.eventName=CreateNetworkAc1) (\$.eventName=CreateNetworkAc1Entry) (\$.eventName>DeleteNetworkAc1) (\$.eventName>DeleteNetworkAc1Entry) (\$.eventName=ReplaceNetworkAc1Entry) (\$.eventName=ReplaceNetworkAc1Association)}</pre>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è... rispetto a...	Maggiore/Uguale 1

[CloudWatch.12] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche ai gateway di rete

Requisiti correlati: CIS Foundations Benchmark v1.2.0/3.12, CIS AWS Foundations Benchmark v1.4.0/4.12 AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo AWS::Logs::MetricFilter AWS::CloudWatch::Alarm di AWS::CloudTrail::Trail
risorsa:,,, AWS::SNS::Topic

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti. I gateway di rete sono necessari per inviare e ricevere traffico a una destinazione all'esterno di un VPC.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche ai gateway di rete. Il monitoraggio di tali modifiche garantisce che tutto il traffico in entrata e in uscita attraversa il bordo del VPC tramite un percorso controllato.

Per eseguire questo controllo, Security Hub utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 4.12 nel [CIS AWS Foundations Benchmark v1.2](#). Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà FAILED risultati nei seguenti casi:

- Non è configurato alcun percorso.

- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà del conto corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

ListSubscriptionsByTopic Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso che si applichi a tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<code>{ (\$.eventName=CreateCustomerGateway) (\$.eventName>DeleteCustomerGateway) (\$.eventName=AttachInternetGateway) (\$.eventName=CreateInternetGateway) (\$.eventName>DeleteInternetGateway) (\$.eventName=DetachInternetGateway)}</code>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è...	Maggiore/Uguale
rispetto a...	1

[CloudWatch.13] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte

Requisiti correlati: CIS Foundations Benchmark v1.2.0/3.13, CIS AWS Foundations Benchmark v1.4.0/4.13 AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo AWS::Logs::MetricFilter AWS::CloudWatch::Alarm di AWS::CloudTrail::Trail
risorsa:,, AWS::SNS::Topic

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se monitorate le chiamate API in tempo reale indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti. Le tabelle di routing instradano il traffico di rete tra le sottoreti e i gateway di rete.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche alle tabelle di routing. Il monitoraggio di queste modifiche garantisce che tutto il traffico VPC passi attraverso un percorso previsto.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà FAILED risultati nei seguenti casi:

- Non è configurato alcun percorso.
- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà del conto corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

ListSubscriptionsByTopic Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Note

Lo schema di filtro consigliato in queste fasi di riparazione è diverso dal modello di filtro indicato nelle linee guida CIS. I nostri filtri consigliati hanno come target solo gli eventi provenienti dalle chiamate API Amazon Elastic Compute Cloud (EC2).

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.

2. Crea un CloudTrail percorso che si applichi a tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<code>{{\$.eventSource=ec2.amazonaws.com) && ((\$.eventName=CreateRoute) (\$.eventName=CreateRouteTable) (\$.eventName=ReplaceRoute) (\$.eventName=ReplaceRouteTableAssociation) (\$.eventName>DeleteRouteTable) (\$.eventName>DeleteRoute) (\$.eventName=DisassociateRouteTable))}}</code>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è...	Maggiore/Uguale
rispetto a...	1

[CloudWatch.14] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche al VPC

Requisiti correlati: CIS Foundations Benchmark v1.2.0/3.14, CIS AWS Foundations Benchmark v1.4.0/4.14 AWS

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo AWS::Logs::MetricFilter AWS::CloudWatch::Alarm di AWS::CloudTrail::Trail
risorsa:,,, AWS::SNS::Topic

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Puoi monitorare in tempo reale le chiamate API indirizzando i log verso CloudTrail Logs e stabilendo i filtri CloudWatch metrici e gli allarmi corrispondenti. Un account può contenere più VPC ed è possibile creare una connessione peer tra due VPC, consentendo l'instradamento del traffico di rete tra i VPC.

Il CIS consiglia di creare un filtro metrico e un allarme per le modifiche ai VPC. Il monitoraggio di queste modifiche garantisce che i controlli di autenticazione e autorizzazione rimangano invariati.

Per eseguire questo controllo, Security Hub utilizza una logica personalizzata per eseguire gli esatti passaggi di controllo prescritti per il controllo 4.14 nel [CIS AWS Foundations Benchmark v1.4.0](#). Questo controllo non riesce se non vengono utilizzati i filtri di parametri esatti prescritti da CIS. Non è possibile aggiungere campi o termini ulteriori ai filtri di parametri.

Note

Quando Security Hub esegue il controllo per questo controllo, cerca le CloudTrail tracce utilizzate dall'account corrente. Questi percorsi potrebbero essere percorsi organizzativi che appartengono a un altro account. I percorsi multiregionali potrebbero anche avere sede in una regione diversa.

Il controllo dà FAILED risultati nei seguenti casi:

- Non è configurato alcun percorso.

- I percorsi disponibili che si trovano nella regione corrente e che sono di proprietà del conto corrente non soddisfano i requisiti di controllo.

Il controllo determina uno stato di controllo pari NO_DATA a nei seguenti casi:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Consigliamo gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta uno stato di controllo pari a NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Per l'allarme, l'account corrente deve essere proprietario dell'argomento Amazon SNS di riferimento o deve accedere all'argomento Amazon SNS chiamando.

ListSubscriptionsByTopic Altrimenti Security Hub genera WARNING risultati per il controllo.

Correzione

Per passare questo controllo, segui questi passaggi per creare un argomento Amazon SNS, un AWS CloudTrail percorso, un filtro metrico e un allarme per il filtro metrico.

1. Creazione di un argomento Amazon SNS. Per istruzioni, consulta la sezione [Guida introduttiva ad Amazon SNS nella Guida per gli sviluppatori di Amazon Simple Notification Service](#). Crea un argomento che riceva tutti gli allarmi CIS e crea almeno un abbonamento all'argomento.
2. Crea un CloudTrail percorso che si applichi a tutti. Regioni AWS Per istruzioni, consulta [Creazione di un percorso](#) nella Guida AWS CloudTrail per l'utente.

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Il filtro metrico per quel gruppo di log viene creato nel passaggio successivo.

3. Creazione di un filtro parametri. Per istruzioni, consulta [Creare un filtro metrico per un gruppo di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Definisci modello, modello di filtro	<pre>{ (\$.eventName=CreateVpc) (\$.eventName>DeleteVpc) (\$.eventName=ModifyVpcAttribute) (\$.eventName=AcceptVpcPeeringConnection) (\$.eventName>CreateVpcPeeringConnection) (\$.eventName>DeleteVpcPeeringConnection) (\$.eventName=RejectVpcPeeringConnection) (\$.eventName=AttachClassicLinkVpc) (\$.eventName=DetachClassicLinkVpc) (\$.eventName=DisableVpcClassicLink) (\$.eventName=EnableVpcClassicLink)}</pre>
Namespace metrico	LogMetrics
Valore del parametro	1
Valore predefinito	0

4. Crea un allarme basato sul filtro. Per istruzioni, consulta [Creazione di un CloudWatch allarme basato su un filtro metrico per gruppi di log](#) nella Amazon CloudWatch User Guide. Utilizzare i seguenti valori:

Campo	Valore
Condizioni, tipo di soglia	Statico
Ogni volta che <i>your-metric-name</i> è... rispetto a...	Maggiore/Uguale 1

[CloudWatch.15] gli CloudWatch allarmi devono avere azioni specificate configurate

Categoria: Rilevamento > Servizi di rilevamento

Requisiti correlati: NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 CA-7, NIST.800-53.r5 IR-4 (1), NIST.800-53.r5 IR-4 (5), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-20, nIST.IST. 800-53.r5 SI-4 (12), NIT 800-53r5 SI-4 (5)

Gravità: alta

Tipo di risorsa: AWS::CloudWatch::Alarm

AWS Config regola: [cloudwatch-alarm-action-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>alarmActionRequired</code>	Il controllo rileva PASSED se il parametro è impostato su <code>true</code> e l'allarme agisce quando lo stato dell'allarme cambia a ALARM.	Booleano	Non personalizzabile	<code>true</code>
<code>insufficientDataAction</code>	Il controllo rileva PASSED se il parametro è impostato	Booleano	<code>true</code> o <code>false</code>	<code>false</code>

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
tionRequired	su <code>true</code> e l'allarme agisce quando lo stato dell'allarme cambia a <code>INSUFFICIENT_DATA</code> .			
okActionRequired	Il controllo rileva <code>PASSED</code> se il parametro è impostato su <code>true</code> e l'allarme agisce quando lo stato di allarme cambia a <code>OK</code> .	Booleano	<code>true</code> o <code>false</code>	<code>false</code>

Questo controllo verifica se un CloudWatch allarme Amazon ha almeno un'azione configurata per lo ALARM stato. Il controllo fallisce se l'allarme non ha un'azione configurata per lo ALARM stato. Facoltativamente, è possibile includere valori di parametri personalizzati per richiedere anche azioni di allarme per gli OK stati `INSUFFICIENT_DATA` or.

Note

Security Hub valuta questo controllo sulla base di allarmi CloudWatch metrici. Gli allarmi metrici possono far parte di allarmi compositi con le azioni specificate configurate. Il controllo genera `FAILED` risultati nei seguenti casi:

- Le azioni specificate non sono configurate per un allarme metrico.
- L'allarme metrico fa parte di un allarme composito in cui sono configurate le azioni specificate.

Questo controllo si concentra sul fatto che un CloudWatch allarme abbia un'azione di allarme configurata, mentre [CloudWatch.17](#) si concentra sullo stato di attivazione di un'azione di CloudWatch allarme.

Consigliamo azioni di CloudWatch allarme per avvisare automaticamente l'utente quando una metrica monitorata supera la soglia definita. Il monitoraggio degli allarmi consente di identificare attività insolite e di rispondere rapidamente ai problemi operativi e di sicurezza quando un allarme entra

in uno stato specifico. Il tipo più comune di azione di allarme consiste nell'avvisare uno o più utenti inviando un messaggio a un argomento di Amazon Simple Notification Service (Amazon SNS).

Correzione

Per informazioni sulle azioni supportate dagli CloudWatch allarmi, consulta [Azioni di allarme](#) nella Amazon CloudWatch User Guide.

[CloudWatch.16] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato

Categoria: Identificazione > Registrazione

Requisiti correlati: NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-11, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-12

Gravità: media

Tipo di risorsa: AWS::Logs::LogGroup

AWS Config regola: [cw-loggroup-retention-period-check](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personali zzati consentiti	Valore predefinito di Security Hub
minRetentionTime	Periodo minimo di conservazione in giorni per i gruppi di CloudWatch log	Enum	365, 400, 545, 731, 1827, 3653	365

Questo controllo verifica se un gruppo di CloudWatch log Amazon ha un periodo di conservazione di almeno il numero di giorni specificato. Il controllo fallisce se il periodo di conservazione è inferiore al

numero specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di conservazione, Security Hub utilizza un valore predefinito di 365 giorni.

CloudWatch I log centralizzano i log di tutti i sistemi e le applicazioni Servizi AWS in un unico servizio altamente scalabile. Puoi usare CloudWatch Logs per monitorare, archiviare e accedere ai tuoi file di log da istanze Amazon Elastic Compute Cloud (EC2) AWS CloudTrail, Amazon Route 53 e altre fonti. Conservare i log per almeno 1 anno può aiutarti a rispettare gli standard di conservazione dei log.

Correzione

Per configurare le impostazioni di conservazione dei log, consulta [Change log data retention in CloudWatch Logs](#) nella Amazon CloudWatch User Guide.

[CloudWatch.17] le azioni di CloudWatch allarme devono essere attivate

Categoria: Rilevamento > Servizi di rilevamento

Requisiti correlati: NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-4 (12)

Gravità: alta

Tipo di risorsa: AWS::CloudWatch::Alarm

AWS Config regola: [cloudwatch-alarm-action-enabled-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le azioni di CloudWatch allarme sono attivate (ActionEnabled deve essere impostato su true). Il controllo fallisce se l'azione di allarme per un CloudWatch allarme è disattivata.

Note

Security Hub valuta questo controllo sulla base di allarmi CloudWatch metrici. Gli allarmi metrici possono far parte di allarmi compositi che hanno le azioni di allarme attivate. Il controllo genera FAILED risultati nei seguenti casi:

- Le azioni specificate non sono configurate per un allarme metrico.

- L'allarme metrico fa parte di un allarme composito con azioni di allarme attivate.

Questo controllo si concentra sullo stato di attivazione di un'azione di CloudWatch allarme, mentre [CloudWatch.15](#) si concentra sulla configurazione di ALARM un'azione in un CloudWatch allarme.

Le azioni di allarme avvisano automaticamente l'utente quando una metrica monitorata supera la soglia definita. Se l'azione di allarme è disattivata, non viene eseguita alcuna azione quando l'allarme cambia stato e non sarai avvisato delle modifiche nelle metriche monitorate. Ti consigliamo di attivare le azioni di CloudWatch allarme per aiutarti a rispondere rapidamente ai problemi operativi e di sicurezza.

Correzione

Per attivare un'azione CloudWatch di allarme (console)

1. Apri la CloudWatch console all'[indirizzo https://console.aws.amazon.com/cloudwatch/](https://console.aws.amazon.com/cloudwatch/).
2. Nel pannello di navigazione, in Allarmi, scegli Tutti gli allarmi.
3. Seleziona l'allarme per il quale desideri attivare le azioni.
4. Per Azioni, scegli Azioni di allarme: nuove, quindi scegli Abilita.

Per ulteriori informazioni sull'attivazione delle azioni di CloudWatch allarme, consulta le [azioni di allarme](#) nella Amazon CloudWatch User Guide.

AWS CodeArtifact controlli

Questi controlli sono correlati alle CodeArtifact risorse.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[CodeArtifact.1] i CodeArtifact repository devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::CodeArtifact::Repository

AWS Config regola: tagged-codeartifact-repository (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un AWS CodeArtifact repository ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il repository non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il repository non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un CodeArtifact repository, consulta Etichettare [un repository CodeArtifact nella Guida per l'utente.AWS CodeArtifact](#)

AWS CodeBuild controlli

Questi controlli sono correlati alle CodeBuild risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili

Requisiti correlati: PCI DSS v3.2.1/8.2.1, NIST.800-53.r5 SA-3

Categoria: Protezione > Sviluppo protetto

Severità: critica

Tipo di risorsa: AWS::CodeBuild::Project

Regola AWS Config : [codebuild-project-source-repo-url-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'URL del repository di origine Bitbucket di un AWS CodeBuild progetto contiene token di accesso personali o un nome utente e una password. Il controllo fallisce se l'URL del repository di origine Bitbucket contiene token di accesso personali o un nome utente e una password.

Note

Questo controllo valuta sia la fonte primaria che le fonti secondarie di un progetto di compilazione. CodeBuild Per ulteriori informazioni sulle fonti del progetto, consulta l'[esempio di fonti di input e artefatti di output multipli](#) nella Guida per l'AWS CodeBuild utente.

Le credenziali di accesso non devono essere archiviate o trasmesse in testo non crittografato o apparire nell'URL del repository di origine. Invece dei token di accesso personali o delle credenziali di accesso, dovresti accedere al tuo provider di origine e modificare l'URL del repository di origine in CodeBuild modo che contenga solo il percorso della posizione del repository Bitbucket. L'utilizzo di token di accesso personali o credenziali di accesso potrebbe comportare l'esposizione involontaria dei dati o l'accesso non autorizzato.

Correzione

Puoi aggiornare il tuo CodeBuild progetto per utilizzare OAuth.

Per rimuovere l'autenticazione di base/(GitHub) Personal Access Token dal sorgente del progetto CodeBuild

1. Apri la CodeBuild console all'[indirizzo https://console.aws.amazon.com/codebuild/](https://console.aws.amazon.com/codebuild/).
2. Scegliere il progetto di compilazione contenente i token di accesso personali o un nome utente e una password.
3. Da Edit (Modifica), scegliere Source (Sorgente).
4. Scegli Disconnetti da GitHub /Bitbucket.
5. Scegli Connetti tramite OAuth, quindi scegli Connetti GitHub a/Bitbucket.
6. Quando richiesto, scegliere authorize as appropriate (autorizza come appropriato).
7. Riconfigurare l'URL repository) e le impostazioni di configurazione aggiuntive, se necessario.
8. Scegliere Update source (Aggiorna origine).

Per ulteriori informazioni, consulta gli esempi [basati su casi CodeBuild d'uso](#) nella Guida per l'utente.AWS CodeBuild

[CodeBuild.2] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato

Requisiti correlati: PCI DSS v3.2.1/8.2.1, NIST.800-53.r5 IA-5 (7), NIST.800-53.r5 SA-3

Categoria: Protezione > Sviluppo protetto

Severità: critica

Tipo di risorsa: AWS::CodeBuild::Project

Regola AWS Config : [codebuild-project-envvar-awscred-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il progetto contiene le variabili di ambiente `AWS_ACCESS_KEY_ID` e `AWS_SECRET_ACCESS_KEY`.

Le credenziali di autenticazione `AWS_ACCESS_KEY_ID` e `AWS_SECRET_ACCESS_KEY` non devono mai essere memorizzate in testo non crittografato, in quanto ciò potrebbe comportare l'esposizione non intenzionale dei dati e l'accesso non autorizzato.

Correzione

Per rimuovere le variabili di ambiente da un CodeBuild progetto, consulta [Modificare le impostazioni di un progetto di build AWS CodeBuild nella Guida per l'AWS CodeBuild utente](#). Assicurati che non sia selezionato nulla per le variabili di ambiente.

Puoi memorizzare le variabili di ambiente con valori sensibili nel AWS Systems Manager Parameter Store o AWS Secrets Manager recuperarle dalle specifiche di build. Per istruzioni, consulta la casella denominata Importante nella [sezione Ambiente della Guida](#) per l'AWS CodeBuild utente.

[CodeBuild.3] I log CodeBuild S3 devono essere crittografati

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia di data-at-rest

Gravità: bassa

Tipo di risorsa: `AWS::CodeBuild::Project`

Regola AWS Config : [codebuild-project-s3-logs-encrypted](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i log di Amazon S3 per un AWS CodeBuild progetto sono crittografati. Il controllo fallisce se la crittografia è disattivata per i log S3 di un progetto. CodeBuild

La crittografia dei dati inattivi è una best practice consigliata per aggiungere un livello di gestione degli accessi ai dati. La crittografia dei registri inattivi riduce il rischio che un utente non autenticato da acceda AWS ai dati archiviati su disco. Aggiunge un altro set di controlli di accesso per limitare la capacità degli utenti non autorizzati di accedere ai dati.

Correzione

Per modificare le impostazioni di crittografia per i log CodeBuild del progetto S3, consulta [Modificare le impostazioni di un progetto di build AWS CodeBuild nella Guida](#) per l'AWS CodeBuild utente.

[CodeBuild.4] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config

Requisiti correlati: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::CodeBuild::Project`

Regola AWS Config : [codebuild-project-logging-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un ambiente di CodeBuild progetto ha almeno un'opzione di registro, su S3 o sui CloudWatch log abilitati. Questo controllo fallisce se un ambiente di CodeBuild progetto non ha almeno un'opzione di registro abilitata.

Dal punto di vista della sicurezza, la registrazione è una funzionalità importante per consentire future attività di analisi forense in caso di incidenti di sicurezza. La correlazione delle anomalie nei CodeBuild progetti con il rilevamento delle minacce può aumentare la fiducia nell'accuratezza di tali rilevamenti di minacce.

Correzione

Per ulteriori informazioni su come configurare le impostazioni CodeBuild del registro di progetto, consulta [Creare un progetto di compilazione \(console\) nella Guida](#) per l'utente. CodeBuild

[CodeBuild.5] gli ambienti di CodeBuild progetto non dovrebbero avere la modalità privilegiata abilitata

Important

Security Hub ha ritirato questo controllo nell'aprile 2024. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6 (10), nIST.800-53.r5 AC-6 (10), nIST. 800-53,5 AC-6 (2)

Categoria: Protezione > Gestione sicura degli accessi

Gravità: alta

Tipo di risorsa: AWS::CodeBuild::Project

Regola AWS Config : [codebuild-project-environment-privileged-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'ambiente di AWS CodeBuild progetto ha la modalità privilegiata abilitata o disabilitata. Il controllo fallisce se in un ambiente di CodeBuild progetto è abilitata la modalità privilegiata.

Per impostazione predefinita, i contenitori Docker non consentono l'accesso a nessun dispositivo. La modalità privilegiata garantisce l'accesso al contenitore Docker di un progetto a tutti i dispositivi. L'impostazione `privilegedMode` con valore `true` consente al demone Docker di funzionare all'interno di un contenitore Docker. Il daemon Docker ascolta le richieste dell'API Docker e gestisce oggetti Docker come immagini, contenitori, reti e volumi. Questo parametro deve essere impostato su `true` solo se il progetto di compilazione viene utilizzato per creare immagini Docker. Altrimenti, questa impostazione dovrebbe essere disabilitata per impedire l'accesso involontario alle API Docker e all'hardware sottostante del contenitore. Impostazione `privilegedMode` che `false` consente di proteggere le risorse critiche da manomissioni ed eliminazioni.

Correzione

Per configurare le impostazioni dell'ambiente di CodeBuild progetto, consulta [Creare un progetto di compilazione \(console\) nella Guida](#) per l'CodeBuild utente. Nella sezione Ambiente, non selezionare l'impostazione Privileged.

AWS Config controlli

Questi controlli sono correlati alle AWS Config risorse.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[Config.1] AWS Config dovrebbe essere abilitato

Requisiti correlati: PCI DSS versione 3.2.1/10.5.2, PCI DSS versione 3.2.1/11.5, benchmark CIS Foundations versione 1.2.0/2.5, benchmark CIS Foundations v1.4.0/3.5, benchmark CIS AWS Foundations v3.0.0/3.3, NIST.800-53.r5 CM-3, NIST.800-53.r5 CM-6 (1), AWS NIST.800-53.r5 CM-8, NITS. 800-53,5 AWS CM-8 (2)

Categoria: Identificazione > Inventario

Gravità: media

Tipo di risorsa: AWS : : : Account

AWS Config regola: Nessuna (regola personalizzata del Security Hub)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se AWS Config è abilitato nel tuo account nella regione corrente e sta registrando tutte le risorse. Il controllo fallisce se AWS Config non è abilitato o non registra tutte le risorse.

Il AWS Config servizio esegue la gestione della configurazione delle AWS risorse supportate nel tuo account e ti fornisce i file di registro. Le informazioni registrate includono l'elemento di configurazione (AWS risorsa), le relazioni tra gli elementi di configurazione e qualsiasi modifica alla configurazione tra le risorse.

Security Hub consiglia di abilitarlo AWS Config in tutte le regioni. La cronologia degli elementi di AWS configurazione AWS Config acquisita consente l'analisi della sicurezza, il monitoraggio delle modifiche alle risorse e il controllo della conformità.

Note

Config.1 richiede che AWS Config sia abilitato in tutte le regioni in cui si utilizza Security Hub. Poiché Security Hub è un servizio regionale, il controllo eseguito per questo controllo verifica solo la regione corrente dell'account. Non controlla tutte le regioni.

Per consentire controlli di sicurezza sulle risorse globali in ogni regione, è necessario registrare anche le risorse globali. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

I tipi di risorse registrati a livello globale che AWS Config supportano sono utenti, gruppi, ruoli e politiche gestite dai clienti IAM. Puoi prendere in considerazione la possibilità di disabilitare i controlli del Security Hub che controllano questi tipi di risorse nelle regioni in cui la registrazione globale delle risorse è disattivata. Poiché IAM è un servizio globale, le risorse IAM verranno registrate solo nella regione in cui è attivata la registrazione globale delle risorse. Per ulteriori informazioni, consulta [Controlli del Security Hub che potresti voler disabilitare](#).

Correzione

Per abilitarlo AWS Config e configurarlo per registrare tutte le risorse, consulta [Configurazione manuale](#) nella Guida per gli AWS Config sviluppatori. Per registrare le risorse globali e garantire che nessun tipo di risorsa sia escluso, seleziona Tutte le risorse con sostituzioni personalizzabili. Rimuovi tutte le impostazioni Override e imposta la frequenza di registrazione su Registrazione continua.

Puoi anche utilizzare un AWS CloudFormation modello per automatizzare questo processo. Per ulteriori informazioni, consulta i [modelli AWS CloudFormation StackSets di esempio](#) nella Guida per l'AWS CloudFormation utente.

Controlli Amazon Data Firehose

Questi controlli sono correlati alle risorse di Amazon Data Firehose.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi

Requisiti correlati: NIST.800-53.r5 AC-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::KinesisFirehose::DeliveryStream

Regola AWS Config : [kinesis-firehose-delivery-stream-encrypted](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un flusso di distribuzione di Amazon Data Firehose è crittografato quando è inattivo con crittografia lato server. Questo controllo fallisce se un flusso di distribuzione Firehose non è crittografato a riposo con la crittografia lato server.

La crittografia lato server è una funzionalità dei flussi di distribuzione di Amazon Data Firehose che crittografa automaticamente i dati prima che siano inattivi utilizzando una chiave creata in (). AWS Key Management Service AWS KMS I dati vengono crittografati prima di essere scritti nel layer di storage stream Data Firehose e decrittografati dopo essere stati recuperati dallo storage. Ciò consente di rispettare i requisiti normativi e di migliorare la sicurezza dei dati.

Correzione

Per abilitare la crittografia lato server sui flussi di distribuzione Firehose, consulta la sezione [Protezione dei dati in Amazon Data Firehose nella Amazon Data Firehose Developer Guide](#).

Controlli Amazon Detective

Questi controlli sono legati alle risorse del Detective.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[Detective.1] I grafici del comportamento dei Detective devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::Detective::Graph

AWS Config regola: tagged-detective-graph (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un grafico comportamentale di Amazon Detective contiene tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il grafico del comportamento non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il grafico del comportamento non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un grafico del comportamento di un Detective, consulta [Aggiungere tag a un grafico comportamentale](#) nella Amazon Detective Administration Guide.

AWS Database Migration Service controlli

Questi controlli sono correlati alle AWS DMS risorse.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[DMS.1] Le istanze di replica del Database Migration Service non devono essere pubbliche

Requisiti correlati: PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.4, PCI DSS versione 3.2.1/1.3.2, PCI DSS versione 3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.r5 SC-7 (16),

NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20) 3.5 SC-7 (21), NIT 800-53.r5 SC-7 (3), NIT 800-53.5 SC-7 (4), NIT 800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: AWS::DMS::ReplicationInstance

Regola AWS Config : [dms-replication-not-public](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se le istanze di AWS DMS replica sono pubbliche. A tale scopo, esamina il valore del campo. PubliclyAccessible

Un'istanza di replica privata ha un indirizzo IP privato a cui non è possibile accedere al di fuori della rete di replica. Un'istanza di replica deve avere un indirizzo IP privato quando i database di origine e di destinazione si trovano nella stessa rete. La rete deve inoltre essere connessa al VPC dell'istanza di replica utilizzando una VPN o un AWS Direct Connect peering VPC. Per ulteriori informazioni sulle istanze di replica pubbliche e private, consulta Istanze di replica [pubbliche e private](#) nella Guida per l'utente.AWS Database Migration Service

È inoltre necessario assicurarsi che l'accesso alla configurazione dell' AWS DMS istanza sia limitato ai soli utenti autorizzati. A tale scopo, limita le autorizzazioni IAM degli utenti per modificare AWS DMS impostazioni e risorse.

Correzione

Non è possibile modificare l'impostazione di accesso pubblico per un'istanza di replica DMS dopo averla creata. Per modificare l'impostazione di accesso pubblico, [elimina l'istanza corrente](#) e quindi [ricreala](#). Non selezionare l'opzione Accessibile pubblicamente.

[DMS.2] I certificati DMS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::DMS::Certificate

AWS Config regola: tagged-dms-certificate (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un AWS DMS certificato ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il certificato non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il certificato non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un certificato DMS, consulta [Tagging resources AWS Database Migration Service nella Guida per l'utente.AWS Database Migration Service](#)

[DMS.3] Le sottoscrizioni agli eventi DMS devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::DMS::EventSubscription

AWS Config regola: tagged-dms-eventsubscription (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se una sottoscrizione a un AWS DMS evento ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se la sottoscrizione all'evento non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di

tag e fallisce se la sottoscrizione all'evento non è contrassegnata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing. Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in [Riferimenti generali di AWS](#)

Correzione

Per aggiungere tag a un abbonamento a un evento DMS, consulta [Tagging resources AWS Database Migration Service nella Guida per l'utente](#). AWS Database Migration Service

[DMS.4] Le istanze di replica DMS devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::DMS::ReplicationInstance`

AWS Config regola: `tagged-dms-replicationinstance` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un'istanza di AWS DMS replica ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo ha esito negativo se l'istanza di replica non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'istanza di replica non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'istanza di replica DMS, consulta [Tagging resources nella AWS Database Migration Service Guida per l'utente](#).AWS Database Migration Service

[DMS.5] I sottoreti di replica DMS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::DMS::ReplicationSubnetGroup

AWS Config regola: tagged-dms-replicationsubnetgroup (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un gruppo di sottoreti di AWS DMS replica dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo ha esito negativo se il gruppo di sottorete di replica non dispone di chiavi di tag o se non dispone di tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di sottorete di replica non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un sottogruppo di replica DMS, consulta [Tagging resources](#) nella Guida per l'utente. AWS Database Migration ServiceAWS Database Migration Service

[DMS.6] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato

Requisiti correlati: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoria: Rileva > Gestione di vulnerabilità, patch e versioni

Gravità: media

Tipo di risorsa: AWS::DMS::ReplicationInstance

Regola AWS Config : [dms-auto-minor-version-upgrade-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'aggiornamento automatico della versione secondaria è abilitato per un'istanza di AWS DMS replica. Il controllo fallisce se l'aggiornamento automatico della versione secondaria non è abilitato per un'istanza di replica DMS.

DMS fornisce l'aggiornamento automatico delle versioni secondarie a ciascun motore di replica supportato, in modo da poter mantenere l'istanza di replica up-to-date. Le versioni minori possono introdurre nuove funzionalità software, correzioni di bug, patch di sicurezza e miglioramenti delle prestazioni. Abilitando l'aggiornamento automatico delle versioni secondarie sulle istanze di replica DMS, gli aggiornamenti minori vengono applicati automaticamente durante la finestra di manutenzione o immediatamente se viene selezionata l'opzione *Applica modifiche immediatamente*.

Correzione

Per abilitare l'aggiornamento automatico delle versioni secondarie sulle istanze di replica DMS, vedere [Modifica](#) di un'istanza di replica nella Guida per l'utente AWS Database Migration Service

[DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIS.800-53.R 5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::DMS::ReplicationTask

Regola AWS Config : [dms-replication-task-targetdb-logging](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la registrazione è abilitata con il livello di gravità minimo di `LOGGER_SEVERITY_DEFAULT` per le attività di replica DMS e. `TARGET_APPLY TARGET_LOAD II`

controllo ha esito negativo se la registrazione non è abilitata per queste attività o se il livello di gravità minimo è inferiore a. `LOGGER_SEVERITY_DEFAULT`

DMS utilizza Amazon CloudWatch per registrare le informazioni durante il processo di migrazione. Utilizzando le impostazioni delle attività di registrazione, puoi specificare quali attività dei componenti vengono registrate e quante informazioni vengono registrate. È necessario specificare la registrazione per le seguenti attività:

- `TARGET_APPLY`: i dati e le istruzioni DDL (Data Definition Language) vengono applicati al database di destinazione.
- `TARGET_LOAD`: i dati vengono caricati nel database di destinazione.

La registrazione svolge un ruolo fondamentale nelle attività di replica DMS poiché consente il monitoraggio, la risoluzione dei problemi, il controllo, l'analisi delle prestazioni, il rilevamento e il ripristino degli errori, nonché l'analisi e il reporting cronologici. Contribuisce a garantire la corretta replica dei dati tra database, mantenendo al contempo l'integrità dei dati e la conformità ai requisiti normativi. Livelli di registrazione diversi da `DEFAULT` sono raramente necessari per questi componenti durante la risoluzione dei problemi. Si consiglia di mantenere il livello di registrazione come `DEFAULT` per questi componenti, a meno che non venga espressamente richiesto di modificarlo entro. AWS Support Un livello di registrazione minimo `DEFAULT` garantisce che i messaggi informativi, gli avvisi e i messaggi di errore vengano scritti nei log. Questo controllo verifica se il livello di registrazione è almeno uno dei seguenti per le attività di replica precedenti:, o. `LOGGER_SEVERITY_DEFAULT` `LOGGER_SEVERITY_DEBUG` `LOGGER_SEVERITY_DETAILED_DEBUG`

Correzione

Per abilitare la registrazione per le attività di replica DMS del database di destinazione, vedere [Visualizzazione e gestione dei AWS DMS](#) registri delle attività nella Guida per l'utente.AWS Database Migration Service

[DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIS.800-53.R 5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::DMS::ReplicationTask

Regola AWS Config : [dms-replication-task-sourcedb-logging](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la registrazione è abilitata con il livello di gravità minimo di `LOGGER_SEVERITY_DEFAULT` per le attività di replica DMS e `SOURCE_CAPTURE` `SOURCE_UNLOAD`. Il controllo ha esito negativo se la registrazione non è abilitata per queste attività o se il livello di gravità minimo è inferiore a `LOGGER_SEVERITY_DEFAULT`.

DMS utilizza Amazon CloudWatch per registrare le informazioni durante il processo di migrazione. Utilizzando le impostazioni delle attività di registrazione, puoi specificare quali attività dei componenti vengono registrate e quante informazioni vengono registrate. È necessario specificare la registrazione per le seguenti attività:

- `SOURCE_CAPTURE`— I dati di replica continua o di acquisizione dei dati di modifica (CDC) vengono acquisiti dal database o dal servizio di origine e passati al componente del `SORTER` servizio.
- `SOURCE_UNLOAD`— I dati vengono scaricati dal database o dal servizio di origine durante il pieno caricamento.

La registrazione svolge un ruolo fondamentale nelle attività di replica DMS poiché consente il monitoraggio, la risoluzione dei problemi, il controllo, l'analisi delle prestazioni, il rilevamento e il ripristino degli errori, nonché l'analisi e il reporting cronologici. Contribuisce a garantire la corretta replica dei dati tra database, mantenendo al contempo l'integrità dei dati e la conformità ai requisiti normativi. Livelli di registrazione diversi da `DEFAULT` sono raramente necessari per questi componenti durante la risoluzione dei problemi. Si consiglia di mantenere il livello di registrazione come `DEFAULT` per questi componenti, a meno che non venga espressamente richiesto di modificarlo entro. AWS Support Un livello di registrazione minimo `DEFAULT` garantisce che i messaggi informativi, gli avvisi e i messaggi di errore vengano scritti nei log. Questo controllo verifica se il livello di registrazione è almeno uno dei seguenti per le attività di replica precedenti:, o. `LOGGER_SEVERITY_DEFAULT` `LOGGER_SEVERITY_DEBUG` `LOGGER_SEVERITY_DETAILED_DEBUG`

Correzione

Per abilitare la registrazione per le attività di replica DMS del database di origine, vedere [Visualizzazione e gestione dei AWS DMS](#) registri delle attività nella Guida per l'utente. AWS Database Migration Service

[DMS.9] Gli endpoint DMS devono utilizzare SSL

Requisiti correlati: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (1) -53,5 SC-8 (2)

Categoria: Protezione > Crittografia di data-in-transit

Gravità: media

Tipo di risorsa: AWS::DMS::Endpoint

Regola AWS Config : [dms-endpoint-ssl-configured](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS DMS endpoint utilizza una connessione SSL. Il controllo fallisce se l'endpoint non utilizza SSL.

Le connessioni SSL/TLS forniscono un livello di sicurezza crittografando le connessioni tra le istanze di replica DMS e il database. L'utilizzo dei certificati fornisce un ulteriore livello di sicurezza convalidando che la connessione venga stabilita al database previsto. A tale scopo, verifica il certificato del server che viene installato automaticamente su tutte le istanze di database fornite. Abilitando la connessione SSL sugli endpoint DMS, proteggi la riservatezza dei dati durante la migrazione.

Correzione

Per aggiungere una connessione SSL a un endpoint DMS nuovo o esistente, consulta [Using SSL](#) with nella Guida per l'utente. AWS Database Migration Service AWS Database Migration Service

[DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata

Requisiti correlati: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-17, NIST.800-53.r5 IA-2, NIST.800-53.r5 IA-5

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: media

Tipo di risorsa: AWS::DMS::Endpoint

Regola AWS Config : [dms-neptune-iam-authorization-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS DMS endpoint per un database Amazon Neptune è configurato con l'autorizzazione IAM. Il controllo fallisce se l'endpoint DMS non ha l'autorizzazione IAM abilitata.

AWS Identity and Access Management (IAM) fornisce un controllo granulare degli accessi su tutto il territorio. AWS Con IAM, puoi specificare chi può accedere a quali servizi e risorse e in quali condizioni. Con le policy IAM, gestisci le autorizzazioni per la tua forza lavoro e i tuoi sistemi per garantire le autorizzazioni con privilegi minimi. Abilitando l'autorizzazione IAM sugli AWS DMS endpoint per i database Neptune, puoi concedere privilegi di autorizzazione agli utenti IAM utilizzando un ruolo di servizio specificato dal parametro. `ServiceAccessRoleARN`

Correzione

Per abilitare l'autorizzazione IAM sugli endpoint DMS per i database Neptune, consulta Using Amazon [Neptune come target nella Guida per l'utente](#). AWS Database Migration ServiceAWS Database Migration Service

[DMS.11] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato

Requisiti correlati: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-6, NIST.800-53.r5 IA-2, NIST.800-53.r5 IA-5

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: media

Tipo di risorsa: AWS::DMS::Endpoint

Regola AWS Config : [dms-mongo-db-authentication-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS DMS endpoint per MongoDB è configurato con un meccanismo di autenticazione. Il controllo fallisce se non è impostato un tipo di autenticazione per l'endpoint.

AWS Database Migration Service supporta due metodi di autenticazione per MongoDB: MONGODB-CR per MongoDB versione 2.x e SCRAM-SHA-1 per MongoDB versione 3.x o successiva. Questi metodi di autenticazione vengono utilizzati per autenticare e crittografare le password MongoDB se gli utenti desiderano utilizzare le password per accedere ai database. L'autenticazione sugli AWS DMS endpoint garantisce che solo gli utenti autorizzati possano accedere e modificare i dati migrati tra i database. Senza un'autenticazione adeguata, gli utenti non autorizzati potrebbero essere in grado di accedere ai dati sensibili durante il processo di migrazione. Ciò può causare violazioni dei dati, perdita di dati o altri incidenti di sicurezza.

Correzione

Per abilitare un meccanismo di autenticazione sugli endpoint DMS per MongoDB, consulta [Usare MongoDB](#) come fonte nella Guida per l'utente. AWS DMSAWS Database Migration Service

[DMS.12] Gli endpoint DMS per Redis devono avere TLS abilitato

Requisiti correlati: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-13

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: AWS::DMS::Endpoint

Regola AWS Config : [dms-redis-tls-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS DMS endpoint per Redis è configurato con una connessione TLS. Il controllo fallisce se sull'endpoint non è abilitato TLS.

TLS fornisce end-to-end sicurezza quando i dati vengono inviati tra applicazioni o database su Internet. Quando configuri la crittografia SSL per l'endpoint DMS, abilita la comunicazione crittografata tra i database di origine e di destinazione durante il processo di migrazione. Questo aiuta a prevenire l'intercettazione e l'intercettazione di dati sensibili da parte di malintenzionati. Senza la crittografia SSL, è possibile accedere ai dati sensibili, con conseguenti violazioni dei dati, perdita di dati o altri incidenti di sicurezza.

Correzione

Per abilitare una connessione TLS sugli endpoint DMS per Redis, consulta [Using Redis come target](#) nella Guida per l'utente. AWS Database Migration ServiceAWS Database Migration Service

Controlli Amazon DocumentDB

Questi controlli sono correlati alle risorse di Amazon DocumentDB.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[DocumentDB.1] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [docdb-cluster-encrypted](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon DocumentDB è crittografato a riposo. Il controllo fallisce se un cluster Amazon DocumentDB non è crittografato a riposo.

I dati inattivi si riferiscono a tutti i dati archiviati in uno storage persistente e non volatile per qualsiasi durata. La crittografia consente di proteggere la riservatezza di tali dati, riducendo il rischio che un utente non autorizzato possa accedervi. I dati nei cluster Amazon DocumentDB devono essere crittografati quando sono inattivi per un ulteriore livello di sicurezza. Amazon DocumentDB utilizza l'Advanced Encryption Standard (AES-256) a 256 bit per crittografare i dati utilizzando chiavi di crittografia memorizzate in (). AWS Key Management Service AWS KMS

Correzione

Puoi abilitare la crittografia a riposo quando crei un cluster Amazon DocumentDB. Non è possibile modificare le impostazioni di crittografia dopo aver creato un cluster. Per ulteriori informazioni, consulta [Enabling encryption at rest for an Amazon DocumentDB cluster nella Amazon DocumentDB Developer Guide](#).

[DocumentDB.2] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato

Requisiti correlati: NIST.800-53.r5 SI-12

Categoria: Ripristino > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [docdb-cluster-backup-retention-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personali zzati consentiti	Valore predefinito di Security Hub
minimumBackupRetention	Periodo minimo di conservazione dei backup in giorni	Numero intero	7 Da a 35	7

Parametro	Descrizione	Type	Valori personali zzati consentiti	Valore predefinito di Security Hub
tionPeriod				

Questo controllo verifica se un cluster Amazon DocumentDB ha un periodo di conservazione dei backup maggiore o uguale al periodo di tempo specificato. Il controllo fallisce se il periodo di conservazione del backup è inferiore al periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di conservazione del backup, Security Hub utilizza un valore predefinito di 7 giorni.

I backup aiutano a ripristinare più rapidamente un incidente di sicurezza e a rafforzare la resilienza dei sistemi. Automatizzando i backup per i cluster Amazon DocumentDB, sarai in grado di ripristinare i sistemi in un determinato momento e ridurre al minimo i tempi di inattività e la perdita di dati. In Amazon DocumentDB, i cluster hanno un periodo di conservazione dei backup predefinito di 1 giorno. Questo periodo deve essere aumentato a un valore compreso tra 7 e 35 giorni per passare questo controllo.

Correzione

Per modificare il periodo di conservazione dei backup per i cluster Amazon DocumentDB, consulta [Modifying an Amazon DocumentDB cluster nella Amazon DocumentDB Developer Guide](#). Per Backup, scegli il periodo di conservazione del backup.

[DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa:AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

Regola AWS Config : [docdb-cluster-snapshot-public-prohibited](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se uno snapshot manuale del cluster di Amazon DocumentDB è pubblico. Il controllo fallisce se lo snapshot manuale del cluster è pubblico.

Uno snapshot manuale del cluster di Amazon DocumentDB non deve essere pubblico a meno che non sia previsto. Se condividi uno snapshot manuale non crittografato come pubblico, lo snapshot è disponibile per tutti. Account AWS Le istantanee pubbliche possono causare un'esposizione involontaria dei dati.

Note

Questo controllo valuta le istantanee manuali del cluster. Non puoi condividere uno snapshot del cluster automatizzato di Amazon DocumentDB. Tuttavia, puoi creare uno snapshot manuale copiando lo snapshot automatico e quindi condividerlo.

Correzione

Per rimuovere l'accesso pubblico agli snapshot manuali dei cluster di Amazon DocumentDB, consulta [Sharing a snapshot nella Amazon DocumentDB Developer Guide](#). A livello di codice, puoi utilizzare l'operazione Amazon DocumentDB. `modify-db-snapshot-attribute` Imposta `attribute-name` come `e.comerestore`. `values-to-remove` all

[DocumentDB.4] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIS.800-53.R 5 SI-4 (20), NID 800-53.R 5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [docdb-cluster-audit-logging-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon DocumentDB pubblica log di audit su Amazon Logs. CloudWatch Il controllo fallisce se il cluster non pubblica i log di controllo su Logs. CloudWatch

Amazon DocumentDB (con compatibilità con MongoDB) ti consente di controllare gli eventi che sono stati eseguiti nel tuo cluster. Sono esempi di eventi registrati i tentativi di autenticazione riusciti e non riusciti, l'eliminazione di una raccolta in un database o la creazione di un indice. Per impostazione predefinita, il controllo è disabilitato in Amazon DocumentDB e richiede l'intervento dell'utente per abilitarlo.

Correzione

Per pubblicare i log di audit di Amazon DocumentDB su CloudWatch Logs, consulta [Enabling auditing nella Amazon DocumentDB Developer Guide](#).

[DocumentDB.5] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoria: Proteggi > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [docdb-cluster-deletion-protection-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon DocumentDB ha la protezione da eliminazione abilitata. Il controllo fallisce se nel cluster non è abilitata la protezione da eliminazione.

L'attivazione della protezione dall'eliminazione del cluster offre un ulteriore livello di protezione contro l'eliminazione accidentale del database o l'eliminazione da parte di un utente non autorizzato. Un cluster Amazon DocumentDB non può essere eliminato mentre la protezione da eliminazione è abilitata. È necessario innanzitutto disabilitare la protezione da eliminazione prima che una richiesta di eliminazione possa avere successo. La protezione da eliminazione è abilitata per impostazione predefinita quando crei un cluster nella console Amazon DocumentDB.

Correzione

Per abilitare la protezione da eliminazione per un cluster Amazon DocumentDB esistente, consulta [Modifying an Amazon DocumentDB cluster nella Amazon DocumentDB Developer Guide](#). Nella sezione Modifica cluster, scegli Abilita la protezione da eliminazione.

Controlli Amazon DynamoDB

Questi controlli sono correlati alle risorse DynamoDB.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[DynamoDB.1] Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::DynamoDB::Table

Regola AWS Config : [dynamodb-autoscaling-enabled](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personalizzati validi	Valore predefinito di Security Hub
<code>minProvisionedReadCapacity</code>	Numero minimo di unità di capacità di lettura assegnate per la scalabilità automatica di DynamoDB	Numero intero	1 Da a 40000	Nessun valore predefinito
<code>targetReadUtilization</code>	Percentuale di utilizzo prevista per la capacità di lettura	Numero intero	20 Da a 90	Nessun valore predefinito
<code>minProvisionedWriteCapacity</code>	Numero minimo di unità di capacità di scrittura assegnate per la scalabilità automatica di DynamoDB	Numero intero	1 Da a 40000	Nessun valore predefinito
<code>targetWriteUtilization</code>	Percentuale di utilizzo prevista per la capacità di scrittura	Numero intero	20 Da a 90	Nessun valore predefinito

Questo controllo verifica se una tabella Amazon DynamoDB è in grado di scalare la propria capacità di lettura e scrittura in base alle esigenze. Il controllo fallisce se la tabella non utilizza la modalità di capacità su richiesta o la modalità provisioning con scalabilità automatica configurata. Per impostazione predefinita, questo controllo richiede solo la configurazione di una di queste modalità, indipendentemente da livelli specifici di capacità di lettura o scrittura. Facoltativamente, è possibile fornire valori di parametri personalizzati per richiedere livelli specifici di capacità di lettura e scrittura o di utilizzo del target.

La scalabilità della capacità in base alla domanda evita le eccezioni di limitazione, il che aiuta a mantenere la disponibilità delle applicazioni. Le tabelle DynamoDB in modalità di capacità su richiesta sono limitate solo dalle quote di tabella predefinite del throughput di DynamoDB. Per aumentare queste quote, puoi inviare un ticket di supporto con AWS Support tabelle.DynamoDB in modalità provisioned con auto scaling, regolare dinamicamente la capacità di throughput assegnata in base ai modelli di traffico. Per ulteriori informazioni sulla limitazione delle richieste di DynamoDB, [consulta Request throttling and burst capacity nella Amazon DynamoDB Developer Guide](#).

Correzione

Per abilitare la scalabilità automatica di DynamoDB su tabelle esistenti in modalità capacità, consulta [Enabling DynamoDB auto scaling su tabelle esistenti nella Amazon DynamoDB Developer Guide](#).

[DynamoDB.2] Le tabelle DynamoDB dovrebbero avere il ripristino abilitato point-in-time

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST.800-53.r5 SI-13 (5)

Categoria: Ripristino > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: AWS::DynamoDB::Table

Regola AWS Config : [dynamodb-pitr-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il point-in-time ripristino (PITR) è abilitato per una tabella Amazon DynamoDB.

I backup consentono di ripristinare più rapidamente un incidente di sicurezza. Inoltre, rafforzano la resilienza dei sistemi. Il ripristino point-in-time DynamoDB automatizza i backup per le tabelle DynamoDB. Riduce i tempi di ripristino in seguito a operazioni di cancellazione o scrittura accidentali. Le tabelle DynamoDB con PITR abilitato possono essere ripristinate in qualsiasi momento negli ultimi 35 giorni.

Correzione

Per ripristinare una tabella DynamoDB in un momento specifico, consulta [Restoring a DynamoDB table to a point-in-time nella Amazon DynamoDB Developer Guide](#).

[DynamoDB.3] I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::DynamoDB::Cluster

Regola AWS Config : [dax-encryption-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un cluster DAX è crittografato quando è inattivo.

La crittografia dei dati inattivi riduce il rischio di accesso ai dati archiviati su disco da parte di un utente non autenticato. AWS La crittografia aggiunge un altro set di controlli di accesso per limitare la capacità degli utenti non autorizzati di accedere ai dati. Ad esempio, sono necessarie le autorizzazioni API per decrittografare i dati prima che possano essere letti.

Correzione

Non è possibile abilitare o disabilitare la crittografia a riposo dopo la creazione di un cluster. È necessario ricreare il cluster per abilitare la crittografia a riposo. Per istruzioni dettagliate su come creare un cluster DAX con la crittografia a riposo abilitata, consulta [Enabling encryption at rest using the AWS Management Console](#) nella Amazon DynamoDB Developer Guide.

[DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST .800-53,5 SI-13 (5)

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: AWS::DynamoDB::Table

AWS Config regola: [dynamodb-resources-protected-by-backup-plan](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
backupVaultLockCheck	Il controllo restituisce un PASSED risultato se il parametro è impostato su true e la risorsa utilizza AWS Backup Vault Lock.	Booleano	true o false	Nessun valore predefinito

Questo controllo valuta se una ACTIVE tabella Amazon DynamoDB in stato è coperta da un piano di backup. Il controllo fallisce se la tabella DynamoDB non è coperta da un piano di backup. Se si imposta il backupVaultLockCheck parametro uguale a true, il controllo passa solo se viene eseguito il backup della tabella DynamoDB in AWS Backup un vault bloccato.

AWS Backup è un servizio di backup completamente gestito che consente di centralizzare e automatizzare il backup dei dati in tutto il mondo. Servizi AWS Con AWS Backup, è possibile creare piani di backup che definiscono i requisiti di backup, ad esempio la frequenza con cui eseguire il backup dei dati e per quanto tempo conservare tali backup. L'inclusione delle tabelle DynamoDB nei piani di backup consente di proteggere i dati da perdite o cancellazioni involontarie.

Correzione

Per aggiungere una tabella DynamoDB a AWS Backup un piano di backup, [consulta Assegnazione di risorse a un piano di backup](#) nella Developer Guide.AWS Backup

[DynamoDB.5] Le tabelle DynamoDB devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::DynamoDB::Table

AWS Config regola: tagged-dynamodb-table (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se una tabella Amazon DynamoDB contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la tabella non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la tabella non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una tabella DynamoDB, [consulta Tagging resources in DynamoDB nella Amazon DynamoDB Developer Guide](#).

[DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoria: Proteggi > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: media

Tipo di risorsa: AWS::DynamoDB::Table

AWS Config regola: [dynamodb-table-deletion-protection-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una tabella Amazon DynamoDB ha la protezione da eliminazione abilitata. Il controllo fallisce se una tabella DynamoDB non ha la protezione da eliminazione abilitata.

È possibile proteggere una tabella DynamoDB dall'eliminazione accidentale con la proprietà di protezione dall'eliminazione. L'attivazione di questa proprietà per le tabelle aiuta a garantire che le tabelle non vengano eliminate accidentalmente durante le normali operazioni di gestione delle tabelle da parte degli amministratori. Questo aiuta a prevenire interruzioni delle normali operazioni aziendali.

Correzione

Per abilitare la protezione da eliminazione per una tabella DynamoDB, [consulta](#) Using delete protection nella Amazon DynamoDB Developer Guide.

[DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito

Requisiti correlati: NIST.800-53.r5 AC-17, NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: AWS::DynamoDB::Table

AWS Config regola: [dax-tls-endpoint-encryption](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un cluster Amazon DynamoDB Accelerator (DAX) è crittografato in transito, con il tipo di crittografia degli endpoint impostato su TLS. Il controllo fallisce se il cluster DAX non è crittografato in transito.

HTTPS (TLS) può essere utilizzato per impedire a potenziali aggressori di utilizzare person-in-the-middle o attacchi simili per intercettare o manipolare il traffico di rete. È necessario consentire solo alle connessioni crittografate tramite TLS di accedere ai cluster DAX. Tuttavia, la crittografia dei dati in transito può influire sulle prestazioni. È consigliabile testare l'applicazione con la crittografia attivata per comprendere il profilo delle prestazioni e l'impatto del TLS.

Correzione

Non è possibile modificare l'impostazione di crittografia TLS dopo aver creato un cluster DAX. Per crittografare un cluster DAX esistente, crea un nuovo cluster con la crittografia in transito abilitata, sposta il traffico dell'applicazione su di esso, quindi elimina il vecchio cluster. Per ulteriori informazioni, consulta [Using Deletion Protection](#) nella Amazon DynamoDB Developer Guide.

Controlli di Amazon Elastic Container Registry

Questi controlli sono correlati alle risorse Amazon ECR.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[ECR.1] Gli archivi privati ECR devono avere la scansione delle immagini configurata

Requisiti correlati: NIST.800-53.R5 RA-5

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: alta

Tipo di risorsa: AWS::ECR::Repository

Regola AWS Config : [ecr-private-image-scanning-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se in un repository Amazon ECR privato è configurata la scansione delle immagini. Il controllo fallisce se l'archivio ECR privato non è configurato per la scansione in modalità push o la scansione continua.

La scansione delle immagini ECR aiuta a identificare le vulnerabilità del software nelle immagini dei contenitori. La configurazione della scansione delle immagini negli archivi ECR aggiunge un livello di verifica dell'integrità e della sicurezza delle immagini archiviate.

Correzione

Per configurare la scansione delle immagini per un repository ECR, consulta [Scansione delle immagini](#) nella Amazon Elastic Container Registry User Guide.

[ECR.2] I repository privati ECR devono avere l'immutabilità dei tag configurata

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-8 (1)

Categoria: Identificazione > Inventario > Etichettatura

Gravità: media

Tipo di risorsa: AWS::ECR::Repository

Regola AWS Config : [ecr-private-tag-immutability-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un repository ECR privato ha l'immutabilità dei tag abilitata. Questo controllo ha esito negativo se in un repository ECR privato l'immutabilità dei tag è disabilitata. Questa regola è valida se l'immutabilità dei tag è abilitata e ha il valore. IMMUTABLE

Amazon ECR Tag Immutability consente ai clienti di fare affidamento sui tag descrittivi di un'immagine come meccanismo affidabile per tracciare e identificare in modo univoco le immagini.

Un tag immutabile è statico, il che significa che ogni tag fa riferimento a un'immagine unica. Ciò migliora l'affidabilità e la scalabilità poiché l'uso di un tag statico porterà sempre alla distribuzione della stessa immagine. Una volta configurata, l'immutabilità dei tag impedisce che i tag vengano sovrascritti, riducendo la superficie di attacco.

Correzione

Per creare un repository con tag immutabili configurati o per aggiornare le impostazioni di mutabilità dei tag di immagine per un repository esistente, consulta [Image tag mutability nella Amazon Elastic Container Registry User Guide](#).

[ECR.3] I repository ECR devono avere almeno una politica del ciclo di vita configurata

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificazione > Configurazione delle risorse

Gravità: media

Tipo di risorsa: AWS::ECR::Repository

Regola AWS Config : [ecr-private-lifecycle-policy-configured](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un repository Amazon ECR ha almeno una policy del ciclo di vita configurata. Questo controllo fallisce se un repository ECR non ha alcuna politica del ciclo di vita configurata.

Le policy del ciclo di vita di Amazon ECR consentono di specificare la gestione del ciclo di vita delle immagini in un repository. Configurando le politiche del ciclo di vita, è possibile automatizzare la pulizia delle immagini non utilizzate e la scadenza delle immagini in base all'età o al numero di immagini. L'automazione di queste attività può aiutarti a evitare l'uso involontario di immagini obsolete nel tuo repository.

Correzione

Per configurare una policy del ciclo di vita, consulta [Creating a lifecycle policy preview nella Amazon Elastic Container Registry User Guide](#).

[ECR.4] Gli archivi pubblici ECR devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::ECR::PublicRepository

AWS Config regola: tagged-ecr-publicrepository (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un repository pubblico Amazon ECR dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'archivio pubblico non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'archivio pubblico non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un repository pubblico ECR, consulta [Tagging an Amazon ECR public repository nella Amazon](#) Elastic Container Registry User Guide.

Controlli Amazon ECS

Questi controlli sono correlati alle risorse Amazon ECS.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[ECS.1] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: alta

Tipo di risorsa: AWS::ECS::TaskDefinition

Regola AWS Config : [ecs-task-definition-user-for-host-mode-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `SkipInactiveTaskDefinitions`: true (non personalizzabile)

Questo controllo verifica se una definizione di attività Amazon ECS attiva con modalità di rete host include definizioni `privileged` di `user container`. Il controllo ha esito negativo per le definizioni di attività che hanno definizioni di modalità di rete host e contenitore `privileged=false` uguali, vuote e/o vuote. `user=root`

Questo controllo valuta solo l'ultima revisione attiva di una definizione di attività Amazon ECS.

Lo scopo di questo controllo è garantire che l'accesso sia definito intenzionalmente quando si eseguono attività che utilizzano la modalità di rete host. Se una definizione di attività ha privilegi elevati, è perché hai scelto quella configurazione. Questo controllo verifica l'eventuale aumento imprevisto dei privilegi quando la definizione di un'attività ha la rete host abilitata e non si scelgono privilegi elevati.

Correzione

Per informazioni su come aggiornare una definizione di attività, consulta la sezione [Aggiornamento di una definizione di attività](#) nella Amazon Elastic Container Service Developer Guide.

Quando aggiorni una definizione di attività, non aggiorna le attività in esecuzione che sono state avviate dalla definizione di attività precedente. Per aggiornare un'attività in esecuzione, è necessario ridistribuire l'attività con la nuova definizione di attività.

[ECS.2] Ai servizi ECS non devono essere assegnati automaticamente indirizzi IP pubblici

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: AWS::ECS::Service

AWS Config regola: `ecs-service-assign-public-ip-disabled` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

- `exemptEcsServiceArns`(non personalizzabile). Security Hub non inserisce questo parametro. Elenco separato da virgole di ARN dei servizi Amazon ECS che sono esenti da questa regola.

Questa regola si applica `COMPLIANT` se un servizio Amazon ECS è `AssignPublicIP` impostato su `ENABLED` ed è specificato in questo elenco di parametri.

Questa regola si `NON_COMPLIANT` applica se un servizio Amazon ECS è `AssignPublicIP` impostato `ENABLED` e non è specificato in questo elenco di parametri.

Questo controllo verifica se i servizi Amazon ECS sono configurati per assegnare automaticamente indirizzi IP pubblici. Se `AssignPublicIP` lo è, questo controllo fallisce. `ENABLED` Questo controllo viene eseguito se lo `AssignPublicIP` è `DISABLED`.

Un indirizzo IP pubblico è un indirizzo IP raggiungibile da Internet. Se avvii le istanze Amazon ECS con un indirizzo IP pubblico, le istanze Amazon ECS sono raggiungibili da Internet. I servizi Amazon ECS non devono essere accessibili al pubblico, in quanto ciò potrebbe consentire l'accesso involontario ai server delle applicazioni container.

Correzione

Per disabilitare l'assegnazione automatica degli IP pubblici, consulta [Per configurare le impostazioni di VPC e gruppi di sicurezza per il tuo servizio](#) nella Amazon Elastic Container Service Developer Guide.

[ECS.3] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Identifica > Configurazione delle risorse

Gravità: alta

Tipo di risorsa: `AWS::ECS::TaskDefinition`

AWS Config regola: [ecs-task-definition-pid-mode-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le definizioni delle attività di Amazon ECS sono configurate per condividere lo spazio dei nomi dei processi di un host con i relativi contenitori. Il controllo fallisce se la definizione dell'attività condivide lo spazio dei nomi del processo dell'host con i contenitori in esecuzione su di esso. Questo controllo valuta solo l'ultima revisione attiva di una definizione di attività Amazon ECS.

Uno spazio dei nomi PID (Process ID) fornisce la separazione tra i processi. Impedisce la visibilità dei processi di sistema e consente il riutilizzo dei PID, incluso il PID 1. Se lo spazio dei nomi PID dell'host è condiviso con i contenitori, consentirebbe ai contenitori di visualizzare tutti i processi sul sistema host. Ciò riduce i vantaggi dell'isolamento a livello di processo tra l'host e i contenitori. Queste circostanze potrebbero portare all'accesso non autorizzato ai processi sull'host stesso, inclusa la possibilità di manipolarli e terminarli. I clienti non devono condividere lo spazio dei nomi dei processi dell'host con i contenitori in esecuzione su di esso.

Correzione

Per configurare la `pidMode` definizione di un'attività, consulta [i parametri di definizione dell'attività](#) nella Amazon Elastic Container Service Developer Guide.

[ECS.4] I contenitori ECS devono essere eseguiti come non privilegiati

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Categoria: Proteggi > Gestione sicura degli accessi > Restrizioni all'accesso degli utenti root

Gravità: alta

Tipo di risorsa: `AWS::ECS::TaskDefinition`

Regola AWS Config: [ecs-containers-nonprivileged](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il `privileged` parametro nella definizione del contenitore di Amazon ECS Task Definitions è impostato `true` su. Il controllo fallisce se questo parametro è uguale a `true`. Questo controllo valuta solo l'ultima revisione attiva di una definizione di attività Amazon ECS.

Ti consigliamo di rimuovere i privilegi elevati dalle definizioni delle attività ECS. Quando il parametro `privileged` è `true`, al contenitore vengono assegnati privilegi elevati sull'istanza del contenitore host (analogamente all'utente `root`).

Correzione

Per configurare il `privileged` parametro su una definizione di attività, consulta [i parametri di definizione avanzata dei container](#) nella Amazon Elastic Container Service Developer Guide.

[ECS.5] I contenitori ECS devono essere limitati all'accesso in sola lettura ai filesystem `root`

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: alta

Tipo di risorsa: `AWS::ECS::TaskDefinition`

Regola AWS Config: [ecs-containers-readonly-access](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i contenitori Amazon ECS sono limitati all'accesso in sola lettura ai filesystem `root` montati. Il controllo fallisce se il `readonlyRootFilesystem` parametro è impostato su `false` o se il parametro non esiste nella definizione del contenitore all'interno della definizione dell'attività. Questo controllo valuta solo l'ultima revisione attiva di una definizione di attività Amazon ECS.

L'attivazione di questa opzione riduce i vettori di attacco alla sicurezza poiché il file system dell'istanza del contenitore non può essere manomesso o scritto su di esso a meno che l'istanza non disponga di autorizzazioni esplicite di lettura/scrittura sulla cartella e sulle directory del filesystem. Questo controllo aderisce anche al principio del privilegio minimo.

Correzione

Limitazione delle definizioni dei contenitori all'accesso in sola lettura ai filesystem root

1. Apri la console classica Amazon ECS all'indirizzo <https://console.aws.amazon.com/ecs/>.
2. Nel riquadro di navigazione a sinistra, scegli Definizioni delle attività.
3. Seleziona una definizione di attività con definizioni di contenitore che devono essere aggiornate. Per ognuno di essi, completa i seguenti passaggi:
 - Dal menu a discesa, scegli Crea nuova revisione con JSON.
 - Aggiungi il `readOnlyRootFilesystem` parametro e impostalo `true` nella definizione del contenitore all'interno della definizione dell'attività.
 - Scegli Crea.

[ECS.8] I segreti non devono essere passati come variabili di ambiente del contenitore

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Sviluppo sicuro > Credenziali non codificate

Gravità: alta

Tipo di risorsa: AWS::ECS::TaskDefinition

Regola AWS Config: [ecs-no-environment-secrets](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `SecretKeys = AWS_ACCESS_KEY_ID,AWS_SECRET_ACCESS_KEY, ECS_ENGINE_AUTH_DATA` (non personalizzabile)

Questo controllo verifica se il valore chiave di qualsiasi variabile nel `environment` parametro delle definizioni dei contenitori include `AWS_ACCESS_KEY_ID,AWS_SECRET_ACCESS_KEY`, o `ECS_ENGINE_AUTH_DATA`. Questo controllo ha esito negativo se una singola variabile di ambiente in qualsiasi definizione di contenitore è uguale a `AWS_ACCESS_KEY_ID,AWS_SECRET_ACCESS_KEY`, o `ECS_ENGINE_AUTH_DATA`. Questo controllo non copre le variabili ambientali trasmesse da altre

postazioni come Amazon S3. Questo controllo valuta solo l'ultima revisione attiva di una definizione di attività Amazon ECS.

AWS Systems Manager Parameter Store può aiutarti a migliorare il livello di sicurezza della tua organizzazione. Ti consigliamo di utilizzare Parameter Store per archiviare segreti e credenziali invece di passarli direttamente alle istanze del contenitore o di codificarli nel codice.

Correzione

Per creare parametri utilizzando SSM, vedere [Creazione dei parametri di Systems Manager](#) nella Guida per l'AWS Systems Manager utente. Per ulteriori informazioni sulla creazione di una definizione di attività che specifichi un segreto, consulta [Specificare dati sensibili utilizzando Secrets Manager](#) nella Amazon Elastic Container Service Developer Guide.

[ECS.9] Le definizioni delle attività ECS devono avere una configurazione di registrazione

Requisiti correlati: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (4) R5 CA-7, NIST. 800-53.R5 SC-7 (9), NIST. 800-53.5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: alta

Tipo di risorsa: AWS::ECS::TaskDefinition

AWS Config regola: ecs-task-definition-log [-configuration](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'ultima definizione di attività attiva di Amazon ECS ha una configurazione di registrazione specificata. Il controllo fallisce se la definizione dell'attività non ha la `LogConfiguration` proprietà definita o se il valore di `logDriver` è nullo in almeno una definizione di contenitore.

La registrazione aiuta a mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon ECS. La raccolta di dati dalle definizioni delle attività offre visibilità, che può aiutarti a eseguire il debug dei

processi e a trovare la causa principale degli errori. Se si utilizza una soluzione di registrazione che non deve essere definita nella definizione dell'attività ECS (ad esempio una soluzione di registrazione di terze parti), è possibile disabilitare questo controllo dopo aver verificato che i log vengano acquisiti e consegnati correttamente.

Correzione

Per definire una configurazione di log per le definizioni delle attività di Amazon ECS, consulta [Specificare una configurazione di log nella definizione del task nella Amazon Elastic Container Service Developer Guide](#).

[ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate

Requisiti correlati: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: media

Tipo di risorsa: AWS::ECS::Service

Regola AWS Config: [ecs-fargate-latest-platform-version](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `latestLinuxVersion`: 1.4.0(non personalizzabile)
- `latestWindowsVersion`: 1.0.0(non personalizzabile)

Questo controllo verifica se i servizi Amazon ECS Fargate eseguono l'ultima versione della piattaforma Fargate. Questo controllo fallisce se la versione della piattaforma non è la più recente.

AWS Fargate le versioni della piattaforma si riferiscono a un ambiente di runtime specifico per l'infrastruttura di attività Fargate, che è una combinazione di versioni di runtime del kernel e del container. Le nuove versioni della piattaforma vengono rilasciate man mano che l'ambiente di runtime si evolve. Ad esempio, può essere rilasciata una nuova versione per aggiornamenti del kernel o del sistema operativo, nuove funzionalità, correzioni di bug o aggiornamenti di sicurezza. Gli

aggiornamenti e le patch di sicurezza vengono implementati automaticamente per le attività Fargate. Se viene rilevato un problema di sicurezza che riguarda una versione della piattaforma, corregge la versione della AWS piattaforma.

Correzione

Per aggiornare un servizio esistente, inclusa la versione della piattaforma, consulta la sezione [Aggiornamento di un servizio](#) nella Amazon Elastic Container Service Developer Guide.

[ECS.12] I cluster ECS devono utilizzare Container Insights

Requisiti correlati: NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::ECS::Cluster

Regola AWS Config: [ecs-container-insights-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i cluster ECS utilizzano Container Insights. Questo controllo fallisce se Container Insights non è configurato per un cluster.

Il monitoraggio è una parte importante del mantenimento dell'affidabilità, della disponibilità e delle prestazioni dei cluster Amazon ECS. Usa CloudWatch Container Insights per raccogliere, aggregare e riepilogare metriche e log delle tue applicazioni e microservizi containerizzati. CloudWatch raccoglie automaticamente le metriche per molte risorse, come CPU, memoria, disco e rete. Container Insights fornisce inoltre informazioni diagnostiche, ad esempio errori di riavvio del container, che consentono di isolare i problemi e risolverli in modo rapido. Puoi anche impostare CloudWatch allarmi sulle metriche raccolte da Container Insights.

Correzione

Per utilizzare Container Insights, consulta la sezione [Aggiornamento di un servizio](#) nella Amazon CloudWatch User Guide.

[ECS.13] I servizi ECS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::ECS::Service

AWS Config regola: tagged-ecs-service (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un servizio Amazon ECS dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il servizio non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il servizio non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un servizio ECS, consulta [Tagging your Amazon ECS resources nella Amazon Elastic Container Service Developer Guide](#).

[ECS.14] I cluster ECS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::ECS::Cluster`

AWS Config regola: `tagged-ecs-cluster` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfan	Nessun valore predefinito

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se un cluster Amazon ECS dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il cluster non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il cluster non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in Riferimenti generali di AWS

Correzione

Per aggiungere tag a un cluster ECS, consulta [Tagging your Amazon ECS resources nella Amazon Elastic Container Service Developer Guide](#).

[ECS.15] Le definizioni delle attività ECS devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::ECS::TaskDefinition`

AWS Config regola: `tagged-ecs-taskdefinition` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se una definizione di attività di Amazon ECS contiene tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se la definizione dell'attività non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la definizione dell'attività non è contrassegnata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se gli snapshot di Amazon Elastic Block Store non sono pubblici. Il controllo fallisce se gli snapshot di Amazon EBS sono ripristinabili da chiunque.

Gli snapshot EBS vengono utilizzati per eseguire il backup dei dati sui volumi EBS su Amazon S3 in un momento specifico. Puoi utilizzare gli snapshot per ripristinare gli stati precedenti dei volumi EBS. Raramente è accettabile condividere uno snapshot con il pubblico. In genere la decisione di condividere pubblicamente uno snapshot viene presa per errore o senza una completa comprensione delle implicazioni. Questo controllo consente di garantire che tale condivisione sia stata completamente pianificata ed è intenzionale.

Per rendere privata una snapshot EBS pubblica, consulta [Share a snapshot](#) nella Amazon EC2 User Guide for Linux Instances. Per Azioni, Modifica le autorizzazioni, scegli Privato.

[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita

Requisiti correlati: PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.4, PCI DSS versione 3.2.1/2.1, benchmark CIS Foundations versione 1.2.0/4.3, benchmark CIS Foundations v1.4.0/5.3, benchmark CIS AWS Foundations v3.0.0/5.4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5) AWS AWS

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: AWS::EC2::SecurityGroup

Regola AWS Config : [vpc-default-security-group-closed](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il gruppo di sicurezza predefinito di un VPC consente il traffico in entrata o in uscita. Il controllo fallisce se il gruppo di sicurezza consente il traffico in entrata o in uscita.

Le regole per il [gruppo di sicurezza predefinito](#) consentono tutto il traffico in uscita e in ingresso dalle interfacce di rete (e le istanze associate) assegnate allo stesso gruppo di sicurezza. Ti consigliamo

di non utilizzare il gruppo di sicurezza predefinito. Poiché il gruppo di sicurezza predefinito non può essere eliminato, è necessario modificare l'impostazione delle regole di gruppo di sicurezza predefinito per limitare il traffico in ingresso e in uscita. Ciò impedisce il traffico non intenzionale se il gruppo di sicurezza predefinito viene configurato accidentalmente per risorse come le istanze EC2.

Correzione

Per risolvere questo problema, inizia creando nuovi gruppi di sicurezza con privilegi minimi. Per istruzioni, consulta [Creare un gruppo di sicurezza](#) nella Amazon VPC User Guide. Quindi, assegna i nuovi gruppi di sicurezza alle tue istanze EC2. Per istruzioni, consulta [Modificare il gruppo di sicurezza di un'istanza](#) nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Dopo aver assegnato i nuovi gruppi di sicurezza alle tue risorse, rimuovi tutte le regole in entrata e in uscita dai gruppi di sicurezza predefiniti. Per istruzioni, consulta [Eliminare le regole dei gruppi di sicurezza](#) nella Guida per l'utente di Amazon VPC.

[EC2.3] I volumi Amazon EBS collegati devono essere crittografati a riposo

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::EC2::Volume

Regola AWS Config : [encrypted-volumes](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i volumi EBS che si trovano in uno stato collegato sono crittografati. Per superare questo controllo, i volumi EBS devono essere in uso e crittografati. Se il volume EBS non è collegato, non è destinato a questo controllo.

Per un ulteriore livello di sicurezza dei dati sensibili nei volumi EBS, è necessario abilitare la crittografia EBS dei dati inattivi. La crittografia Amazon EBS offre una soluzione di crittografia semplice per le risorse EBS che non richiede di creare, mantenere e proteggere la propria infrastruttura di gestione delle chiavi. Utilizza le chiavi KMS per la creazione di volumi e istantanee crittografati.

Per ulteriori informazioni sulla crittografia Amazon EBS, consulta [Amazon EBS encryption](#) nella Amazon EC2 User Guide for Linux Instances.

Correzione

Non esiste un modo diretto per crittografare un volume o uno snapshot non crittografato esistente. È possibile crittografare un nuovo volume o snapshot solo quando viene creato.

Se hai abilitato la crittografia per impostazione predefinita, Amazon EBS crittografa il nuovo volume o snapshot risultante utilizzando la tua chiave predefinita per la crittografia Amazon EBS. Anche se non la crittografia non è abilitata per impostazione predefinita, è possibile abilitare la crittografia al momento della creazione di uno specifico volume o snapshot. In entrambi i casi, puoi sostituire la chiave predefinita per la crittografia Amazon EBS e scegliere una chiave simmetrica gestita dal cliente.

Per ulteriori informazioni, consulta [Creazione di un volume Amazon EBS](#) e [copia di uno snapshot Amazon EBS](#) nella Guida per l'utente di Amazon EC2 per le istanze Linux.

[EC2.4] Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificazione > Inventario

Gravità: media

Tipo di risorsa: AWS::EC2::Instance

Regola AWS Config : [ec2-stopped-instance](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
AllowedDays	Numero di giorni in cui l'istanza EC2 può rimanere	Numero intero	1 Da a 365	30

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	in uno stato di arresto prima della generazione di un risultato non riuscito.			

Questo controllo verifica se un'istanza Amazon EC2 è stata interrotta per un periodo superiore al numero di giorni consentito. Il controllo fallisce se un'istanza EC2 viene interrotta per un periodo di tempo superiore al periodo di tempo massimo consentito. A meno che non si fornisca un valore di parametro personalizzato per il periodo di tempo massimo consentito, Security Hub utilizza un valore predefinito di 30 giorni.

Quando un'istanza EC2 non viene eseguita per un periodo di tempo significativo, crea un rischio per la sicurezza perché l'istanza non viene gestita attivamente (analizzata, patchata, aggiornata). Se viene avviata in un secondo momento, la mancanza di una manutenzione adeguata potrebbe causare problemi imprevedibili nell'ambiente AWS. Per mantenere in modo sicuro un'istanza EC2 nel tempo in uno stato inattivo, avviala periodicamente per la manutenzione e poi interrompila dopo la manutenzione. Idealmente, questo dovrebbe essere un processo automatizzato.

Correzione

Per terminare un'istanza EC2 inattiva, consulta [Terminare un'istanza](#) nella Amazon EC2 User Guide for Linux Instances.

[EC2.6] La registrazione del flusso VPC deve essere abilitata in tutti i VPC

Requisiti correlati: Benchmark CIS AWS Foundations versione 1.2.0/2.9, benchmark CIS Foundations versione 1.4.0/3.9, benchmark CIS AWS Foundations versione 3.0.0/3.7, PCI DSS v3.2.1/10.3.3, PCI DSS versione 3.2.1/10.3.4, PCI DSS v3.2.1/10.3.5, PCI DSS v3.2.1/10.3.6, NIST.800-53.r5 AWS AC-4 (26), NIST.800-53.R5 AU-12, NIST.800-53.R5 AU-2, NIST.800-53.R5 AU-3, NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 CA-7, NIST.800-53.R5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS :: EC2 :: VPC

Regola AWS Config : [vpc-flow-logs-enabled](#)

Tipo di pianificazione: periodica

Parametri:

- `trafficType`: REJECT (non personalizzabile)

Questo controllo verifica se i log di flusso di Amazon VPC vengono trovati e abilitati per i VPC. Il tipo di traffico è impostato su. `Reject`

Con la funzione VPC Flow Logs, puoi acquisire informazioni sul traffico di indirizzi IP che va e viene dalle interfacce di rete nel tuo VPC. Dopo aver creato un log di flusso, puoi visualizzarne e recuperarne i dati in Logs. CloudWatch Per ridurre i costi, puoi anche inviare i log di flusso ad Amazon S3.

Security Hub consiglia di abilitare la registrazione del flusso per i pacchetti rifiutati per i VPC. I log di flusso forniscono visibilità sul traffico di rete che attraversa il VPC e possono rilevare traffico anomalo o fornire informazioni durante i flussi di lavoro di sicurezza.

Per impostazione predefinita, il record include i valori per i diversi componenti del flusso di indirizzi IP, tra cui origine, destinazione e protocollo. Per ulteriori informazioni e descrizioni dei campi di log, consulta [VPC Flow Logs](#) nella Amazon VPC User Guide.

Correzione

Per creare un log di flusso VPC, consulta [Create a Flow Log](#) nella Amazon VPC User Guide. Dopo aver aperto la console Amazon VPC, scegli i tuoi VPC. Per Filtro, scegli Rifiuta o Tutto.

[EC2.7] La crittografia predefinita di EBS deve essere abilitata

Requisiti correlati: CIS AWS Foundations Benchmark v1.4.0/2.2.1, CIS Foundations Benchmark v3.0.0/2.2.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), nIST.800-53.r5 SC-28 (1) IST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6) AWS

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS :: Account

Regola AWS Config : [ec2-ebs-encryption-by-default](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la crittografia a livello di account è abilitata per impostazione predefinita per Amazon Elastic Block Store (Amazon EBS). Il controllo fallisce se la crittografia a livello di account non è abilitata.

Quando la crittografia è abilitata per il tuo account, i volumi Amazon EBS e le copie degli snapshot vengono crittografati quando sono inattivi. Ciò aggiunge un ulteriore livello di protezione per i tuoi dati. Per ulteriori informazioni, consultare la sezione [Crittografia per impostazione predefinita](#) nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Tieni presente che i seguenti tipi di istanza non supportano la crittografia: R1, C1 e M1.

Correzione

Per configurare la crittografia predefinita per i volumi Amazon EBS, consulta [Encryption by default](#) nella Amazon EC2 User Guide for Linux Instances.

[EC2.8] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 (IMDSv2)

Requisiti correlati: CIS AWS Foundations Benchmark v3.0.0/5.6, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoria: Proteggi > Sicurezza della rete

Gravità: alta

Tipo di risorsa: AWS::EC2::Instance

Regola AWS Config : [ec2-imdsv2-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la versione dei metadati dell'istanza EC2 è configurata con Instance Metadata Service versione 2 (IMDSv2). Il controllo passa se `HttpTokens` è impostato su obbligatorio per IMDSv2. Il controllo ha esito negativo se `HttpTokens` è impostato su `optional`.

I metadati dell'istanza vengono utilizzati per configurare o gestire l'istanza in esecuzione. L'IMDS fornisce l'accesso a credenziali temporanee, che vengono ruotate frequentemente. Queste credenziali eliminano la necessità di codificare o distribuire credenziali riservate alle istanze manualmente o programmaticamente. L'IMDS è collegato localmente a ogni istanza EC2. Funziona su uno speciale indirizzo IP «link local» 169.254.169.254. Questo indirizzo IP è accessibile solo dal software in esecuzione sull'istanza.

La versione 2 dell'IMDS aggiunge nuove protezioni per i seguenti tipi di vulnerabilità. Queste vulnerabilità potrebbero essere utilizzate per tentare di accedere all'IMDS.

- Apri i firewall delle applicazioni del sito Web
- Apri proxy inversi
- Vulnerabilità SSRF (Server-side Request Forgery)
- Firewall Open Layer 3 e NAT (Network Address Translation)

Security Hub consiglia di configurare le istanze EC2 con iMDSv2.

Correzione

Per configurare le istanze EC2 con IMDSv2, consulta [Percorso consigliato per richiedere IMDSv2 nella Amazon EC2 User Guide for Linux Instances](#).

[EC2.9] Le istanze Amazon EC2 non devono avere un indirizzo IPv4 pubblico

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete sicura > Indirizzi IP pubblici

Gravità: alta

Tipo di risorsa: AWS::EC2::Instance

Regola AWS Config : [ec2-instance-no-public-ip](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le istanze EC2 hanno un indirizzo IP pubblico. Il controllo fallisce se il `publicIp` campo è presente nell'elemento di configurazione dell'istanza EC2. Questo controllo si applica solo agli indirizzi IPv4.

Un indirizzo IPv4 pubblico è un indirizzo IP raggiungibile da Internet. Se avvii l'istanza con un indirizzo IP pubblico, l'istanza EC2 è raggiungibile da Internet. Un indirizzo IPv4 privato è un indirizzo IP non raggiungibile da Internet. Puoi utilizzare indirizzi IPv4 privati per la comunicazione tra istanze EC2 nello stesso VPC o nella tua rete privata connessa.

Gli indirizzi IPv6 sono unici a livello globale e quindi sono raggiungibili da Internet. Tuttavia, per impostazione predefinita, tutte le sottoreti hanno l'attributo di indirizzamento IPv6 impostato su `false`. Per ulteriori informazioni su IPv6, consulta la sezione [Indirizzamento IP nel tuo VPC nella Amazon VPC User Guide](#).

Se hai un caso d'uso legittimo per mantenere istanze EC2 con indirizzi IP pubblici, puoi eliminare i risultati di questo controllo. Per ulteriori informazioni sulle opzioni di architettura front-end, consulta l'Architecture [Blog o la serie This Is My AWS Architecture](#).

Correzione

Utilizza un VPC non predefinito in modo che all'istanza non venga assegnato un indirizzo IP pubblico per impostazione predefinita.

Quando avvii un'istanza EC2 in un VPC predefinito, a essa viene assegnato un indirizzo IP pubblico. Quando avvii un'istanza EC2 in un VPC non predefinito, la configurazione della sottorete determina se riceve un indirizzo IP pubblico. La sottorete dispone di un attributo per determinare se le nuove istanze EC2 nella sottorete ricevono un indirizzo IP pubblico dal pool di indirizzi IPv4 pubblico.

Non è possibile associare o dissociare manualmente un indirizzo IP pubblico assegnato automaticamente dalla propria istanza EC2. Per controllare se l'istanza EC2 riceve un indirizzo IP pubblico, esegui una delle seguenti operazioni:

- Modifica l'attributo di indirizzo IP pubblico della tua sottorete. Per ulteriori informazioni, consulta l'argomento sulla [modifica dell'attributo di assegnazione degli indirizzi IPv4 pubblici della sottorete](#) nella Guida per l'utente di Amazon VPC.
- Abilita o disabilita la funzionalità di indirizzamento IP pubblico durante l'avvio. Ciò sostituisce l'attributo di indirizzamento IP pubblico della sottorete. Per ulteriori informazioni, consulta [Assegnare un indirizzo IPv4 pubblico durante l'avvio dell'istanza](#) nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Per ulteriori informazioni, consulta [Indirizzi IPv4 pubblici e nomi host DNS esterni](#) nella Guida dell'utente di Amazon EC2 per le istanze Linux.

Se l'istanza EC2 è associata a un indirizzo IP elastico, l'istanza EC2 è raggiungibile da Internet. È possibile annullare l'associazione di un indirizzo IP elastico da un'istanza o un'interfaccia di rete in qualsiasi momento. Per dissociare un indirizzo IP elastico, consulta [Dissociare un indirizzo IP elastico](#) nella Amazon EC2 User Guide for Linux Instances.

[EC2.10] Amazon EC2 deve essere configurato per utilizzare endpoint VPC creati per il servizio Amazon EC2

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIT.800-53.r5 SC-7 (21), NIS.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4)

Categoria: Protezione > Configurazione di rete sicura > Accesso privato alle API

Gravità: media

Tipo di risorsa: AWS :: EC2 :: VPC

Regola AWS Config : [service-vpc-endpoint-enabled](#)

Tipo di pianificazione: periodica

Parametri:

- `serviceName: ec2` (non personalizzabile)

Questo controllo verifica se viene creato un endpoint di servizio per Amazon EC2 per ogni VPC. Il controllo fallisce se un VPC non dispone di un endpoint VPC creato per il servizio Amazon EC2.

Questo controllo valuta le risorse in un unico account. Non può descrivere risorse esterne all'account. Poiché AWS Config Security Hub non effettua controlli tra account, vedrai FAILED i risultati relativi ai VPC condivisi tra account. Security Hub consiglia di eliminare questi FAILED risultati.

Per migliorare il livello di sicurezza del tuo VPC, puoi configurare Amazon EC2 per utilizzare un endpoint VPC di interfaccia. Gli endpoint di interfaccia sono basati su una tecnologia che consente di accedere alle operazioni delle API di Amazon EC2 in modo privato. AWS PrivateLink Limita tutto

il traffico di rete tra il tuo VPC e Amazon EC2 alla rete Amazon. Poiché gli endpoint sono supportati solo all'interno della stessa regione, non è possibile creare un endpoint tra un VPC e un servizio in una regione diversa. In questo modo si evitano chiamate involontarie all'API Amazon EC2 verso altre regioni.

Per ulteriori informazioni sulla creazione di endpoint VPC per Amazon EC2, consulta [Amazon EC2 e interfaccia gli endpoint VPC nella Amazon EC2 User Guide for Linux Instances](#).

Correzione

Per creare un endpoint di interfaccia verso Amazon EC2 dalla console Amazon VPC, consulta [Creare un endpoint VPC](#) nella Guida.AWS PrivateLink. Per il nome del servizio, scegli `com.amazonaws.regione.ec2`.

Puoi anche creare e allegare una policy per gli endpoint al tuo endpoint VPC per controllare l'accesso all'API Amazon EC2. Per istruzioni sulla creazione di una policy per gli endpoint VPC, consulta [Create an endpoint policy](#) nella Amazon EC2 User Guide for Linux Instances.

[EC2.12] Gli EIP Amazon EC2 non utilizzati devono essere rimossi

Requisiti correlati: PCI DSS v3.2.1/2.4, NIST.800-53.r5 CM-8 (1)

Categoria: Protezione > Configurazione di rete protetta

Gravità: bassa

Tipo di risorsa: AWS::EC2::EIP

Regola AWS Config : [eip-attached](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se gli indirizzi IP elastici (EIP) allocati a un VPC sono collegati a istanze EC2 o interfacce di rete elastiche (ENI) in uso.

Un risultato non riuscito indica che potresti avere EIP EC2 inutilizzati.

Ciò ti aiuterà a mantenere un inventario accurato degli asset EIP nel tuo ambiente di dati dei titolari di carta (CDE).

Per rilasciare un EIP inutilizzato, consulta [Release an Elastic IP address](#) nella Amazon EC2 User Guide for Linux Instances.

[EC2.13] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o :/0 alla porta 22

Requisiti correlati: benchmark CIS AWS Foundations versione 1.2.0/4.1, PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/2.2.2, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), nIST.800-53.r5 CM-7, nIST.800-53.r5 SC-7, nIST. NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: AWS::EC2::SecurityGroup

Regola AWS Config : [restricted-ssh](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo di sicurezza Amazon EC2 consente l'ingresso da 0.0.0.0/0 o :/0 alla porta 22. Il controllo fallisce se il gruppo di sicurezza consente l'ingresso da 0.0.0.0/0 o :/0 alla porta 22.

I gruppi di sicurezza forniscono filtraggio stateful del traffico di rete in entrata e in uscita a risorse AWS . È opportuno che nessun gruppo di sicurezza consenta accesso di entratata illimitato alla porta 22. La rimozione di connettività senza alcuna restrizione a servizi della console remota, ad esempio SSH, riduce l'esposizione di un server ai rischi.

Correzione

Per vietare l'accesso alla porta 22, rimuovi la regola che consente tale accesso per ogni gruppo di sicurezza associato a un VPC. Per istruzioni, consulta [Aggiornare le regole dei gruppi di sicurezza](#) nella Guida per l'utente di Amazon EC2 per le istanze Linux. Dopo aver selezionato un gruppo di sicurezza nella console Amazon EC2, scegli Azioni, Modifica regole in entrata. Rimuovi la regola che consente l'accesso alla porta 22.

[EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389

Requisiti correlati AWS : CIS Foundations Benchmark v1.2.0/4.2

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: AWS::EC2::SecurityGroup

AWS Config regola: [restricted-common-ports](#) (la regola creata è restricted-rdp)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo di sicurezza Amazon EC2 consente l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389. Il controllo fallisce se il gruppo di sicurezza consente l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389.

I gruppi di sicurezza forniscono filtraggio stateful del traffico di rete in entrata e in uscita a risorse AWS. È opportuno che nessun gruppo di sicurezza consenta accesso di entrata illimitato alla porta 3389. La rimozione di connettività senza alcuna restrizione a servizi della console remota, ad esempio RDP, riduce l'esposizione di un server ai rischi.

Correzione

Per vietare l'accesso alla porta 3389, rimuovi la regola che consente tale accesso per ogni gruppo di sicurezza associato a un VPC. Per istruzioni, consulta [Aggiornare le regole dei gruppi di sicurezza](#) nella Amazon VPC User Guide. Dopo aver selezionato un gruppo di sicurezza nella console Amazon VPC, scegli Azioni, Modifica regole in entrata. Rimuovi la regola che consente l'accesso alla porta 3389.

[EC2.15] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Proteggi > Sicurezza della rete

Gravità: media

Tipo di risorsa: AWS::EC2::Subnet

Regola AWS Config : [subnet-auto-assign-public-ip-disabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'assegnazione degli IP pubblici nelle MapPublicIpOnLaunch sottoreti Amazon Virtual Private Cloud (Amazon VPC) è impostata su. FALSE Il controllo passa se il flag è impostato su. FALSE

Tutte le sottoreti hanno un attributo che determina se un'interfaccia di rete creata nella sottorete riceve automaticamente un indirizzo IPv4 pubblico. Le istanze avviate in sottoreti con questo attributo abilitato hanno un indirizzo IP pubblico assegnato alla loro interfaccia di rete principale.

Correzione

Per configurare una sottorete in modo che non assegni indirizzi IP pubblici, consulta [Modificare l'attributo di indirizzamento IPv4 pubblico per la sottorete nella Amazon VPC User Guide](#).

Deseleziona la casella di controllo Abilita l'assegnazione automatica dell'indirizzo IPv4 pubblico.

[EC2.16] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse

Requisiti correlati: NIST.800-53.r5 CM-8 (1)

Categoria: Prevenire > Sicurezza della rete

Gravità: bassa

Tipo di risorsa: AWS::EC2::NetworkACL

Regola AWS Config : [vpc-network-acl-unused-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se sono presenti elenchi di controllo degli accessi alla rete (ACL) non utilizzati.

Il controllo verifica la configurazione degli elementi della risorsa `AWS::EC2::NetworkACL` e determina le relazioni dell'ACL di rete.

Se l'unica relazione è il VPC dell'ACL di rete, il controllo fallisce.

Se sono elencate altre relazioni, il controllo passa.

Correzione

Per istruzioni sull'eliminazione di un ACL di rete non utilizzato, consulta [Eliminazione di un ACL di rete nella Amazon VPC](#) User Guide. Non puoi eliminare l'ACL di rete predefinito o un ACL associato alle sottoreti.

[EC2.17] Le istanze Amazon EC2 non devono utilizzare più ENI

Requisiti correlati: NIST.800-53.r5 AC-4 (21)

Categoria: Sicurezza di rete

Gravità: bassa

Tipo di risorsa: `AWS::EC2::Instance`

Regola AWS Config : [ec2-instance-multiple-eni-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `Adapterids`— Un elenco di ID di interfaccia di rete collegati alle istanze EC2 (non personalizzabili)

Questo controllo verifica se un'istanza EC2 utilizza più Elastic Network Interface (ENI) o Elastic Fabric Adapter (EFA). Questo controllo passa se viene utilizzata una singola scheda di rete. Il controllo include un elenco di parametri opzionale per identificare gli ENI consentiti. Questo controllo fallisce anche se un'istanza EC2 appartenente a un cluster Amazon EKS utilizza più di un ENI. Se

le tue istanze EC2 devono avere più ENI come parte di un cluster Amazon EKS, puoi eliminare tali risultati di controllo.

Più ENI possono causare istanze dual-homed, ossia istanze con più sottoreti. Ciò può aumentare la complessità della sicurezza della rete e introdurre percorsi e accessi di rete indesiderati.

Correzione

Per scollegare un'interfaccia di rete da un'istanza EC2, consulta [Scollegare un'interfaccia di rete da un'istanza](#) nella Amazon EC2 User Guide for Linux Instances.

[EC2.18] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate

Requisiti correlati: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53,5 SC-7 (5)

Categoria: Protezione > Configurazione di rete sicura > Configurazione del gruppo di sicurezza

Gravità: alta

Tipo di risorsa: AWS::EC2::SecurityGroup

Regola AWS Config : [vpc-sg-open-only-to-authorized-ports](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>authorizeTcpPorts</code>	Elenco delle porte TCP autorizzate	IntegerList (massimo 32 articoli)	1 Da a 65535	[80, 443]
<code>authorizeUdpPorts</code>	Elenco delle porte UDP autorizzate	IntegerList (massimo 32 articoli)	1 Da a 65535	Nessun valore predefinito

Questo controllo verifica se un gruppo di sicurezza Amazon EC2 consente il traffico in entrata senza restrizioni da porte non autorizzate. Lo stato del controllo è determinato come segue:

- Se si utilizza il valore predefinito `perauthorizedTcpPorts`, il controllo ha esito negativo se il gruppo di sicurezza consente il traffico in entrata senza restrizioni da qualsiasi porta diversa dalle porte 80 e 443.
- Se fornisci valori personalizzati per `authorizedTcpPorts` o `authorizedUdpPorts`, il controllo ha esito negativo se il gruppo di sicurezza consente il traffico in entrata senza restrizioni da qualsiasi porta non elencata.
- Se non viene utilizzato alcun parametro, il controllo ha esito negativo per qualsiasi gruppo di sicurezza con una regola del traffico in entrata senza restrizioni.

I gruppi di sicurezza forniscono un filtraggio statico del traffico di rete in ingresso e in uscita verso. AWS Le regole dei gruppi di sicurezza devono seguire il principio dell'accesso con privilegi minimi. L'accesso illimitato (indirizzo IP con suffisso `/0`) aumenta la possibilità di attività dannose come pirateria informatica, denial-of-service attacchi e perdita di dati. A meno che una porta non sia espressamente consentita, la porta dovrebbe negare l'accesso illimitato.

Correzione

Per modificare un gruppo di sicurezza, consulta [Work with security groups](#) nella Amazon VPC User Guide.

[EC2.19] I gruppi di sicurezza non devono consentire l'accesso illimitato alle porte ad alto rischio

Requisiti correlati: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7, NIST.800-53.r5 R5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (21), NIS.800-53.R5 SC-7 (4), NIS.800-53.r5 SC-7 (5)

Categoria: Protezione > Accesso limitato alla rete

Severità: critica

Tipo di risorsa: AWS::EC2::SecurityGroup

AWS Config regola: [restricted-common-ports](#) (la regola creata è `vpc-sg-restricted-common-ports`)

Tipo di pianificazione: modifica attivata

Parametri: "blockedPorts":

"20, 21, 22, 23, 25, 110, 135, 143, 445, 1433, 1434, 3000, 3306, 3389, 4333, 5000, 5432, 5500, 5601"
(non personalizzabile)

Questo controllo verifica se il traffico in entrata senza restrizioni per un gruppo di sicurezza Amazon EC2 è accessibile alle porte specificate considerate ad alto rischio. Questo controllo ha esito negativo se una delle regole di un gruppo di sicurezza consente il traffico in ingresso da '0.0.0.0/0' o ':/0' verso tali porte.

I gruppi di sicurezza forniscono filtraggio stateful del traffico di rete in entrata e in uscita a risorse AWS. L'accesso senza restrizioni (0.0.0.0/0) aumenta le opportunità di attività dannose, come pirateria informatica, attacchi e perdita di dati. Nessun gruppo di sicurezza dovrebbe consentire l'accesso illimitato in ingresso alle seguenti porte:

- 20, 21 (FTP)
- 22 (SSH)
- 23 (Telnet)
- 25 (SMTP)
- 110 (POP3)
- 135 (RPC)
- 143 (IMAP)
- 445 (CIF)
- 1433, 1434 (SQL)
- 3000 (framework di sviluppo web Go, Node.js e Ruby)
- 3306 (MySQL)
- 3389 (RDP)
- 4333 (ahsp)
- 5000 (framework di sviluppo web in Python)
- 5432 (postgresql)
- 5500 (1) fcp-addr-srvr
- 5601 (Cruscoti) OpenSearch
- 8080 (proxy)

- 8088 (porta HTTP precedente)
- 8888 (porta HTTP alternativa)
- 9200 o 9300 () OpenSearch

Correzione

Per eliminare le regole da un gruppo di sicurezza, consulta [Eliminare le regole da un gruppo di sicurezza](#) nella Guida per l'utente di Amazon EC2 per le istanze Linux.

[EC2.20] Entrambi i tunnel VPN per una connessione VPN da sito a sito devono essere AWS attivi

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Resilienza > Recupero > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::EC2::VPNConnection

Regola AWS Config : [vpc-vpn-2-tunnels-up](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Un tunnel VPN è un collegamento crittografato in cui i dati possono passare dalla rete del cliente a o dall' AWS interno di una AWS connessione VPN Site-to-Site. Ogni connessione VPN include due tunnel VPN che è possibile utilizzare contemporaneamente per una disponibilità elevata. Garantire che entrambi i tunnel VPN siano attivi per una connessione VPN è importante per confermare una connessione sicura e ad alta disponibilità tra un AWS VPC e la rete remota.

Questo controllo verifica che entrambi i tunnel VPN forniti dalla VPN AWS Site-to-Site siano nello stato UP. Il controllo fallisce se uno o entrambi i tunnel sono nello stato INATTIVO.

Correzione

Per modificare le opzioni del tunnel VPN, consulta [Modificare le opzioni del tunnel VPN da sito a sito nella Guida per l' AWS utente VPN da sito a sito](#) a sito.

[EC2.21] Gli ACL di rete non dovrebbero consentire l'ingresso dalla porta 0.0.0.0/0 alla porta 22 o alla porta 3389

Requisiti correlati: CIS AWS Foundations Benchmark v1.4.0/5.1, CIS AWS Foundations Benchmark v3.0.0/5.1, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-7, NIST.800-53.r5 CM-7, NIST.800-53.r5 3.5r SC-7, NIT 800-53.r5 SC-7 (21), NIT 800-53.5 SC-7 (5)

Categoria: Protezione > Configurazione di rete sicura

Gravità: media

Tipo di risorsa: AWS::EC2::NetworkACL

Regola AWS Config : [nacl-no-unrestricted-ssh-rdp](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una lista di controllo degli accessi alla rete (NACL) consente l'accesso illimitato alle porte TCP predefinite per il traffico in ingresso SSH/RDP. La regola fallisce se una voce NACL in entrata consente un blocco CIDR di origine di '0.0.0.0/0' o ':/0' per le porte TCP 22 o 3389.

L'accesso alle porte di amministrazione del server remoto, come la porta 22 (SSH) e la porta 3389 (RDP), non dovrebbe essere accessibile al pubblico, in quanto ciò potrebbe consentire l'accesso non intenzionale alle risorse all'interno del tuo VPC.

Correzione

Per ulteriori informazioni sui NAC, consulta gli ACL di [rete nella Guida](#) per l'utente VPC.

[EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi

Important

RITIRATO DA STANDARD SPECIFICI — Security Hub ha rimosso questo controllo il 20 settembre 2023 dallo standard AWS Foundational Security Best Practices e dal NIST SP 800-53 Rev. 5. Questo controllo fa ancora parte di Service-Managed Standard: AWS Control Tower. Questo controllo produce un risultato positivo se i gruppi di sicurezza sono collegati a istanze EC2 o a un'interfaccia di rete elastica. Tuttavia, in alcuni casi d'uso, i gruppi di

sicurezza non collegati non rappresentano un rischio per la sicurezza. Puoi utilizzare altri controlli EC2, come EC2.2, EC2.13, EC2.14, EC2.18 ed EC2.19, per monitorare i tuoi gruppi di sicurezza.

Categoria: Identificazione > Inventario

Gravità: media

Tipo di risorsa: AWS::EC2::NetworkInterface AWS::EC2::SecurityGroup

Regola AWS Config : [ec2-security-group-attached-to-eni-periodic](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo AWS controllo verifica che i gruppi di sicurezza siano collegati alle istanze Amazon Elastic Compute Cloud (Amazon EC2) o a un'interfaccia di rete elastica. Il controllo avrà esito negativo se il gruppo di sicurezza non è associato a un'istanza Amazon EC2 o a un'interfaccia di rete elastica.

Correzione

Per creare, assegnare ed eliminare gruppi di sicurezza, consulta la guida per l'utente [dei gruppi di sicurezza](#) in Amazon EC2.

[EC2.23] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC

Requisiti correlati: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: AWS::EC2::TransitGateway

Regola AWS Config : [ec2-transit-gateway-auto-vpc-attach-disabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i gateway di transito EC2 accettano automaticamente allegati VPC condivisi. Questo controllo non riesce per un gateway di transito che accetta automaticamente richieste di allegati VPC condivise.

L'attivazione `AutoAcceptSharedAttachments` configura un gateway di transito per accettare automaticamente qualsiasi richiesta di allegati VPC tra account senza verificare la richiesta o l'account da cui proviene l'allegato. Per seguire le migliori pratiche di autorizzazione e autenticazione, consigliamo di disattivare questa funzionalità per garantire che vengano accettate solo le richieste di allegati VPC autorizzate.

Correzione

Per modificare un gateway di transito, consulta [Modificare un gateway di transito](#) nella Amazon VPC Developer Guide.

[EC2.24] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati

Requisiti correlati: NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: media

Tipo di risorsa: AWS::EC2::Instance

Regola AWS Config : [ec2-paravirtual-instance-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il tipo di virtualizzazione di un'istanza EC2 è paravirtuale. Il controllo fallisce se l'istanza EC2 è `virtualizationType` impostata su `paravirtual`

Le Amazon Machine Images (AMI) Linux utilizzano uno dei due tipi di virtualizzazione: `paravirtual` (PV) o `hardware virtual machine` (HVM). Le principali differenze tra le AMI PV e HVM risiedono nel modo in cui vengono avviate e nella loro capacità di sfruttare i vantaggi delle estensioni hardware speciali (CPU, rete e archiviazione) per l'ottimizzazione delle prestazioni.

Storicamente parlando, i sistemi guest PV sono caratterizzati da prestazioni migliori rispetto ai sistemi guest HVM in molti casi, ma in seguito ai miglioramenti apportati alla virtualizzazione HVM e alla disponibilità di driver PV per AMI HVM, ciò non è più vero. Per ulteriori informazioni, consulta i [tipi di virtualizzazione delle AMI Linux](#) nella Guida per l'utente di Amazon EC2 per le istanze Linux.

Correzione

Per aggiornare un'istanza EC2 a un nuovo tipo di istanza, consulta [Modifica del tipo di istanza](#) nella Amazon EC2 User Guide for Linux Instances.

[EC2.25] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: alta

Tipo di risorsa: AWS::EC2::LaunchTemplate

Regola AWS Config : [ec2-launch-template-public-ip-disabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i modelli di lancio di Amazon EC2 sono configurati per assegnare indirizzi IP pubblici alle interfacce di rete al momento dell'avvio. Il controllo fallisce se un modello di avvio EC2 è configurato per assegnare un indirizzo IP pubblico alle interfacce di rete o se esiste almeno un'interfaccia di rete con un indirizzo IP pubblico.

Un indirizzo IP pubblico è raggiungibile da Internet. Se configuri le interfacce di rete con un indirizzo IP pubblico, le risorse associate a tali interfacce di rete potrebbero essere raggiungibili da Internet. Le risorse EC2 non dovrebbero essere accessibili al pubblico perché ciò potrebbe consentire l'accesso involontario ai tuoi carichi di lavoro.

Correzione

Per aggiornare un modello di lancio EC2, consulta [Modifica delle impostazioni dell'interfaccia di rete predefinita nella Guida](#) per l'utente di Amazon EC2 Auto Scaling.

[EC2.28] I volumi EBS devono essere coperti da un piano di backup

Categoria: Recover > Resilience > Backup abilitati

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST .800-53,5 SI-13 (5)

Gravità: bassa

Tipo di risorsa: AWS::EC2::Volume

AWS Config regola: [ebs-resources-protected-by-backup-plan](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
backupVaultLockCheck	Il controllo restituisce un PASSED risultato se il parametro è impostato su true e la risorsa utilizza AWS Backup Vault Lock.	Booleano	true o false	Nessun valore predefinito

Questo controllo valuta se un volume Amazon EBS in in-use stato è coperto da un piano di backup. Il controllo fallisce se un volume EBS non è coperto da un piano di backup. Se si imposta il backupVaultLockCheck parametro uguale a true, il controllo passa solo se viene eseguito il backup del volume EBS in un vault AWS Backup bloccato.

I backup consentono di ripristinare più rapidamente un incidente di sicurezza. Inoltre, rafforzano la resilienza dei sistemi. L'inclusione dei volumi Amazon EBS in un piano di backup aiuta a proteggere i dati da perdite o eliminazioni involontarie.

Correzione

Per aggiungere un volume Amazon EBS a un piano di AWS Backup backup, consulta [Assegnazione di risorse a un piano di backup](#) nella AWS Backup Developer Guide.

[EC2.33] Gli allegati del gateway di transito EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EC2::TransitGatewayAttachment`

AWS Config regola: `tagged-ec2-transitgatewayattachment` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un allegato del gateway di transito Amazon EC2 ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo ha esito negativo se l'allegato Transit Gateway non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se l'allegato del gateway di transito non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli

accessi basati sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un allegato del gateway di transito EC2, consulta [Etichettare le risorse Amazon EC2](#) nella Amazon EC2 User Guide for Linux Instances.

[EC2.34] Le tabelle delle rotte dei gateway di transito EC2 devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::TransitGatewayRouteTable

AWS Config regola: tagged-ec2-transitgatewayroutetable (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfano	Nessun valore predefinito

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se una tabella di routing del gateway di transito Amazon EC2 contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo ha esito negativo se la tabella delle rotte del gateway di transito non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la tabella di route del gateway di transito non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una tabella di routing del gateway di transito EC2, consulta [Etichettare le risorse Amazon EC2](#) nella Amazon EC2 User Guide for Linux Instances.

[EC2.35] Le interfacce di rete EC2 devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::NetworkInterface

AWS Config regola: tagged-ec2-networkinterface (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un'interfaccia di rete Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'interfaccia di rete non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'interfaccia di rete non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'interfaccia di rete EC2, consulta Etichettare [le risorse Amazon EC2 nella Amazon EC2](#) User Guide for Linux Instances.

[EC2.36] I gateway per i clienti EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::CustomerGateway

AWS Config regola: tagged-ec2-customergateway (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un gateway per clienti Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il gateway del cliente non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gateway del cliente non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gateway per clienti EC2, consulta Etichettare [le risorse Amazon EC2 nella Amazon EC2 User Guide for Linux Instances](#).

[EC2.37] Gli indirizzi IP elastici EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::EIP

AWS Config regola: tagged-ec2-eip (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un indirizzo IP elastico di Amazon EC2 ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'indirizzo IP elastico non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'indirizzo IP elastico non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un indirizzo IP elastico EC2, consulta Etichettare le risorse [Amazon EC2 nella Amazon EC2 User Guide for Linux Instances](#).

[EC2.38] Le istanze EC2 devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::Instance

AWS Config regola: tagged-ec2-instance (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un'istanza Amazon EC2 ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se l'istanza non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'istanza non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing. Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in Riferimenti generali di AWS.

Correzione

Per aggiungere tag a un'istanza EC2, consulta Etichettare [le risorse Amazon EC2 nella Amazon EC2 User Guide for Linux Instances](#).

[EC2.39] I gateway Internet EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::InternetGateway

AWS Config regola: tagged-ec2-internetgateway (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un gateway Internet Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gateway Internet non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se il gateway Internet non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gateway Internet EC2, consulta Etichettare [le risorse Amazon EC2 nella Amazon EC2](#) User Guide for Linux Instances.

[EC2.40] I gateway NAT EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::NatGateway

AWS Config regola: tagged-ec2-natgateway (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un gateway NAT (Network Address Translation) di Amazon EC2 ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gateway NAT non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gateway NAT non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gateway NAT EC2, consulta Etichettare [le risorse Amazon EC2 nella Amazon EC2 User Guide for Linux Instances](#).

[EC2.41] Gli ACL di rete EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::NetworkACL

AWS Config regola: tagged-ec2-networkacl (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se una lista di controllo degli accessi alla rete di Amazon EC2 (Network ACL) contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'ACL di rete non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'ACL di rete non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un ACL di rete EC2, consulta Etichettare [le risorse Amazon EC2 nella Amazon EC2 User Guide for Linux Instances](#).

[EC2.42] Le tabelle di routing EC2 devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::RouteTable

AWS Config regola: tagged-ec2-routetable (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se una tabella di routing di Amazon EC2 contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la tabella di routing non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la tabella delle rotte non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una tabella di routing EC2, consulta [Etichettare le risorse Amazon EC2 nella Amazon EC2 User Guide for Linux Instances](#).

[EC2.43] I gruppi di sicurezza EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::SecurityGroup

AWS Config regola: tagged-ec2-securitygroup (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un gruppo di sicurezza Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gruppo di sicurezza non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di sicurezza non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gruppo di sicurezza EC2, consulta Etichettare [le risorse Amazon EC2 nella Amazon EC2](#) User Guide for Linux Instances.

[EC2.44] Le sottoreti EC2 devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::Subnet

AWS Config regola: tagged-ec2-subnet (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se una sottorete Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la sottorete non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la sottorete non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una sottorete EC2, consulta Etichettare [le risorse Amazon EC2 nella Amazon EC2 User Guide for Linux Instances](#).

[EC2.45] I volumi EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::Subnet

AWS Config regola: tagged-ec2-subnet (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un volume Amazon EC2 ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il volume non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il volume non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un volume EC2, consulta Etichettare [le risorse Amazon EC2 nella Amazon EC2 User Guide for Linux Instances](#).

[EC2.46] I VPC Amazon devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS :: EC2 :: VPC

AWS Config regola: tagged-ec2-vpc (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un Amazon Virtual Private Cloud (Amazon VPC) ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se Amazon VPC non dispone di chiavi di tag o se non dispone di tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se Amazon VPC non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing. Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in Riferimenti generali di AWS.

Correzione

Per aggiungere tag a un VPC, consulta Etichettare [le risorse Amazon EC2 nella Amazon EC2 User Guide for Linux Instances](#).

[EC2.47] I servizi endpoint Amazon VPC devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::VPCEndpointService

AWS Config regola: tagged-ec2-vpcendpointservice (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un servizio endpoint Amazon VPC dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il servizio endpoint non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il servizio endpoint non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un servizio endpoint Amazon VPC, consulta [Manage Tags](#) nella sezione [Configura un servizio endpoint](#) della Guida.AWS PrivateLink

[EC2.48] I log di flusso di Amazon VPC devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::FlowLog

AWS Config regola: tagged-ec2-flowlog (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un log di flusso Amazon VPC contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il log di flusso non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il log di flusso non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un log di flusso di Amazon VPC, consulta Etichettare [un log di flusso](#) nella Amazon VPC User Guide.

[EC2.49] Le connessioni peering Amazon VPC devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::VPCPeeringConnection

AWS Config regola: tagged-ec2-vpcpeeringconnection (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se una connessione peering Amazon VPC ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la connessione peering non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la connessione peering non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari,

ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una connessione peering Amazon VPC, consulta [Tagga le tue risorse Amazon EC2 nella Amazon EC2](#) User Guide for Linux Instances.

[EC2.50] I gateway VPN EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::VPNGateway

AWS Config regola: tagged-ec2-vpngateway (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un gateway VPN Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il gateway VPN non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se il gateway VPN non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gateway VPN EC2, consulta Etichettare [le risorse Amazon EC2 nella Amazon EC2 User Guide for Linux Instances](#).

[EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata

Requisiti correlati: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: bassa

Tipo di risorsa: AWS::EC2::ClientVpnEndpoint

AWS Config regola: [ec2-client-vpn-connection-log-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS Client VPN endpoint ha abilitato la registrazione delle connessioni client. Il controllo fallisce se sull'endpoint non è abilitata la registrazione delle connessioni client.

Gli endpoint Client VPN consentono ai client remoti di connettersi in modo sicuro alle risorse in un Virtual Private Cloud (VPC) in AWS. I log di connessione consentono di tracciare l'attività degli utenti sull'endpoint VPN e forniscono visibilità. Quando attivi la registrazione delle connessioni, puoi specificare il nome di un flusso di log nel gruppo di log. Se non specifichi un flusso di log, il servizio Client VPN ne crea uno per te.

Correzione

Per abilitare la registrazione delle connessioni, consulta [Abilitare la registrazione della connessione per un endpoint Client VPN esistente](#) nella Guida per l'AWS Client VPN amministratore.

[EC2.52] I gateway di transito EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EC2::TransitGateway

AWS Config regola: tagged-ec2-transitgateway (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un gateway di transito Amazon EC2 dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il gateway di transito non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gateway di transito non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una

singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui, AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gateway di transito EC2, consulta [Etichettare le risorse Amazon EC2 nella Amazon EC2 User Guide for Linux Instances](#).

[EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da 0.0.0.0/0 alle porte di amministrazione remota del server

Requisiti correlati: AWS CIS Foundations Benchmark v3.0.0/5.2

Categoria: Protezione > Configurazione di rete sicura > Configurazione del gruppo di sicurezza

Gravità: alta

Tipo di risorsa: AWS::EC2::SecurityGroup

Regola AWS Config : [vpc-sg-port-restriction-check](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
ipType	La versione IP	Stringa	Non personalizzabile	IPv4

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
restrictPorts	Elenco di porte che dovrebbero rifiutare il traffico in ingresso	IntegerList	Non personalizzabile	22, 3389

Questo controllo verifica se un gruppo di sicurezza Amazon EC2 consente l'ingresso da 0.0.0.0/0 alle porte di amministrazione remota del server (porte 22 e 3389). Il controllo fallisce se il gruppo di sicurezza consente l'ingresso da 0.0.0.0/0 alla porta 22 o 3389.

I gruppi di sicurezza forniscono un filtraggio statico del traffico di rete in ingresso e in uscita verso le risorse. AWS È consigliabile che nessun gruppo di sicurezza consenta l'accesso illimitato in ingresso alle porte di amministrazione remota del server, come SSH alla porta 22 e RDP alla porta 3389, utilizzando i protocolli TDP (6), UDP (17) o ALL (-1). Consentire l'accesso pubblico a queste porte aumenta la superficie di attacco delle risorse e il rischio di compromissione delle risorse.

Correzione

Per aggiornare una regola del gruppo di sicurezza EC2 per vietare il traffico in ingresso verso le porte specificate, consulta [Update security group rules](#) nella Amazon EC2 User Guide for Linux Instances. Dopo aver selezionato un gruppo di sicurezza nella console Amazon EC2, scegli Azioni, Modifica regole in entrata. Rimuovi la regola che consente l'accesso alla porta 22 o alla porta 3389.

[EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server

Requisiti correlati: CIS Foundations Benchmark v3.0.0/5.3 AWS

Categoria: Protezione > Configurazione di rete sicura > Configurazione del gruppo di sicurezza

Gravità: alta

Tipo di risorsa: AWS::EC2::SecurityGroup

Regola AWS Config : [vpc-sg-port-restriction-check](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
ipType	La versione IP	Stringa	Non personalizzabile	IPv6
restrictPorts	Elenco di porte che dovrebbero rifiutare il traffico in ingresso	IntegerList	Non personalizzabile	22, 3389

Questo controllo verifica se un gruppo di sicurezza Amazon EC2 consente l'accesso da: :/0 alle porte di amministrazione del server remoto (porte 22 e 3389). Il controllo fallisce se il gruppo di sicurezza consente l'ingresso da: :/0 alla porta 22 o 3389.

I gruppi di sicurezza forniscono un filtraggio statico del traffico di rete in ingresso e in uscita verso le risorse. AWS È consigliabile che nessun gruppo di sicurezza consenta l'accesso illimitato in ingresso alle porte di amministrazione remota del server, come SSH alla porta 22 e RDP alla porta 3389, utilizzando i protocolli TDP (6), UDP (17) o ALL (-1). Consentire l'accesso pubblico a queste porte aumenta la superficie di attacco delle risorse e il rischio di compromissione delle risorse.

Correzione

Per aggiornare una regola del gruppo di sicurezza EC2 per vietare il traffico in ingresso verso le porte specificate, consulta [Update security group rules](#) nella Amazon EC2 User Guide for Linux Instances. Dopo aver selezionato un gruppo di sicurezza nella console Amazon EC2, scegli Azioni, Modifica regole in entrata. Rimuovi la regola che consente l'accesso alla porta 22 o alla porta 3389.

Controlli di Amazon EC2 Auto Scaling

Questi controlli sono correlati alle risorse di Amazon EC2 Auto Scaling.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[AutoScaling.1] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB

Requisiti correlati: PCI DSS v3.2.1/2.2, NIST.800-53.r5 CA-7, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 SI-2

Categoria: Identificazione > Inventario

Gravità: bassa

Tipo di risorsa: AWS::AutoScaling::AutoScalingGroup

Regola AWS Config : [autoscaling-group-elb-healthcheck-required](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo Amazon EC2 Auto Scaling associato a un sistema di bilanciamento del carico utilizza i controlli di integrità Elastic Load Balancing (ELB). Il controllo fallisce se il gruppo Auto Scaling non utilizza i controlli di integrità ELB.

I controlli di integrità ELB aiutano a garantire che un gruppo di Auto Scaling possa determinare lo stato di un'istanza sulla base di test aggiuntivi forniti dal sistema di bilanciamento del carico. L'utilizzo dei controlli di integrità di Elastic Load Balancing aiuta anche a supportare la disponibilità delle applicazioni che utilizzano i gruppi di Auto Scaling EC2.

Correzione

Per aggiungere i controlli di integrità di Elastic Load Balancing, consulta [Add Elastic Load Balancing health](#) check nella Amazon EC2 Auto Scaling User Guide.

[AutoScaling.2] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::AutoScaling::AutoScalingGroup

Regola AWS Config : [autoscaling-multiple-az](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personali zzati consentiti	Valore predefinito di Security Hub
minAvailabilityZones	Numero minimo di zone di disponibilità	Enum	2, 3, 4, 5, 6	2

Questo controllo verifica se un gruppo Amazon EC2 Auto Scaling copre almeno il numero specificato di zone di disponibilità (AZ). Il controllo fallisce se un gruppo di Auto Scaling non copre almeno il numero specificato di AZ. A meno che non si fornisca un valore di parametro personalizzato per il numero minimo di AZ, Security Hub utilizza un valore predefinito di due AZ.

Un gruppo di Auto Scaling che non si estende su più AZ non può avviare istanze in un'altra AZ per compensare se la singola AZ configurata non è più disponibile. Tuttavia, un gruppo di Auto Scaling con una singola zona di disponibilità può essere preferito in alcuni casi d'uso, come i lavori in batch o quando i costi di trasferimento tra le AZ devono essere ridotti al minimo. In questi casi, è possibile disabilitare questo controllo o eliminarne i risultati.

Correzione

Per aggiungere AZ a un gruppo Auto Scaling esistente, [consulta Aggiungere e rimuovere zone di disponibilità](#) nella Guida per l'utente di Amazon EC2 Auto Scaling.

[AutoScaling.3] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 (IMDSv2)

Requisiti correlati: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: AWS::AutoScaling::LaunchConfiguration

Regola AWS Config : [autoscaling-launchconfig-requires-imdsv2](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se IMDSv2 è abilitato su tutte le istanze lanciate dai gruppi Amazon EC2 Auto Scaling. Il controllo fallisce se la versione di Instance Metadata Service (IMDS) non è inclusa nella configurazione di avvio o se sono abilitati sia IMDSv1 che IMDSv2.

IMDS fornisce dati sull'istanza che è possibile utilizzare per configurare o gestire l'istanza in esecuzione.

La versione 2 dell'IMDS aggiunge nuove protezioni che non erano disponibili in IMDSv1 per proteggere ulteriormente le istanze EC2.

Correzione

Un gruppo Auto Scaling è associato a una configurazione di avvio alla volta. Non è possibile modificare una configurazione di avvio dopo averla creata. Per modificare la configurazione di avvio per un gruppo Auto Scaling, usa una configurazione di avvio esistente come base per una nuova configurazione di avvio con iMDSv2 abilitato. Per ulteriori informazioni, consulta [Configurare le opzioni dei metadati delle istanze per le nuove istanze](#) nella Guida per l'utente di Amazon EC2 per le istanze Linux.

[AutoScaling.4] La configurazione di avvio del gruppo Auto Scaling non deve avere un limite di hop di risposta ai metadati superiore a 1

Important

Security Hub ha ritirato questo controllo nell'aprile 2024. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: `AWS::AutoScaling::LaunchConfiguration`

Regola AWS Config : [autoscaling-launch-config-hop-limit](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica il numero di hop di rete che un token di metadati può percorrere. Il controllo ha esito negativo se il limite dell'hop di risposta ai metadati è maggiore di 1.

L'Instance Metadata Service (IMDS) fornisce informazioni sui metadati su un'istanza Amazon EC2 ed è utile per la configurazione delle applicazioni. La limitazione della PUT risposta HTTP per il servizio di metadati alla sola istanza EC2 protegge l'IMDS dall'uso non autorizzato.

Il campo Time To Live (TTL) nel pacchetto IP viene ridotto di uno per ogni hop. Questa riduzione può essere utilizzata per garantire che il pacchetto non viaggi al di fuori di EC2. IMDSv2 protegge le istanze EC2 che potrebbero essere state configurate erroneamente come router aperti, firewall di livello 3, VPN, tunnel o dispositivi NAT, impedendo così agli utenti non autorizzati di recuperare i metadati. Con IMDSv2, la PUT risposta che contiene il token segreto non può uscire dall'istanza perché il limite di hop di risposta ai metadati predefinito è impostato su 1. Tuttavia, se questo valore è maggiore di 1, il token può lasciare l'istanza EC2.

Correzione

Per modificare il limite dell'hop di risposta ai metadati per una configurazione di avvio esistente, consulta [Modificare le opzioni dei metadati delle istanze per le istanze esistenti](#) nella Amazon EC2 User Guide for Linux Instances.

[Autoscaling.5] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: `AWS::AutoScaling::LaunchConfiguration`

Regola AWS Config : [autoscaling-launch-config-public-ip-disabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la configurazione di avvio associata a un gruppo di Auto Scaling assegna un [indirizzo IP pubblico](#) alle istanze del gruppo. Il controllo fallisce se la configurazione di avvio associata assegna un indirizzo IP pubblico.

Le istanze Amazon EC2 in una configurazione di avvio del gruppo Auto Scaling non devono avere un indirizzo IP pubblico associato, tranne in casi limite limitati. Le istanze Amazon EC2 dovrebbero essere accessibili solo da un sistema di bilanciamento del carico anziché essere esposte direttamente a Internet.

Correzione

Un gruppo Auto Scaling è associato a una configurazione di avvio alla volta. Non è possibile modificare una configurazione di avvio dopo averla creata. Per modificare la configurazione di avvio per un gruppo con scalabilità automatica, utilizza una configurazione di avvio esistente come base per una nuova configurazione. Quindi, aggiorna il gruppo Auto Scaling affinché utilizzi la nuova configurazione di avvio. Per step-by-step istruzioni, consulta [Modifica della configurazione di avvio per un gruppo Auto Scaling](#) nella Guida per l'utente di Amazon EC2 Auto Scaling. Quando crei la nuova configurazione di avvio, in Configurazione aggiuntiva, per Dettagli avanzati, Tipo di indirizzo IP, scegli Non assegnare un indirizzo IP pubblico a nessuna istanza.

Dopo aver modificato la configurazione di avvio, Auto Scaling avvia nuove istanze con le nuove opzioni di configurazione. Le istanze esistenti non sono interessate. Per aggiornare un'istanza esistente, ti consigliamo di aggiornare l'istanza o di consentire il ridimensionamento automatico per sostituire gradualmente le istanze più vecchie con quelle più recenti in base alle tue politiche di terminazione. Per ulteriori informazioni sull'aggiornamento delle istanze di Auto Scaling, consulta Update Auto [Scaling instances nella Amazon EC2 Auto Scaling](#) User Guide.

[AutoScaling.6] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2 (2), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::AutoScaling::AutoScalingGroup

Regola AWS Config : [autoscaling-multiple-instance-types](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo Amazon EC2 Auto Scaling utilizza più tipi di istanze. Il controllo fallisce se il gruppo Auto Scaling ha un solo tipo di istanza definito.

È possibile aumentare la disponibilità distribuendo l'applicazione su più tipi di istanze in esecuzione in più zone di disponibilità. Security Hub consiglia di utilizzare più tipi di istanze in modo che il gruppo Auto Scaling possa avviare un altro tipo di istanza se la capacità delle istanze nelle zone di disponibilità scelte è insufficiente.

Correzione

Per creare un gruppo Auto Scaling con più tipi di istanze, consulta [Gruppi di Auto Scaling con più tipi di istanze e opzioni di acquisto](#) nella Guida per l'utente di Amazon EC2 Auto Scaling.

[AutoScaling.9] I gruppi di Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificazione > Configurazione delle risorse

Gravità: media

Tipo di risorsa: AWS::AutoScaling::AutoScalingGroup

Regola AWS Config : [autoscaling-launch-template](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo Amazon EC2 Auto Scaling viene creato a partire da un modello di lancio EC2. Questo controllo fallisce se un gruppo Amazon EC2 Auto Scaling non viene creato con un modello di avvio o se un modello di avvio non è specificato in una politica di istanze miste.

Un gruppo Auto Scaling EC2 può essere creato da un modello di lancio EC2 o da una configurazione di avvio. Tuttavia, l'utilizzo di un modello di avvio per creare un gruppo Auto Scaling garantisce l'accesso alle funzionalità e ai miglioramenti più recenti.

Correzione

Per creare un gruppo Auto Scaling con un modello di lancio EC2, consulta [Creare un gruppo Auto Scaling utilizzando un modello di avvio nella Guida per l'utente di Amazon EC2 Auto Scaling](#). Per informazioni su come sostituire una configurazione di avvio con un modello di avvio, consulta [Sostituire una configurazione di avvio con un modello di avvio](#) nella Amazon EC2 User Guide for Windows Instances.

[AutoScaling.10] I gruppi di Auto Scaling EC2 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::AutoScaling::AutoScalingGroup

AWS Config regola: tagged-autoscaling-autoscalinggroup (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfano	Nessun valore predefinito

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se un gruppo Amazon EC2 Auto Scaling dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gruppo Auto Scaling non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo Auto Scaling non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gruppo di Auto Scaling, consulta [Gruppi e istanze di Tag Auto Scaling](#) nella Guida per l'utente di Amazon EC2 Auto Scaling.

Controlli di Amazon EC2 Systems Manager

Questi controlli sono correlati alle istanze Amazon EC2 gestite da AWS Systems Manager

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[SSM.1] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager

Requisiti correlati: PCI DSS versione 3.2.1/2.4, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (1), NIST.800-53.r5 CM-8 (2), NIST.800-53.r5 CM-8 (2), NIST.800-53.r5 CM-8 (2), NIST.800-53.r5 CM-8 (2), NIST.800-53.r5 CM-8 (2), NIST.800-53.R5 SA-15 (2), NIST.800-53.R5 SA-15 (8), NIST.800-53.R5 SA-3, NIST.800-53R5 SI-2 (3)

Categoria: Identificazione > Inventario

Gravità: media

Risorsa valutata: AWS::EC2::Instance

Risorse AWS Config di registrazione richieste: AWS::EC2::Instance, AWS::SSM::ManagedInstanceInventory

Regola AWS Config : [ec2-instance-managed-by-systems-manager](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le istanze EC2 interrotte e in esecuzione nel tuo account sono gestite da AWS Systems Manager. Systems Manager è uno Servizio AWS strumento che puoi utilizzare per visualizzare e controllare la tua AWS infrastruttura.

Per aiutarvi a mantenere la sicurezza e la conformità, Systems Manager analizza le istanze gestite interrotte e in esecuzione. Un'istanza gestita è una macchina configurata per l'uso con Systems Manager. Systems Manager segnala quindi o intraprende azioni correttive in caso di violazioni delle policy rilevate. Systems Manager consente inoltre di configurare e gestire le istanze gestite.

Per saperne di più, consulta la [Guida AWS Systems Manager per l'utente](#).

Correzione

Per gestire le istanze EC2 con Systems Manager, consulta la gestione degli [host di Amazon EC2](#) nella AWS Systems Manager Guida per l'utente. Nella sezione Opzioni di configurazione, puoi mantenere le scelte predefinite o modificarle secondo necessità per la tua configurazione preferita.

[SSM.2] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch

Requisiti correlati: PCI DSS versione 3.2.1/6.2, NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (3), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: AWS::SSM::PatchCompliance

Regola AWS Config : [ec2-managedinstance-patch-compliance-status-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se lo stato di conformità della patch di Systems Manager è COMPLIANT o NON_COMPLIANT dopo l'installazione della patch sull'istanza. Il controllo ha esito negativo se lo stato di conformità è NON_COMPLIANT. Il controllo controlla solo le istanze gestite da Systems Manager Patch Manager.

L'applicazione di patch alle istanze EC2 come richiesto dall'organizzazione riduce la superficie di attacco della vostra. Account AWS

Correzione

Systems Manager consiglia di utilizzare [le policy di patch](#) per configurare l'applicazione delle patch per le istanze gestite. È inoltre possibile utilizzare [i documenti Systems Manager](#), come descritto nella procedura seguente, per applicare patch a un'istanza.

Per correggere le patch non conformi

1. Aprire la AWS Systems Manager console all'[indirizzo https://console.aws.amazon.com/systems-manager/](https://console.aws.amazon.com/systems-manager/).
2. Per la gestione dei nodi, scegli Esegui comando, quindi scegli Esegui comando.

3. Scegli l'opzione per AWS- RunPatchBaseline.
4. Modificare l'operazione su Install (Installa).
5. Scegli le istanze manualmente, quindi scegli le istanze non conformi.
6. Seleziona Esegui.
7. Una volta completato il comando, per monitorare il nuovo stato di conformità delle istanze a cui è stata applicata la patch, scegli Conformità nel riquadro di navigazione.

[SSM.3] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT

Requisiti correlati: PCI DSS versione 3.2.1/2.4, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-8, NIST.800-53.r5 CM-8 (1), NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 -53,5 SI-2 (3)

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa: AWS::SSM::AssociationCompliance

Regola AWS Config : [ec2-managedinstance-association-compliance-status-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se lo stato della conformità dell' AWS Systems Manager associazione è COMPLIANT o NON_COMPLIANT dopo l'esecuzione dell'associazione su un'istanza. Il controllo ha esito negativo se lo stato di conformità dell'associazione èNON_COMPLIANT.

Un'associazione State Manager è una configurazione assegnata alle istanze gestite. La configurazione definisce lo stato che desideri mantenere sulle istanze. Ad esempio, un'associazione può specificare che il software antivirus deve essere installato e in esecuzione sulle istanze o che determinate porte devono essere chiuse.

Dopo aver creato una o più associazioni di State Manager, le informazioni sullo stato di conformità sono immediatamente disponibili. È possibile visualizzare lo stato di conformità nella console o in risposta ai AWS CLI comandi o alle azioni API Systems Manager corrispondenti. Per le associazioni, Configuration Compliance mostra lo stato di conformità (CompliantoNon-compliant). Mostra anche il livello di gravità assegnato all'associazione, ad esempio `Critical` o `Medium`.

Per ulteriori informazioni sulla conformità dell'associazione State Manager, vedere [Informazioni sulla conformità all'associazione State Manager](#) nella Guida per l'AWS Systems Manager utente.

Correzione

Un'associazione fallita può essere correlata a diversi fattori, inclusi obiettivi e nomi di documenti SSM. Per risolvere questo problema, è necessario innanzitutto identificare e analizzare l'associazione visualizzando la cronologia delle associazioni. Per istruzioni sulla visualizzazione della cronologia delle associazioni, vedere [Visualizzazione della cronologia delle associazioni nella Guida](#) per l'AWS Systems Manager utente.

Dopo aver esaminato, è possibile modificare l'associazione per correggere il problema identificato. Puoi modificare un'associazione per specificare un nome, una pianificazione, un livello di gravità o target nuovi. Dopo aver modificato un'associazione, AWS Systems Manager crea una nuova versione. Per istruzioni sulla modifica di un'associazione, consulta [Modifica e creazione di una nuova versione di un'associazione](#) nella Guida per l'AWS Systems Manager utente.

[SSM.4] I documenti SSM non devono essere pubblici

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Severità: critica

Tipo di risorsa: AWS :: SSM :: Document

Regola AWS Config : [ssm-document-not-public](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se AWS Systems Manager i documenti di proprietà dell'account sono pubblici. Questo controllo fallisce se i documenti SSM con il proprietario Self sono pubblici.

I documenti SSM pubblici potrebbero consentire l'accesso involontario ai tuoi documenti. Un documento SSM pubblico può esporre informazioni preziose sull'account, sulle risorse e sui processi interni.

A meno che il tuo caso d'uso non richieda la condivisione pubblica, ti consigliamo di bloccare l'impostazione di condivisione pubblica per i documenti di Systems Manager di proprietà diSelf.

Correzione

Per bloccare la condivisione pubblica dei documenti SSM, consulta [Bloccare la condivisione pubblica per i documenti SSM nella Guida](#) per l'AWS Systems Manager utente.

Controlli Amazon Elastic File System

Questi controlli sono correlati alle risorse Amazon EFS.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[EFS.1] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS

Requisiti correlati: CIS AWS Foundations Benchmark v3.0.0/2.4.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28 (10), NIST.800-53.r5 SC-7 (10), NIST.800-53,5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::EFS::FileSystem

Regola AWS Config : [efs-encrypted-check](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se Amazon Elastic File System è configurato per crittografare i dati dei file utilizzando AWS KMS. Il controllo non riesce nei seguenti casi.

- Encrypted è impostato su false nella risposta [DescribeFileSystems](#).
- La chiave KmsKeyId nella risposta [DescribeFileSystems](#) non corrisponde al parametro KmsKeyId per [efs-encrypted-check](#).

Questo controllo non utilizza il parametro KmsKeyId per [efs-encrypted-check](#). Controlla solo il valore di Encrypted.

Per un ulteriore livello di sicurezza per i dati sensibili in Amazon EFS, è necessario creare file system crittografati. Amazon EFS supporta la crittografia per i file system inattivi. Puoi abilitare la crittografia dei dati inattivi quando crei un file system Amazon EFS. Per ulteriori informazioni sulla crittografia Amazon EFS, consulta la sezione [Crittografia dei dati in Amazon EFS](#) nella Amazon Elastic File System User Guide.

Correzione

Per dettagli su come crittografare un nuovo file system Amazon EFS, [consulta Encrypting data at rest](#) nella Amazon Elastic File System User Guide.

[EFS.2] I volumi Amazon EFS devono essere inclusi nei piani di backup

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST .800-53,5 SI-13 (5)

Categoria: Recupero > Resilienza > Backup

Gravità: media

Tipo di risorsa: AWS::EFS::FileSystem

Regola AWS Config : [efs-in-backup-plan](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se i file system Amazon Elastic File System (Amazon EFS) vengono aggiunti ai piani di backup in AWS Backup. Il controllo fallisce se i file system Amazon EFS non sono inclusi nei piani di backup.

L'inclusione dei file system EFS nei piani di backup consente di proteggere i dati dall'eliminazione e dalla perdita di dati.

Correzione

Per abilitare i backup automatici per un file system Amazon EFS esistente, consulta [Getting started 4: Create backup automatici di Amazon EFS](#) nella AWS Backup Developer Guide.

[EFS.3] I punti di accesso EFS devono applicare una directory principale

Requisiti correlati: NIST.800-53.r5 AC-6 (10)

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS::EFS::AccessPoint

Regola AWS Config : [efs-access-point-enforce-root-directory](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i punti di accesso Amazon EFS sono configurati per applicare una directory principale. Il controllo fallisce se il valore di Path è impostato su / (la directory principale predefinita del file system).

Quando applichi una directory radice, il client NFS che utilizza il punto di accesso usa la directory radice configurata sul punto di accesso anziché la directory radice del file system. L'applicazione di una directory principale per un punto di accesso consente di limitare l'accesso ai dati garantendo che gli utenti del punto di accesso possano accedere solo ai file della sottodirectory specificata.

Correzione

Per istruzioni su come applicare una directory principale per un punto di accesso Amazon EFS, consulta Implementazione di [una directory principale con un punto di accesso](#) nella Amazon Elastic File System User Guide.

[EFS.4] I punti di accesso EFS devono applicare un'identità utente

Requisiti correlati: NIST.800-53.r5 AC-6 (2)

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS::EFS::AccessPoint

Regola AWS Config : [efs-access-point-enforce-user-identity](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i punti di accesso Amazon EFS sono configurati per applicare un'identità utente. Questo controllo ha esito negativo se non viene definita un'identità utente POSIX durante la creazione del punto di accesso EFS.

I punti di accesso Amazon EFS sono punti di accesso specifici dell'applicazione in un file system EFS che semplificano la gestione dell'accesso dell'applicazione ai set di dati condivisi. I punti di accesso possono applicare un'identità utente, inclusi i gruppi dell'utente POSIX, per tutte le richieste al file system effettuate tramite il punto di accesso. I punti di accesso possono inoltre applicare una directory radice diversa per il file system in modo che i client possano accedere solo ai dati nella directory specificata o nelle sue sottodirectory.

Correzione

Per applicare un'identità utente per un punto di accesso Amazon EFS, consulta [Applica un'identità utente utilizzando un punto di accesso](#) nella Amazon Elastic File System User Guide.

[EFS.5] I punti di accesso EFS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::EFS::AccessPoint

AWS Config regola: tagged-efs-accesspoint (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfano	Nessun valore predefinito

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se un punto di accesso Amazon EFS dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il punto di accesso non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il punto di accesso non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un punto di accesso EFS, consulta la sezione [Tagging delle risorse Amazon EFS](#) nella Amazon Elastic File System User Guide.

[EFS.6] I target di montaggio EFS non devono essere associati a una sottorete pubblica

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Gravità: media

Tipo di risorsa: AWS::EFS::FileSystem

Regola AWS Config : [efs-mount-target-public-accessible](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un target di montaggio Amazon EFS è associato a una sottorete privata. Il controllo fallisce se la destinazione di montaggio è associata a una sottorete pubblica.

Per impostazione predefinita, un file system è accessibile solo dal cloud privato virtuale (VPC) in cui è stato creato. Consigliamo di creare target di montaggio EFS in sottoreti private non accessibili da Internet. Questo aiuta a garantire che il file system sia accessibile solo agli utenti autorizzati e non sia vulnerabile ad accessi o attacchi non autorizzati.

Correzione

Non è possibile modificare l'associazione tra una destinazione di montaggio EFS e una sottorete dopo aver creato la destinazione di montaggio. Per associare una destinazione di montaggio esistente a una sottorete diversa, è necessario creare una nuova destinazione di montaggio in una sottorete privata e quindi rimuovere la vecchia destinazione di montaggio. Per informazioni sulla gestione degli obiettivi di montaggio, consulta [Creazione e gestione di destinazioni di montaggio e gruppi di sicurezza](#) nella Amazon Elastic File System User Guide.

Controlli di Amazon Elastic Kubernetes Service

Questi controlli sono correlati alle risorse Amazon EKS.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[EKS.1] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7,

NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Protezione > Gestione sicura degli accessi > Risorsa non accessibile al pubblico

Gravità: alta

Tipo di risorsa: AWS::EKS::Cluster

Regola AWS Config : [eks-endpoint-no-public-access](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un endpoint del cluster Amazon EKS è accessibile pubblicamente. Il controllo fallisce se un cluster EKS ha un endpoint accessibile pubblicamente.

Quando crei un nuovo cluster, Amazon EKS crea un endpoint per il server API Kubernetes gestito che usi per comunicare con il cluster. Per impostazione predefinita, questo endpoint del server API è disponibile pubblicamente su Internet. L'accesso al server API è protetto utilizzando una combinazione di AWS Identity and Access Management (IAM) e il controllo degli accessi basato sul ruolo (RBAC) di Kubernetes nativo. Rimuovendo l'accesso pubblico all'endpoint, puoi evitare l'esposizione e l'accesso involontari al tuo cluster.

Correzione

Per modificare l'accesso agli endpoint per un cluster EKS esistente, consulta [Modificare l'accesso agli endpoint del cluster](#) nella Amazon EKS User Guide. Puoi configurare l'accesso agli endpoint per un nuovo cluster EKS al momento della creazione. Per istruzioni sulla creazione di un nuovo cluster Amazon EKS, consulta [Creazione di un cluster Amazon EKS](#) nella Guida per l'utente di Amazon EKS.

[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: alta

Tipo di risorsa: AWS::EKS::Cluster

Regola AWS Config : [eks-cluster-supported-version](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `oldestVersionSupported`: 1.26 (non personalizzabile)

Questo controllo verifica se un cluster Amazon Elastic Kubernetes Service (Amazon EKS) è in esecuzione su una versione Kubernetes supportata. Il controllo fallisce se il cluster EKS è in esecuzione su una versione non supportata.

Se la tua applicazione non richiede una versione specifica di Kubernetes, ti consigliamo di utilizzare l'ultima versione di Kubernetes disponibile supportata da EKS per i tuoi cluster. Per ulteriori informazioni, consulta il calendario di [rilascio di Amazon EKS Kubernetes](#), il [supporto per la versione di Amazon EKS e le domande frequenti](#) nella Guida per l'utente di Amazon EKS.

Correzione

Per aggiornare un cluster EKS, consulta [Aggiornamento di una versione Kubernetes del cluster Amazon EKS](#) nella Guida per l'utente di Amazon EKS.

[EKS.3] I cluster EKS devono utilizzare segreti Kubernetes crittografati

Requisiti correlati: NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-13, NIST.800-53.r5 SI-28

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: `AWS::EKS::Cluster`

Regola AWS Config : [eks-secrets-encrypted](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un cluster Amazon EKS utilizza segreti Kubernetes crittografati. Il controllo fallisce se i segreti Kubernetes del cluster non sono crittografati.

Quando crittografi i segreti, puoi utilizzare le chiavi AWS Key Management Service (AWS KMS) per fornire la crittografia in busta dei segreti Kubernetes archiviati in etcd per il tuo cluster. Questa crittografia si aggiunge alla crittografia del volume EBS che è abilitata per impostazione predefinita per tutti i dati (inclusi i segreti) archiviati in etcd come parte di un cluster EKS. L'utilizzo della crittografia segreta per il cluster EKS consente di implementare una strategia di difesa approfondita per le applicazioni Kubernetes crittografando i segreti Kubernetes con una chiave KMS definita e gestita dall'utente.

Correzione

Per abilitare la crittografia segreta su un cluster EKS, [consulta Abilitazione della crittografia segreta su un cluster esistente](#) nella Amazon EKS User Guide.

[EKS.6] I cluster EKS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EKS::Cluster`

AWS Config regola: `tagged-eks-cluster` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un cluster Amazon EKS dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il cluster non ha alcuna chiave di tag o se non

ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il cluster non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing. Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in Riferimenti generali di AWS.

Correzione

Per aggiungere tag a un cluster EKS, consulta [Tagging your Amazon EKS Resources](#) nella Amazon EKS User Guide.

[EKS.7] Le configurazioni dei provider di identità EKS devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::EKS::IdentityProviderConfig`

AWS Config regola: `tagged-eks-identityproviderconfig` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se la configurazione di un provider di identità Amazon EKS ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se la configurazione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la configurazione non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag alle configurazioni di un provider di identità EKS, consulta [Tagging your Amazon EKS resources](#) nella Amazon EKS User Guide.

[EKS.8] I cluster EKS devono avere la registrazione di controllo abilitata

Requisiti correlati: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::EKS::Cluster

Regola AWS Config : [eks-cluster-logging-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un cluster Amazon EKS ha abilitato la registrazione di audit. Il controllo fallisce se la registrazione di controllo non è abilitata per il cluster.

La registrazione del piano di controllo EKS fornisce registri di audit e diagnostica direttamente dal piano di controllo EKS ad Amazon CloudWatch Logs nel tuo account. Puoi selezionare i tipi di log di cui hai bisogno e i log vengono inviati come flussi di log a un gruppo per ogni cluster EKS in cui risiede. CloudWatch La registrazione offre visibilità sull'accesso e sulle prestazioni dei cluster EKS. Inviando i log del piano di controllo EKS per i cluster EKS a CloudWatch Logs, è possibile registrare le operazioni a fini di controllo e diagnostica in una posizione centrale.

Correzione

Per abilitare i log di controllo per il tuo cluster EKS, consulta [Abilitazione e disabilitazione dei log del piano di controllo nella Guida per l'utente di Amazon EKS](#).

ElastiCache Controlli Amazon

Questi controlli sono correlati alle ElastiCache risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[ElastiCache.1] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST .800-53,5 SI-13 (5)

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: alta

Tipo di risorsa: AWS::ElastiCache::CacheCluster

AWS Config regola: [elasticache-redis-cluster-automatic-backup-check](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
snapshotRetentionPeriod	Periodo minimo di conservazione delle istantanee in giorni	Numero intero	1 Da a 35	1

Questo controllo valuta se un cluster Amazon ElastiCache for Redis ha pianificati backup automatici. Il controllo fallisce se il periodo di SnapshotRetentionLimit tempo per il cluster Redis è inferiore

al periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di conservazione delle istantanee, Security Hub utilizza un valore predefinito di 1 giorno.

I cluster Amazon ElastiCache for Redis possono eseguire il backup dei propri dati. Il backup può essere utilizzato per ripristinare un cluster o dare fonte a un nuovo cluster. Il backup è costituito dai metadati del cluster, insieme a tutti i dati nel cluster. Tutti i backup vengono scritti su Amazon Simple Storage Service (Amazon S3), che fornisce uno storage durevole. Puoi ripristinare i dati creando un nuovo cluster Redis e popolandolo con i dati di un backup. Puoi gestire i backup utilizzando AWS Management Console, the AWS Command Line Interface (AWS CLI) e l'API. ElastiCache

Correzione

Per pianificare backup automatici su un cluster ElastiCache for Redis, consulta [Scheduling automatic backup nella](#) Amazon User Guide. ElastiCache

[ElastiCache.2] ElastiCache per i cluster di cache Redis dovrebbe avere l'aggiornamento automatico della versione secondaria abilitato

Requisiti correlati: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: alta

Tipo di risorsa: `AWS::ElastiCache::CacheCluster`

Regola AWS Config : [elasticache-auto-minor-version-upgrade-check](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo valuta se ElastiCache per Redis applica automaticamente gli aggiornamenti di versione minori ai cluster di cache. Questo controllo ha esito negativo se ElastiCache per i cluster di cache Redis non vengono applicati automaticamente gli aggiornamenti delle versioni minori.

AutoMinorVersionUpgrade è una funzionalità che puoi attivare ElastiCache per Redis per aggiornare automaticamente i cluster di cache quando è disponibile una nuova versione del motore di cache secondario. Questi aggiornamenti potrebbero includere patch di sicurezza e correzioni di bug. Continuare up-to-date a installare le patch è un passo importante per proteggere i sistemi.

Correzione

Per applicare aggiornamenti automatici delle versioni secondarie a un cluster di cache esistente ElastiCache per Redis, consulta [Upgrading engine versions nella](#) Amazon User Guide. ElastiCache

[ElastiCache.3] ElastiCache per i gruppi di replica Redis dovrebbe avere il failover automatico abilitato

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::ElastiCache::ReplicationGroup

Regola AWS Config : [elasticache-repl-grp-auto-failover-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se ElastiCache per i gruppi di replica Redis è abilitato il failover automatico. Questo controllo ha esito negativo se il failover automatico non è abilitato per un gruppo di replica Redis.

Quando il failover automatico è abilitato per un gruppo di replica, il ruolo del nodo primario eseguirà automaticamente il failover su una delle repliche di lettura. Questa promozione del failover e della replica consente di riprendere la scrittura sul nuovo sistema primario una volta completata la promozione, riducendo così i tempi di inattività complessivi in caso di guasto.

Correzione

Per abilitare il failover automatico per un gruppo di replica esistente ElastiCache per Redis, consulta [Modifying an cluster ElastiCache nella](#) Amazon User Guide. ElastiCache Se usi la ElastiCache console, imposta il failover automatico su abilitato.

[ElastiCache.4] ElastiCache per i gruppi di replica Redis deve essere crittografato a riposo

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia di data-at-rest

Gravità: media

Tipo di risorsa: AWS::ElastiCache::ReplicationGroup

Regola AWS Config : [elasticache-repl-grp-encrypted-at-rest](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se i gruppi ElastiCache di replica Redis sono crittografati a riposo. Questo controllo ha esito negativo se un gruppo di replica ElastiCache for Redis non è crittografato a riposo.

La crittografia dei dati inattivi riduce il rischio che un utente non autenticato acceda ai dati archiviati su disco. ElastiCache per un ulteriore livello di sicurezza, i gruppi di replica di Redis devono essere crittografati quando sono inattivi.

Correzione

Per configurare la crittografia at-rest su un gruppo di replica ElastiCache for Redis, consulta [Enabling at-rest encryption nella](#) Amazon User Guide. ElastiCache

[ElastiCache.5] ElastiCache per i gruppi di replica Redis devono essere crittografati in transito

Requisiti correlati: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia di data-in-transit

Gravità: media

Tipo di risorsa: AWS::ElastiCache::ReplicationGroup

Regola AWS Config : [elasticache-repl-grp-encrypted-in-transit](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se i gruppi ElastiCache di replica Redis sono crittografati in transito. Questo controllo ha esito negativo se un gruppo di replica ElastiCache for Redis non è crittografato in transito.

La crittografia dei dati in transito riduce il rischio che un utente non autorizzato possa intercettare il traffico di rete. L'attivazione della crittografia in transito su un gruppo di replica ElastiCache per Redis crittografa i dati ogni volta che vengono spostati da un luogo all'altro, ad esempio tra i nodi del cluster o tra il cluster e l'applicazione.

Correzione

Per configurare la crittografia in transito su un gruppo di replica ElastiCache per Redis, consulta [Enabling in-transit encryption nella](#) Amazon User Guide. ElastiCache

[ElastiCache.6] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS::ElastiCache::ReplicationGroup

Regola AWS Config : [elasticache-repl-grp-redis-auth-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se ElastiCache per i gruppi di replica Redis è abilitato Redis AUTH. Il controllo ha esito negativo per un gruppo di replica ElastiCache for Redis se la versione Redis dei relativi nodi è inferiore alla 6.0 e non è in uso. AuthToken

Quando si utilizzano token di autenticazione o password Redis, Redis richiede una password prima di consentire ai client di eseguire i comandi, il che migliora la sicurezza dei dati. Per Redis 6.0 e versioni successive, consigliamo di utilizzare Role-Based Access Control (RBAC). Poiché RBAC non è supportato per le versioni di Redis precedenti alla 6.0, questo controllo valuta solo le versioni che non possono utilizzare la funzionalità RBAC.

Correzione

Per utilizzare Redis AUTH su un gruppo di replica ElastiCache for Redis, consulta [Modifica del token AUTH su un cluster for ElastiCache Redis esistente](#) nella Amazon User Guide. ElastiCache

[ElastiCache.7] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito

Requisiti correlati: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53,5 SC-7 (5)

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: AWS::ElastiCache::CacheCluster

Regola AWS Config : [elasticache-subnet-group-check](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se ElastiCache i cluster sono configurati con un gruppo di sottoreti personalizzato. Il controllo ha esito negativo per un ElastiCache cluster se CacheSubnetGroupName ha il valore. default

Quando si avvia un ElastiCache cluster, viene creato un gruppo di sottoreti predefinito se non ne esiste già uno. Il gruppo predefinito utilizza le sottoreti del Virtual Private Cloud (VPC) predefinito. Si consiglia di utilizzare gruppi di sottoreti personalizzati che limitino le sottoreti in cui risiede il cluster e la rete che il cluster eredita dalle sottoreti.

Correzione

Per creare un nuovo gruppo di sottoreti per un ElastiCache cluster, consulta la sezione [Creazione di un gruppo di sottoreti](#) nella Amazon ElastiCache User Guide.

AWS Elastic Beanstalk controlli

Questi controlli sono correlati alle risorse Elastic Beanstalk.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[ElasticBeanstalk.1] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata

Requisiti correlati: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoria: Rileva > Servizi di rilevamento > Monitoraggio delle applicazioni

Gravità: bassa

Tipo di risorsa: AWS::ElasticBeanstalk::Environment

Regola AWS Config : [beanstalk-enhanced-health-reporting-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i report avanzati sullo stato di salute sono abilitati per gli AWS Elastic Beanstalk ambienti in uso.

La reportistica avanzata sullo stato di Elastic Beanstalk consente una risposta più rapida ai cambiamenti nello stato dell'infrastruttura sottostante. Queste modifiche potrebbero comportare una mancanza di disponibilità dell'applicazione.

Il reporting avanzato sull'integrità di Elastic Beanstalk fornisce un descrittore dello stato per valutare la gravità dei problemi identificati e per individuare le possibili cause su cui indagare. L'agente sanitario Elastic Beanstalk, incluso nelle AMI (Amazon Machine Images) supportate, valuta i log e i parametri delle istanze EC2 dell'ambiente.

Per ulteriori informazioni, consulta [Enhanced](#) Health Reporting and Monitoring nella Developer Guide.AWS Elastic Beanstalk

Correzione

Per istruzioni su come abilitare la reportistica sanitaria avanzata, consulta Enhancing [Enhanced Health Reporting using the Elastic Beanstalk console](#) nella Developer Guide.AWS Elastic Beanstalk

[ElasticBeanstalk.2] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati

Requisiti correlati: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoria: Rileva > Gestione di vulnerabilità, patch e versioni

Gravità: alta

Tipo di risorsa: AWS::ElasticBeanstalk::Environment

Regola AWS Config : [elastic-beanstalk-managed-updates-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
UpdateLevel	Livello di aggiornamento della versione	Enum	minor, patch	Nessun valore predefinito

Questo controllo verifica se gli aggiornamenti della piattaforma gestita sono abilitati per un ambiente Elastic Beanstalk. Il controllo fallisce se non sono abilitati gli aggiornamenti gestiti della piattaforma. Per impostazione predefinita, il controllo passa se è abilitato qualsiasi tipo di aggiornamento della piattaforma. Facoltativamente, è possibile fornire un valore di parametro personalizzato per richiedere un livello di aggiornamento specifico.

L'abilitazione degli aggiornamenti gestiti della piattaforma garantisce l'installazione delle correzioni, degli aggiornamenti e delle funzionalità più recenti disponibili per l'ambiente. Mantenersi aggiornati sull'installazione delle patch è un passaggio importante per proteggere i sistemi.

Correzione

Per abilitare gli aggiornamenti gestiti della piattaforma, consulta [Configurare gli aggiornamenti gestiti della piattaforma in Aggiornamenti gestiti della piattaforma](#) nella Guida per gli AWS Elastic Beanstalk sviluppatori.

[ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch

Categoria: Identificazione > Registrazione

Gravità: alta

Tipo di risorsa: AWS::ElasticBeanstalk::Environment

Regola AWS Config : [elastic-beanstalk-logs-to-cloudwatch](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
RetentionInDays	Numero di giorni in cui conservare gli eventi di registro prima della scadenza	Enum	1, 3, 5, 7, 14, 30, 60, 90, 120, 150, 180, 365, 400, 545, 731, 1827, 3653	Nessun valore predefinito

Questo controllo verifica se un ambiente Elastic Beanstalk è configurato per inviare log a Logs. CloudWatch Il controllo fallisce se un ambiente Elastic Beanstalk non è configurato per inviare log a Logs. CloudWatch Facoltativamente, puoi fornire un valore personalizzato per il RetentionInDays parametro se desideri che il controllo passi solo se i log vengono conservati per il numero di giorni specificato prima della scadenza.

CloudWatch consente di raccogliere e monitorare varie metriche per le applicazioni e le risorse dell'infrastruttura. È inoltre possibile utilizzarlo CloudWatch per configurare le azioni di allarme in base

a metriche specifiche. Ti consigliamo di integrare Elastic Beanstalk con per ottenere una maggiore visibilità nel tuo ambiente Elastic CloudWatch Beanstalk. I log di Elastic Beanstalk includono `eb-activity.log`, i log di accesso dall'ambiente `nginx` o dal server proxy Apache e i log specifici di un ambiente.

Correzione

Per integrare Elastic CloudWatch Beanstalk con Logs, [consulta Streaming dei log delle istanze CloudWatch](#) su Logs nella Developer Guide.AWS Elastic Beanstalk

Controlli Elastic Load Balancing

Questi controlli sono correlati alle risorse Elastic Load Balancing.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[ELB.1] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS

Requisiti correlati: PCI DSS versione 3.2.1/2.3, PCI DSS versione 3.2.1/4.1, NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoria: Rilevamento > Servizi di rilevamento

Gravità: media

Tipo di risorsa: AWS::ElasticLoadBalancingV2::LoadBalancer

Regola AWS Config : [alb-http-to-https-redirection-check](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se il reindirizzamento da HTTP a HTTPS è configurato su tutti i listener HTTP di Application Load Balancers. Il controllo ha esito negativo se per uno dei listener HTTP di Application Load Balancers non è configurato il reindirizzamento da HTTP a HTTPS.

Prima di iniziare a utilizzare Application Load Balancer, è necessario aggiungere uno o più listener. Un listener è un processo che utilizza il protocollo e la porta configurati per verificare la presenza di richieste di connessione. I listener supportano entrambi i protocolli HTTP e HTTPS. È possibile utilizzare un listener HTTPS per affidare il lavoro di crittografia e decrittografia al sistema di bilanciamento del carico. Per applicare la crittografia in transito, è necessario utilizzare le azioni di reindirizzamento con Application Load Balancers per reindirizzare le richieste HTTP dei client a una richiesta HTTPS sulla porta 443.

Per ulteriori informazioni, consulta [Listeners for your Application Load Balancers nella User Guide for Application Load Balancers](#).

Correzione

Per reindirizzare le richieste HTTP su HTTPS, è necessario aggiungere una regola listener Application Load Balancer o modificare una regola esistente.

Per istruzioni sull'aggiunta di una nuova regola, consulta [Aggiungere una regola](#) nella Guida utente di Application Load Balancers. Per Protocollo: Porta, scegliete HTTP, quindi immettete. **80** Per Aggiungi azione, Reindirizza a, scegli HTTPS, quindi inserisci **443**.

Per istruzioni sulla modifica di una regola esistente, consulta [Modificare una regola](#) nella Guida utente di Application Load Balancers. Per Protocollo: Porta, scegliete HTTP, quindi immettete. **80** Per Aggiungi azione, Reindirizza a, scegli HTTPS, quindi inserisci **443**.

[ELB.2] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager

Requisiti correlati: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (5), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: AWS::ElasticLoadBalancing::LoadBalancer

Regola AWS Config : [elb-acm-certificate-required](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il Classic Load Balancer utilizza i certificati HTTPS/SSL forniti da (ACM). AWS Certificate Manager Il controllo ha esito negativo se il listener Classic Load Balancer configurato con HTTPS/SSL non utilizza un certificato fornito da ACM.

Per creare un certificato, puoi utilizzare ACM o uno strumento che supporti i protocolli SSL e TLS, come OpenSSL. Security Hub consiglia di utilizzare ACM per creare o importare certificati per il sistema di bilanciamento del carico.

ACM si integra con Classic Load Balancers in modo da poter distribuire il certificato sul sistema di bilanciamento del carico. È inoltre necessario rinnovare automaticamente questi certificati.

Correzione

Per informazioni su come associare un certificato ACM SSL/TLS a un Classic Load Balancer, consulta l'articolo del AWS Knowledge Center [Come posso associare un certificato ACM SSL/TLS a un Classic, Application o Network Load Balancer?](#)

[ELB.3] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS

Requisiti correlati: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: AWS::ElasticLoadBalancing::LoadBalancer

Regola AWS Config : [elb-tls-https-listeners-only](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i listener Classic Load Balancer sono configurati con il protocollo HTTPS o TLS per le connessioni front-end (da client a load balancer). Il controllo è applicabile se un

Classic Load Balancer dispone di ascoltatori. Se il Classic Load Balancer non dispone di un listener configurato, il controllo non riporta alcun risultato.

Il controllo passa se i listener Classic Load Balancer sono configurati con TLS o HTTPS per le connessioni front-end.

Il controllo fallisce se il listener non è configurato con TLS o HTTPS per le connessioni front-end.

Prima di iniziare a utilizzare un sistema di bilanciamento del carico, è necessario aggiungere uno o più listener. Un listener è un processo che utilizza il protocollo e la porta configurati per verificare la presenza di richieste di connessione. I listener possono supportare i protocolli HTTP e HTTPS/TLS. È necessario utilizzare sempre un listener HTTPS o TLS, in modo che il load balancer esegua il lavoro di crittografia e decrittografia in transito.

Correzione

Per risolvere questo problema, aggiorna i listener in modo che utilizzino il protocollo TLS o HTTPS.

Per trasformare tutti gli ascoltatori non conformi in listener TLS/HTTPS

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione, in Bilanciamento del carico, scegli Sistemi di bilanciamento del carico.
3. Seleziona il Classic Load Balancer.
4. Nella scheda Listeners (Listener), seleziona Edit (Modifica).
5. Per tutti i listener in cui Load Balancer Protocol non è impostato su HTTPS o SSL, modificate l'impostazione su HTTPS o SSL.
6. Per tutti i listener modificati, nella scheda Certificati, scegliete Cambia default.
7. Selezionare un certificato per Certificati ACM e IAM.
8. Scegliere Salva come predefinito.
9. Dopo aver aggiornato tutti i listener, scegliete Salva.

[ELB.4] L'Application Load Balancer deve essere configurato per eliminare le intestazioni http

Requisiti correlati: NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8 (2)

Categoria: Proteggi > Sicurezza di rete

Gravità: media

Tipo di risorsa: AWS::ElasticLoadBalancingV2::LoadBalancer

Regola AWS Config : [alb-http-drop-invalid-header-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo valuta gli AWS Application Load Balancer per garantire che siano configurati per eliminare le intestazioni HTTP non valide. Il controllo ha esito negativo se il valore di `routing.http.drop_invalid_header_fields.enabled` è impostato su `false`.

Per impostazione predefinita, gli Application Load Balancer non sono configurati per eliminare valori di intestazione HTTP non validi. La rimozione di questi valori di intestazione impedisce gli attacchi di desincronizzazione HTTP.

Nota che puoi disabilitare questo controllo se [ELB.12](#) è abilitato.

Correzione

Per risolvere questo problema, configura il sistema di bilanciamento del carico in modo da eliminare i campi di intestazione non validi.

Per configurare il load balancer in modo da eliminare i campi di intestazione non validi

1. Apri la console Amazon EC2 all'indirizzo <https://console.aws.amazon.com/ec2/>.
2. Nel riquadro di navigazione selezionare Load Balancers (Sistemi di bilanciamento del carico).
3. Scegliete un Application Load Balancer.
4. Da Azioni, scegli Modifica attributi.
5. In Elimina campi di intestazione non validi, scegli Abilita.
6. Selezionare Salva.

[ELB.5] La registrazione delle applicazioni e dei sistemi Classic Load Balancers deve essere abilitata

Requisiti correlati: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (4) R5 CA-7, NIST. 800-53.R5 SC-7 (9), NIST. 800-53.5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::ElasticLoadBalancing::LoadBalancer,
AWS::ElasticLoadBalancingV2::LoadBalancer

Regola AWS Config : [elb-logging-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'Application Load Balancer e il Classic Load Balancer hanno la registrazione abilitata. Se lo è, il controllo fallisce. `access_logs.s3.enabled false`

Elastic Load Balancing fornisce log di accesso che acquisiscono informazioni dettagliate sulle richieste inviate al tuo load balancer. Ogni log contiene informazioni come l'ora in cui è stata ricevuta la richiesta, l'indirizzo IP del client, le latenze, i percorsi delle richieste e le risposte del server. Puoi utilizzare questi log per analizzare i modelli di traffico e risolvere i problemi che potresti incontrare.

Per ulteriori informazioni, consulta [i registri di accesso per il tuo Classic Load Balancer](#) nella Guida per l'utente dei Classic Load Balancer.

Correzione

Per abilitare i log di accesso, consulta la [Fase 3: Configurazione dei log di accesso](#) nella Guida utente per Application Load Balancers.

[ELB.6] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::ElasticLoadBalancingV2::LoadBalancer

Regola AWS Config : [elb-deletion-protection-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'applicazione, un gateway o un Network Load Balancer ha la protezione da eliminazione abilitata. Il controllo ha esito negativo se la protezione da eliminazione è disattivata.

Abilita la protezione dall'eliminazione per proteggere l'applicazione, il gateway o il Network Load Balancer dall'eliminazione.

Correzione

Per evitare che il sistema di bilanciamento del carico venga eliminato accidentalmente, è possibile abilitare la protezione da eliminazione. Per impostazione predefinita, la protezione da eliminazioni è disabilitata nel sistema di bilanciamento del carico.

Se si abilita la protezione da eliminazione per il sistema di bilanciamento del carico, è necessario disabilitare la protezione da eliminazione prima di poter eliminare il sistema di bilanciamento del carico.

Per abilitare la protezione da eliminazione per un Application Load Balancer, vedere [Protezione da eliminazione](#) nella User Guide for Application Load Balancer. Per abilitare la protezione da eliminazione per un Gateway Load Balancer, vedere [Protezione da eliminazione](#) nella Guida utente di Gateway Load Balancer. Per abilitare la protezione da eliminazione per un Network Load Balancer, vedere [Protezione da eliminazione](#) nella Guida dell'utente per Network Load Balancer.

[ELB.7] I Classic Load Balancer devono avere il drenaggio della connessione abilitato

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Recupero > Resilienza

Gravità: media

Tipo di risorsa: AWS::ElasticLoadBalancing::LoadBalancer

AWS Config regola: elb-connection-draining-enabled (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i Classic Load Balancer hanno abilitato il drenaggio della connessione.

L'abilitazione del drenaggio della connessione sui Classic Load Balancer garantisce che il sistema di bilanciamento del carico interrompa l'invio di richieste alle istanze che non sono registrate o non sono funzionanti. Mantiene aperte le connessioni esistenti. Ciò è particolarmente utile per le istanze nei gruppi di Auto Scaling, per garantire che le connessioni non vengano interrotte bruscamente.

Correzione

Per abilitare il drenaggio della connessione sui Classic Load Balancer, consulta [Configurare il drenaggio della connessione per Classic Load Balancer nella Guida dell'utente per Classic Load Balancer](#).

[ELB.8] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita con una durata elevata AWS Config

Requisiti correlati: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: AWS::ElasticLoadBalancing::LoadBalancer

Regola AWS Config : [elb-predefined-security-policy-ssl-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

- predefinedPolicyName: ELBSecurityPolicy-TLS-1-2-2017-01 (non personalizzabile)

Questo controllo verifica se i listener HTTPS/SSL di Classic Load Balancer utilizzano la policy predefinita. ELBSecurityPolicy-TLS-1-2-2017-01 Il controllo fallisce se i listener HTTPS/SSL di Classic Load Balancer non lo utilizzano. ELBSecurityPolicy-TLS-1-2-2017-01

Una politica di sicurezza è una combinazione di protocolli SSL, cifrari e l'opzione Server Order Preference. Le politiche predefinite controllano i codici, i protocolli e gli ordini di preferenza da supportare durante le negoziazioni SSL tra un client e un sistema di bilanciamento del carico.

L'utilizzo `ELBSecurityPolicy-TLS-1-2-2017-01` può aiutarti a soddisfare gli standard di conformità e sicurezza che richiedono la disabilitazione di versioni specifiche di SSL e TLS. Per ulteriori informazioni, consulta [Policy di sicurezza SSL predefinite per Classic Load Balancers nella Guida per l'utente di Classic Load Balancers](#).

Correzione

Per informazioni su come utilizzare la politica di sicurezza predefinita `ELBSecurityPolicy-TLS-1-2-2017-01` con un Classic Load Balancer, [consulta Configure security settings in User Guide for Classic Load Balancer](#).

[ELB.9] I Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancing::LoadBalancer`

Regola AWS Config : [elb-cross-zone-load-balancing-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se il bilanciamento del carico tra zone è abilitato per i Classic Load Balancer (CLB). Il controllo fallisce se il bilanciamento del carico tra zone non è abilitato per un CLB.

Un nodo di bilanciamento del carico distribuisce il traffico solo tra le destinazioni registrate nella sua zona di disponibilità. Se il bilanciamento del carico tra zone è disabilitato, ogni nodo del sistema di bilanciamento del carico distribuisce il traffico solo tra le destinazioni registrate nella sua zona di disponibilità. Se il numero di destinazioni registrate non è lo stesso nelle zone di disponibilità, il traffico non verrà distribuito in modo uniforme e le istanze in una zona potrebbero finire per essere

utilizzate in modo eccessivo rispetto alle istanze in un'altra zona. Con il bilanciamento del carico tra zone abilitato, ogni nodo di load balancer per Classic Load Balancer distribuisce le richieste in modo uniforme tra le istanze registrate in tutte le zone di disponibilità abilitate. Per i dettagli, consulta [il bilanciamento del carico tra zone nella Elastic Load Balancing User Guide](#).

Correzione

Per abilitare il bilanciamento del carico tra zone in un Classic Load Balancer, [consulta Abilita il bilanciamento del carico tra zone nella Guida utente per Classic Load Balancer](#).

[ELB.10] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::ElasticLoadBalancing::LoadBalancer

Regola AWS Config : [clb-multiple-az](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
minAvailabilityZones	Numero minimo di zone di disponibilità	Enum	2, 3, 4, 5, 6	2

Questo controllo verifica se un Classic Load Balancer è stato configurato per coprire almeno il numero specificato di zone di disponibilità (AZ). Il controllo fallisce se il Classic Load Balancer non copre almeno il numero specificato di AZ. A meno che non si fornisca un valore di parametro personalizzato per il numero minimo di AZ, Security Hub utilizza un valore predefinito di due AZ.

È possibile configurare un Classic Load Balancer per distribuire le richieste in entrata tra le istanze Amazon EC2 in una singola zona di disponibilità o più zone di disponibilità. Un Classic Load Balancer che non si estende su più zone di disponibilità non è in grado di reindirizzare il traffico verso destinazioni in un'altra zona di disponibilità se l'unica zona di disponibilità configurata non è disponibile.

Correzione

Per aggiungere zone di disponibilità a un Classic Load Balancer, consulta [Aggiungere o rimuovere sottoreti per il Classic Load Balancer nella Guida utente per Classic Load Balancer](#).

[ELB.12] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa

Requisiti correlati: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione dei dati > Integrità dei dati

Gravità: media

Tipo di risorsa: AWS::ElasticLoadBalancingV2::LoadBalancer

Regola AWS Config : [alb-desync-mode-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

- desyncMode: defensive, strictest (non personalizzabile)

Questo controllo verifica se un Application Load Balancer è configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa. Il controllo fallisce se un Application Load Balancer non è configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa.

I problemi relativi a HTTP Desync possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della coda di richieste o della cache. A loro volta, queste vulnerabilità possono portare al furto di credenziali o all'esecuzione di comandi non autorizzati. Gli Application Load Balancer configurati con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa proteggono l'applicazione dai problemi di sicurezza che potrebbero essere causati da HTTP Desync.

Correzione

Per aggiornare la modalità di mitigazione della desincronizzazione di un Application Load Balancer, [consulta la modalità di mitigazione Desync nella User Guide for Application Load Balancers](#).

[ELB.13] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::ElasticLoadBalancingV2::LoadBalancer

Regola AWS Config : [elbv2-multiple-az](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
minAvailabilityZones	Numero minimo di zone di disponibilità	Enum	2, 3, 4, 5, 6	2

Questo controllo verifica se un Elastic Load Balancer V2 (Application, Network o Gateway Load Balancer) ha registrato istanze da almeno il numero specificato di zone di disponibilità (AZ). Il controllo fallisce se un Elastic Load Balancer V2 non ha istanze registrate almeno nel numero specificato di AZ. A meno che non si fornisca un valore di parametro personalizzato per il numero minimo di AZ, Security Hub utilizza un valore predefinito di due AZ.

Il servizio Elastic Load Balancing distribuisce automaticamente il traffico in ingresso su più destinazioni, ad esempio istanze EC2, container e indirizzi IP, in una o più zone di disponibilità.

Elastic Load Balancing ridimensiona il load balancer di volta in volta, in quanto il traffico in ingresso varia nel corso del tempo. Si consiglia di configurare almeno due zone di disponibilità per garantire la disponibilità dei servizi, poiché Elastic Load Balancer sarà in grado di indirizzare il traffico verso un'altra zona di disponibilità se una non è disponibile. La configurazione di più zone di disponibilità contribuirà a eliminare la presenza di un unico punto di errore per l'applicazione.

Correzione

Per aggiungere una zona di disponibilità a un Application Load Balancer, consulta [Availability Zones for your Application Load Balancer](#) nella User Guide for Application Load Balancer. Per aggiungere una zona di disponibilità a un Network Load Balancer, consulta [Network Load Balancer](#) nella User Guide for Network Load Balancer. Per aggiungere una zona di disponibilità a un Gateway Load Balancer, vedere [Create a Gateway Load Balancer](#) nella Guida utente per Gateway Load Balancer.

[ELB.14] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa

Requisiti correlati: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione dei dati > Integrità dei dati

Gravità: media

Tipo di risorsa: AWS::ElasticLoadBalancing::LoadBalancer

Regola AWS Config : [clb-desync-mode-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

- desyncMode: defensive, strictest (non personalizzabile)

Questo controllo verifica se un Classic Load Balancer è configurato con la modalità difensiva o la più rigorosa di mitigazione della desincronizzazione. Il controllo fallisce se il Classic Load Balancer non è configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa.

I problemi relativi a HTTP Desync possono portare al contrabbando di richieste e rendere le applicazioni vulnerabili all'avvelenamento della coda delle richieste o della cache. A loro volta, queste vulnerabilità possono portare al dirottamento delle credenziali o all'esecuzione di

comandi non autorizzati. I Classic Load Balancer configurati con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa proteggono l'applicazione dai problemi di sicurezza che potrebbero essere causati da HTTP Desync.

Correzione

Per aggiornare la modalità di mitigazione della desincronizzazione su un Classic Load Balancer, [consulta *Modify desync mitigation*](#) mode nella User Guide for Classic Load Balancer.

[ELB.16] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF

Requisiti correlati: NIST.800-53.r5 AC-4 (21)

Categoria: Proteggi > Servizi di protezione

Gravità: media

Tipo di risorsa: `AWS::ElasticLoadBalancingV2::LoadBalancer`

Regola AWS Config : [alb-waf-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un Application Load Balancer è associato a una lista di controllo degli accessi AWS WAF classica o AWS WAF Web (Web ACL). Il controllo fallisce se il `Enabled` campo per la AWS WAF configurazione è impostato su `false`

AWS WAF è un firewall per applicazioni Web che aiuta a proteggere le applicazioni Web e le API dagli attacchi. Con AWS WAF, puoi configurare un ACL Web, ovvero un insieme di regole che consentono, bloccano o contano le richieste Web in base a regole e condizioni di sicurezza Web personalizzabili da te definite. Ti consigliamo di associare l'Application Load Balancer a AWS WAF un ACL Web per proteggerlo da attacchi dannosi.

Correzione

Per associare un Application Load Balancer a un ACL Web, consulta [Associating or dissociating a Web ACL con una risorsa nella Developer Guide](#). AWS AWS WAF

Controlli Amazon EMR

Questi controlli sono correlati alle risorse Amazon EMR.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici

Requisiti correlati: PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.2, PCI DSS versione 3.2.1/1.3.4, PCI DSS versione 3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20) 3.5 SC-7 (21), NIT 800-53.r5 SC-7 (3), NIT 800-53.5 SC-7 (4), NIT 800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: AWS::EMR::Cluster

Regola AWS Config : [emr-master-no-public-ip](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se i nodi master sui cluster Amazon EMR hanno indirizzi IP pubblici. Il controllo fallisce se gli indirizzi IP pubblici sono associati a una qualsiasi delle istanze del nodo master.

Gli indirizzi IP pubblici sono indicati nel `PublicIp` campo della `NetworkInterfaces` configurazione dell'istanza. Questo controllo controlla solo i cluster Amazon EMR che si trovano in uno `RUNNING` stato o `WAITING`

Correzione

Durante l'avvio, puoi controllare se alla tua istanza in una sottorete predefinita o non predefinita viene assegnato un indirizzo IPv4 pubblico. Per impostazione predefinita, le sottoreti predefinite hanno questo attributo impostato su `true`. Le sottoreti non predefinite hanno l'attributo di indirizzamento

pubblico IPv4 impostato su `false`, a meno che non sia stato creato dalla procedura guidata di avvio dell'istanza di Amazon EC2. In tal caso, l'attributo è impostato su `true`

Dopo il lancio, non puoi dissociare manualmente un indirizzo IPv4 pubblico dalla tua istanza.

Per correggere un risultato non riuscito, è necessario avviare un nuovo cluster in un VPC con una sottorete privata con l'attributo di indirizzamento pubblico IPv4 impostato su `false`. Per istruzioni, consulta [Launch clusters in un VPC](#) nella Amazon EMR Management Guide.

[EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Protezione > Gestione sicura degli accessi > Risorsa non accessibile al pubblico

Severità: critica

Tipo di risorsa: AWS:::Account

Regola AWS Config : [emr-block-public-access](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se il tuo account è configurato con l'accesso pubblico a blocchi di Amazon EMR. Il controllo fallisce se l'impostazione di blocco dell'accesso pubblico non è abilitata o se è consentita una porta diversa dalla porta 22.

L'accesso pubblico a blocchi di Amazon EMR impedisce l'avvio di un cluster in una sottorete pubblica se il cluster ha una configurazione di sicurezza che consente il traffico in entrata da indirizzi IP pubblici su una porta. Quando un utente dal tuo Account AWS avvia un cluster, Amazon EMR controlla le regole delle porte nel gruppo di sicurezza per il cluster e le confronta con le regole del traffico in entrata. Se per il gruppo di sicurezza è impostata una regola in entrata che consente l'apertura delle porte agli indirizzi IP pubblici IPv4 0.0.0.0/0 o IPv6: :/0 e tali porte non sono specificate come eccezioni per il tuo account, Amazon EMR non consente all'utente di creare il cluster.

Note

Il blocco dell'accesso pubblico è abilitato per impostazione predefinita. Per aumentare la protezione degli account, ti consigliamo di mantenerlo abilitato.

Correzione

Per configurare l'accesso pubblico a blocchi per Amazon EMR, consulta Using [Amazon EMR block public access nella](#) Amazon EMR Management Guide.

Controlli Elasticsearch

Questi controlli sono correlati alle risorse Elasticsearch.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[ES.1] I domini Elasticsearch devono avere la crittografia a riposo abilitata

Requisiti correlati: PCI DSS versione 3.2.1/3.4, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 .800-53,5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::Elasticsearch::Domain

Regola AWS Config : [elasticsearch-encrypted-at-rest](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se nei domini Elasticsearch è abilitata la configurazione Encryption at Rest. Il controllo non riesce se la crittografia dei dati inattivi non è abilitata.

Per un ulteriore livello di sicurezza per i tuoi dati sensibili OpenSearch, dovresti configurarli in modo che vengano crittografati quando sono inattivi. OpenSearch I domini Elasticsearch offrono la crittografia dei dati archiviati. La funzionalità consente di AWS KMS archiviare e gestire le chiavi di

crittografia. Per eseguire la crittografia, utilizza l'algoritmo Advanced Encryption Standard con chiavi a 256 bit (AES-256).

Per ulteriori informazioni sulla OpenSearch crittografia a riposo, consulta [Encryption of data at rest for Amazon OpenSearch Service](#) nella Amazon OpenSearch Service Developer Guide.

Alcuni tipi di istanze, come `t.small` et `.medium`, non supportano la crittografia dei dati inattivi. Per i dettagli, consulta la sezione [Tipi di istanze supportati](#) nella Amazon OpenSearch Service Developer Guide.

Correzione

Per abilitare la crittografia a riposo per i domini Elasticsearch nuovi ed esistenti, consulta [Enabling encryption of data at rest nella](#) Amazon OpenSearch Service Developer Guide.

[ES.2] I domini Elasticsearch non devono essere accessibili al pubblico

Requisiti correlati: PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.2, PCI DSS versione 3.2.1/1.3.4, PCI DSS versione 3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20) 3.5 SC-7 (21), NIT 800-53.r5 SC-7 (3), NIT 800-53.5 SC-7 (4), NIT 800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete sicura > Risorse all'interno del VPC

Severità: critica

Tipo di risorsa: AWS::Elasticsearch::Domain

Regola AWS Config : [elasticsearch-in-vpc-only](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se i domini Elasticsearch si trovano in un VPC. Non valuta la configurazione del routing della sottorete VPC per determinare l'accesso pubblico. È necessario assicurarsi che i domini Elasticsearch non siano collegati a sottoreti pubbliche. Consulta [le politiche basate sulle risorse](#) nella Amazon OpenSearch Service Developer Guide. È inoltre necessario assicurarsi che il VPC sia configurato in base alle procedure consigliate. Consulta [le best practice di sicurezza per il tuo VPC](#) nella Amazon VPC User Guide.

I domini Elasticsearch distribuiti all'interno di un VPC possono comunicare con le risorse VPC sulla rete AWS privata, senza la necessità di attraversare la rete Internet pubblica. Questa configurazione aumenta il livello di sicurezza limitando l'accesso ai dati in transito. I VPC forniscono una serie di controlli di rete per proteggere l'accesso ai domini Elasticsearch, inclusi ACL di rete e gruppi di sicurezza. Security Hub consiglia di migrare i domini Elasticsearch pubblici su VPC per sfruttare questi controlli.

Correzione

Se si crea un dominio con un endpoint pubblico, non è possibile inserirlo in un VPC in un secondo momento. Devi invece creare un nuovo dominio ed eseguire la migrazione dei dati. È vero anche il contrario. Se si crea un dominio all'interno di un VPC, non può avere un endpoint pubblico. È invece necessario [creare un altro dominio](#) o disabilitare questo controllo.

Consulta [Lanciare i tuoi domini Amazon OpenSearch Service all'interno di un VPC nella](#) Amazon OpenSearch Service Developer Guide.

[ES.3] I domini Elasticsearch devono crittografare i dati inviati tra i nodi

Requisiti correlati: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (1) -53,5 SC-8 (2)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: AWS::Elasticsearch::Domain

Regola AWS Config : [elasticsearch-node-to-node-encryption-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un dominio Elasticsearch ha node-to-node la crittografia abilitata. Il controllo fallisce se il dominio Elasticsearch non ha la crittografia abilitata. node-to-node Il controllo produce risultati non riusciti anche se una versione di Elasticsearch non supporta i controlli di crittografia. node-to-node

HTTPS (TLS) può essere utilizzato per impedire a potenziali aggressori di intercettare o manipolare il traffico di rete utilizzando attacchi simili. person-in-the-middle Devono essere consentite solo le

connessioni crittografate tramite HTTPS (TLS). L'abilitazione della node-to-node crittografia per i domini Elasticsearch garantisce che le comunicazioni all'interno del cluster siano crittografate in transito.

Questa configurazione può comportare un calo delle prestazioni. È necessario conoscere e testare il compromesso in termini di prestazioni prima di attivare questa opzione.

Correzione

Per informazioni sull'attivazione della node-to-node crittografia su domini nuovi ed esistenti, consulta [node-to-nodeEnabling encryption](#) nella Amazon OpenSearch Service Developer Guide.

[ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIS.800-53.R 5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Categoria: Identificazione - Registrazione

Gravità: media

Tipo di risorsa: AWS::Elasticsearch::Domain

Regola AWS Config : [elasticsearch-logs-to-cloudwatch](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `logtype = 'error'` (non personalizzabile)

Questo controllo verifica se i domini Elasticsearch sono configurati per inviare log di errori a Logs. CloudWatch

È necessario abilitare i log degli errori per i domini Elasticsearch e inviarli a Logs per la conservazione e la risposta. CloudWatch I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

Correzione

Per informazioni su come abilitare la pubblicazione dei log, consulta [Enabling log publishing \(console\)](#) nella Amazon OpenSearch Service Developer Guide.

[ES.5] I domini Elasticsearch devono avere la registrazione di controllo abilitata

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIS.800-53.R 5 SI-4 (20), NID 800-53.R 5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::Elasticsearch::Domain

AWS Config regola: elasticsearch-audit-logging-enabled (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

- `cloudWatchLogsLogGroupArnList`(non personalizzabile). Security Hub non inserisce questo parametro. Elenco separato da virgole di gruppi di CloudWatch log che devono essere configurati per i log di controllo.

Questa regola si applica NON_COMPLIANT se il gruppo di log CloudWatch Logs del dominio Elasticsearch non è specificato in questo elenco di parametri.

Questo controllo verifica se i domini Elasticsearch hanno la registrazione di controllo abilitata. Questo controllo ha esito negativo se un dominio Elasticsearch non ha la registrazione di controllo abilitata.

I log di controllo sono altamente personalizzabili. Ti consentono di tenere traccia delle attività degli utenti sui tuoi cluster Elasticsearch, inclusi i successi e gli errori di autenticazione, le richieste, le modifiche all' OpenSearchindice e le query di ricerca in arrivo.

Correzione

Per istruzioni dettagliate sull'abilitazione dei log di controllo, consulta [Enabling audit logs](#) nella Amazon OpenSearch Service Developer Guide.

[ES.6] I domini Elasticsearch devono avere almeno tre nodi di dati

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::Elasticsearch::Domain

AWS Config regola: `elasticsearch-data-node-fault-tolerance` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i domini Elasticsearch sono configurati con almeno tre nodi di dati e lo è. `zoneAwarenessEnabled true`

Un dominio Elasticsearch richiede almeno tre nodi di dati per un'elevata disponibilità e tolleranza agli errori. L'implementazione di un dominio Elasticsearch con almeno tre nodi di dati garantisce le operazioni del cluster in caso di guasto di un nodo.

Correzione

Per modificare il numero di nodi di dati in un dominio Elasticsearch

1. Apri la console OpenSearch di Amazon Service all'[indirizzo https://console.aws.amazon.com/aos/](https://console.aws.amazon.com/aos/).
2. In Domini, scegli il nome del dominio che desideri modificare.
3. Scegli Modifica dominio.
4. In Nodi di dati, imposta Numero di nodi su un numero maggiore o uguale a 3.

Per tre implementazioni con zone di disponibilità, imposta un multiplo di tre per garantire una distribuzione equa tra le zone di disponibilità.

5. Scegli Invia.

[ES.7] I domini Elasticsearch devono essere configurati con almeno tre nodi master dedicati

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::Elasticsearch::Domain

AWS Config regola: elasticsearch-primary-node-fault-tolerance (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i domini Elasticsearch sono configurati con almeno tre nodi primari dedicati. Questo controllo ha esito negativo se il dominio non utilizza nodi primari dedicati. Questo controllo viene eseguito se i domini Elasticsearch hanno cinque nodi primari dedicati. Tuttavia, l'utilizzo di più di tre nodi primari potrebbe non essere necessario per mitigare il rischio di disponibilità e comportare costi aggiuntivi.

Un dominio Elasticsearch richiede almeno tre nodi primari dedicati per l'elevata disponibilità e la tolleranza agli errori. Le risorse dedicate dei nodi primari possono essere esaurite durante le implementazioni blu/verdi dei nodi dati perché ci sono nodi aggiuntivi da gestire. L'implementazione di un dominio Elasticsearch con almeno tre nodi primari dedicati garantisce una capacità sufficiente delle risorse del nodo primario e le operazioni del cluster in caso di guasto di un nodo.

Correzione

Per modificare il numero di nodi primari dedicati in un dominio OpenSearch

1. Apri la console OpenSearch di Amazon Service all'[indirizzo https://console.aws.amazon.com/aos/](https://console.aws.amazon.com/aos/).
2. In Domini, scegli il nome del dominio che desideri modificare.
3. Scegli Modifica dominio.

4. In Nodi master dedicati, imposta il tipo di istanza sul tipo di istanza desiderato.
5. Imposta il numero di nodi master pari o superiore a tre.
6. Scegli Invia.

[ES.8] Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS

Requisiti correlati: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: AWS::Elasticsearch::Domain

AWS Config regola: `elasticsearch-https-required` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un endpoint del dominio Elasticsearch è configurato per utilizzare la politica di sicurezza TLS più recente. Il controllo fallisce se l'endpoint del dominio Elasticsearch non è configurato per utilizzare la politica supportata più recente o se HTTPS non è abilitato. L'ultima politica di sicurezza TLS attualmente supportata è `Policy-Min-TLS-1-2-PFS-2023-10`

HTTPS (TLS) può essere utilizzato per impedire a potenziali aggressori di utilizzare person-in-the-middle o attacchi simili per intercettare o manipolare il traffico di rete. Devono essere consentite solo le connessioni crittografate tramite HTTPS (TLS). La crittografia dei dati in transito può influire sulle prestazioni. È consigliabile testare l'applicazione con questa funzionalità per comprendere il profilo delle prestazioni e l'impatto del TLS. TLS 1.2 offre diversi miglioramenti della sicurezza rispetto alle versioni precedenti di TLS.

Correzione

Per abilitare la crittografia TLS, utilizzate l'operazione [UpdateDomainConfig](#) API per configurare l'oggetto. [DomainEndpointOptions](#) Questo imposta il `TLSecurityPolicy`

[ES.9] I domini Elasticsearch devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Elasticsearch::Domain`

AWS Config regola: `tagged-elasticsearch-domain` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un dominio Elasticsearch ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il dominio non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il dominio non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un dominio Elasticsearch, consulta [Working with tags](#) nella Amazon OpenSearch Service Developer Guide.

EventBridge Controlli Amazon

Questi controlli sono correlati alle EventBridge risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[EventBridge.2] i bus EventBridge degli eventi devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::Events::EventBus

AWS Config regola: tagged-events-eventbus (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un bus di EventBridge eventi Amazon ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il bus degli eventi non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il bus di eventi non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un bus di EventBridge eventi, consulta i [EventBridge tag Amazon](#) nella Amazon EventBridge User Guide.

[EventBridge.3] i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata

Requisiti correlati: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 R5 AC-6 (3)

Categoria: Protezione > Gestione sicura degli accessi > Configurazione della politica delle risorse

Gravità: bassa

Tipo di risorsa: AWS::Events::EventBus

Regola AWS Config : [custom-schema-registry-policy-attached](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se a un bus di eventi EventBridge personalizzato Amazon è associata una policy basata sulle risorse. Questo controllo fallisce se il bus di eventi personalizzato non dispone di una politica basata sulle risorse.

Per impostazione predefinita, a un bus di eventi EventBridge personalizzato non è associata una policy basata sulle risorse. Ciò consente ai responsabili dell'account di accedere al bus degli eventi. Allegando una policy basata sulle risorse al bus degli eventi, è possibile limitare l'accesso al bus degli eventi a determinati account, nonché concedere intenzionalmente l'accesso alle entità in un altro account.

Correzione

Per allegare una policy basata sulle risorse a un bus di eventi EventBridge personalizzato, consulta [Managing event bus permissions nella Amazon User Guide](#). EventBridge

[EventBridge.4] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::Events::Endpoint

Regola AWS Config : [global-endpoint-event-replication-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la replica degli eventi è abilitata per un endpoint EventBridge globale Amazon. Il controllo fallisce se la replica degli eventi non è abilitata per un endpoint globale.

Gli endpoint globali aiutano a rendere l'applicazione tollerante ai guasti regionali. Innanzitutto, devi assegnare un controllo dell'integrità Amazon Route 53 all'endpoint. Quando viene avviato il failover, il controllo dello stato segnala uno stato «non integro». Entro pochi minuti dall'avvio del failover, tutti gli eventi personalizzati vengono instradati a un router di eventi nella Regione secondaria e vengono elaborati da tale router di eventi. Quando utilizzi endpoint globali, puoi abilitare la replica degli eventi. La replica degli eventi invia tutti gli eventi personalizzati ai router di eventi nelle Regioni primarie e secondarie utilizzando regole gestite. Si consiglia di abilitare la replica degli eventi durante la configurazione degli endpoint globali. La replica degli eventi consente di verificare la corretta configurazione degli endpoint globali. La replica degli eventi è necessaria per il ripristino automatico da un evento di failover. Se non hai abilitato la replica degli eventi, dovrai reimpostare manualmente il controllo di integrità della Route 53 su «integro» prima che gli eventi vengano reindirizzati alla regione principale.

Note

Se utilizzi bus di eventi personalizzati, avrai bisogno di un bus pari personalizzato in ogni regione con lo stesso nome e nello stesso account affinché il failover funzioni correttamente. L'abilitazione della replica degli eventi può aumentare i costi mensili. Per informazioni sui prezzi, consulta la pagina [EventBridge dei prezzi di Amazon](#).

Correzione

Per abilitare la replica degli eventi per gli endpoint EventBridge globali, consulta [Create a global endpoint](#) nella Amazon EventBridge User Guide. Per la replica degli eventi, seleziona Replica degli eventi abilitata.

Controlli Amazon FSx

Questi controlli sono correlati alle risorse Amazon FSx.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::FSx::FileSystem

Regola AWS Config : [fsx-openzfs-copy-tags-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un file system Amazon FSx for OpenZFS è configurato per copiare i tag su backup e volumi. Il controllo fallisce se il file system OpenZFS non è configurato per copiare i tag su backup e volumi.

L'identificazione e l'inventario delle risorse IT sono un aspetto importante della governance e della sicurezza. I tag consentono di classificare AWS le risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Ciò è utile quando si hanno molte risorse dello stesso tipo perché è possibile identificare rapidamente una risorsa specifica in base ai tag che le sono stati assegnati.

Correzione

Per configurare un file system FSx for OpenZFS per copiare i tag su backup e volumi, consulta [Updating a file system nella](#) Amazon FSx OpenZFS User Guide.

[FSX.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup

Requisiti correlati: NIST.800-53.r5 CP-9, NIST.800-53.r5 CM-8

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::FSx::FileSystem

Regola AWS Config : [fsx-lustre-copy-tags-to-backups](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un file system Amazon FSx for Lustre è configurato per copiare tag su backup e volumi. Il controllo fallisce se il file system Lustre non è configurato per copiare i tag su backup e volumi.

L'identificazione e l'inventario delle risorse IT sono un aspetto importante della governance e della sicurezza. I tag consentono di classificare AWS le risorse in diversi modi, ad esempio per scopo, proprietario o ambiente. Ciò è utile quando si hanno molte risorse dello stesso tipo perché è possibile identificare rapidamente una risorsa specifica in base ai tag che le sono stati assegnati.

Correzione

Per configurare un file system FSx for Lustre per copiare i tag nei backup, [consulta Aggiornamento di un file system](#) nella Amazon FSx OpenZFS User Guide.

AWS Global Accelerator controlli

Questi controlli sono correlati alle risorse di Global Accelerator.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[GlobalAccelerator.1] Gli acceleratori Global Accelerator devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::GlobalAccelerator::Accelerator`

AWS Config regola: `tagged-globalaccelerator-accelerator` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un AWS Global Accelerator acceleratore ha tag con i tasti specifici definiti nel parametro `requiredTagKeys`. Il controllo fallisce se l'acceleratore non ha alcuna chiave tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'acceleratore non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un acceleratore globale Global Accelerator, consulta la sezione [Tagging in nella AWS Global Accelerator Developer Guide](#).AWS Global Accelerator

AWS Glue controlli

Questi controlli sono correlati alle AWS Glue risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[Glue.1] i AWS Glue lavori devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::Glue::Job

AWS Config regola: tagged-glue-job (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfano	Nessun valore predefinito

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se un AWS Glue lavoro ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il lavoro non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il lavoro non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un AWS Glue lavoro, consulta i [AWS tag AWS Glue nella Guida](#) per l'AWS Glue utente.

GuardDuty Controlli Amazon

Questi controlli sono correlati alle GuardDuty risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[GuardDuty.1] GuardDuty dovrebbe essere abilitato

Requisiti correlati: PCI DSS versione 3.2.1/11.4, NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AU-6 (1), NIST.800-53.r5 AU-6 (5), NIST.800-53.r5 CA-7, NIST.800-53.r5 CM-8 (3), NIST.800-53.r5 RA-3 (4), NIST.800-53.r5 SA-11 (1), NIST.800-53.r5 SA-11 (6), NIST.800-53.r5 SA-15 (2), NIST.800-53.R5 SA-15 (8), NIST.800-53.R5 SA-8 (19), NIST.800-53.R5 SA-8 (21), NIST.800-53.r5 SA-8 (21) 25), NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-5 (1), NIST.800-53.r5 SC-5 (3), NIST.800-53.r5 SI-20, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4 (1), nIST. 800-53,5 SI-4 (13), NITS 800-53 .r5 SI-4 (2), NIS.800-53.r5 SI-4 (22), NIS.800-53.r5 SI-4 (25), NIS.800-53.r5 SI-4 (4), NIT 800-53.r5 SI-4 (5)

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: AWS : : : Account

Regola AWS Config : [guardduty-enabled-centralized](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se Amazon GuardDuty è abilitato nel tuo GuardDuty account e nella tua regione.

Si consiglia vivamente di abilitarlo GuardDuty in tutte le AWS regioni supportate. In questo modo è possibile GuardDuty generare informazioni su attività non autorizzate o insolite, anche nelle regioni che non vengono utilizzate attivamente. Ciò consente anche GuardDuty di monitorare CloudTrail eventi globali Servizi AWS come IAM.

Correzione

Per risolvere questo problema, abiliti. GuardDuty

Per i dettagli su come abilitare GuardDuty, incluso come utilizzare per AWS Organizations gestire più account, consulta la Guida [introduttiva alla GuardDuty](#) Amazon GuardDuty User Guide.

[GuardDuty.2] GuardDuty i filtri devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::GuardDuty::Filter`

AWS Config regola: `tagged-guardduty-filter` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un GuardDuty filtro Amazon ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il filtro non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il filtro non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una

singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un GuardDuty filtro, [TagResource](#) consulta Amazon GuardDuty API Reference.

[GuardDuty.3] Gli GuardDuty IPSet devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::GuardDuty::IPSet

AWS Config regola: tagged-guardduty-ipset (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un Amazon GuardDuty IPSet ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se l'IPSet non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'IPSet non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un GuardDuty IPSet, consulta [TagResource](#) Amazon GuardDuty API Reference.

[GuardDuty.4] i GuardDuty rilevatori devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::GuardDuty::Detector`

AWS Config regola: `tagged-guardduty-detector` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un GuardDuty rilevatore Amazon dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il rilevatore non dispone di chiavi tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se il rilevatore non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un GuardDuty rilevatore, consulta [TagResource](#) Amazon GuardDuty API Reference.

AWS Identity and Access Management controlli

Questi controlli sono correlati alle risorse IAM.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[IAM.1] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi

Requisiti correlati: PCI DSS versione 3.2.1/7.2.1, benchmark CIS Foundations versione 1.2.0/1.22, benchmark CIS AWS Foundations versione 1.4.0/1.16, NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (15) R5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2), NIST.800-53.r5 AC-6 (3) AWS

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: alta

Tipo di risorsa: AWS::IAM::Policy

Regola AWS Config : [iam-policy-no-statements-with-admin-access](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `excludePermissionBoundaryPolicy: true`(non personalizzabile)

Questo controllo verifica se la versione predefinita delle politiche IAM (note anche come politiche gestite dai clienti) dispone dell'accesso come amministratore includendo un'istruzione "Effect":

"Allow" con "Action": "*" over "Resource": "*". Il controllo fallisce se si dispone di politiche IAM con una dichiarazione di questo tipo.

Il controllo verifica solo le policy gestite dal cliente create dall'utente. Non verifica le politiche in linea e AWS gestite.

Le politiche IAM definiscono una serie di privilegi concessi a utenti, gruppi o ruoli. Seguendo i consigli di sicurezza standard, si AWS consiglia di concedere il privilegio minimo, il che significa concedere solo le autorizzazioni necessarie per eseguire un'attività. Quando si forniscono privilegi amministrativi completi anziché il set di autorizzazioni minimo di cui l'utente ha bisogno, si espongono le risorse a operazioni potenzialmente indesiderate.

Anziché consentire privilegi di amministratore completi, determina ciò che gli utenti devono fare e crea le policy su misura che permettono agli utenti di eseguire solo tali attività. È più sicuro iniziare con un set di autorizzazioni minimo e concedere autorizzazioni aggiuntive quando necessario. Non iniziare con autorizzazioni troppo permissive e cercare di limitarle in un secondo momento.

È necessario rimuovere le policy IAM che hanno una dichiarazione "Effect": "Allow" con "Action": "*" over "Resource": "*"

Note

AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per modificare le policy IAM in modo che non consentano i privilegi amministrativi «*» completi, consulta [Modifica delle policy IAM](#) nella IAM User Guide.

[IAM.2] Gli utenti IAM non devono avere policy IAM allegare

Requisiti correlati: PCI DSS versione 3.2.1/7.2.1, benchmark CIS Foundations versione 3.0.0/1.15, benchmark CIS AWS Foundations versione 1.2.0/1.16, NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (15) 5 AC-3 (7), NIST 800-53.R 5 AC-6, NIST.800-53R5 AC-6 (3) AWS

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: bassa

Tipo di risorsa: AWS::IAM::User

Regola AWS Config : [iam-user-no-policies-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se gli utenti IAM hanno delle policy allegate. Il controllo fallisce se gli utenti IAM hanno delle policy allegate. Gli utenti IAM devono invece ereditare le autorizzazioni dai gruppi IAM o assumere un ruolo.

Per impostazione predefinita, gli utenti, i gruppi e i ruoli IAM non hanno accesso alle AWS risorse. Le policy IAM concedono privilegi a utenti, gruppi o ruoli. Ti consigliamo di applicare le policy IAM direttamente ai gruppi e ai ruoli ma non agli utenti. L'assegnazione di privilegi a livello di gruppo o ruolo riduce la complessità di gestione degli accessi, se il numero di utenti cresce. La riduzione della complessità di gestione degli accessi potrebbe a sua volta ridurre l'opportunità per un principale di ricevere o mantenere inavvertitamente privilegi eccessivi.

Note

Gli utenti IAM creati da Amazon Simple Email Service vengono creati automaticamente utilizzando policy in linea. Security Hub esonera automaticamente questi utenti da questo controllo.

AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per risolvere questo problema, [crea un gruppo IAM](#) e allega la policy al gruppo. Quindi, [aggiungi gli utenti al gruppo](#). La policy viene applicata a ogni utente nel gruppo. Per rimuovere una policy collegata direttamente a un utente, consulta [Aggiungere e rimuovere le autorizzazioni di identità IAM](#) nella Guida per l'utente IAM.

[IAM.3] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno

Requisiti correlati: benchmark CIS AWS Foundations v3.0.0/1.14, benchmark CIS AWS Foundations v1.4.0/1.14, benchmark CIS AWS Foundations v1.2.0/1.4, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), NIST.800-53.r5 AC-3 (15)

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS :: IAM :: User

Regola AWS Config : [access-keys-rotated](#)

Tipo di pianificazione: periodica

Parametri:

- maxAccessKeyAge: 90 (non personalizzabile)

Questo controllo verifica se le chiavi di accesso attive vengono ruotate entro 90 giorni.

Ti consigliamo vivamente di non generare e rimuovere tutte le chiavi di accesso nell'account. Invece, la best practice consigliata consiste nel creare uno o più ruoli IAM o utilizzare la [federazione](#) tramite AWS IAM Identity Center. Puoi utilizzare questi metodi per consentire agli utenti di accedere a AWS Management Console e AWS CLI.

Ogni approccio ha i suoi casi d'uso. La federazione è generalmente la soluzione migliore per le aziende che dispongono di una directory centrale esistente o che prevedono di aver bisogno di più del limite attuale per gli utenti IAM. Le applicazioni eseguite all'esterno di un AWS ambiente necessitano di chiavi di accesso per l'accesso programmatico alle AWS risorse.

Tuttavia, se le risorse che richiedono l'accesso programmatico vengono eseguite all'interno AWS, la migliore pratica consiste nell'utilizzare i ruoli IAM. I ruoli consentono di concedere l'accesso a una risorsa senza codificare l'ID chiave di accesso e la chiave di accesso segreta nella configurazione.

Per ulteriori informazioni sulla protezione delle chiavi di accesso e dell'account, consulta [le migliori pratiche per la gestione delle chiavi di AWS accesso](#) nei Riferimenti generali di AWS. Consulta anche il post del blog [Linee guida per proteggere l'utente Account AWS durante l'utilizzo dell'accesso programmatico](#).

Se disponi già di una chiave di accesso, Security Hub consiglia di ruotare le chiavi di accesso ogni 90 giorni. La rotazione delle chiavi di accesso riduce la possibilità di utilizzo di una chiave di accesso associata a un account compromesso o chiuso. Garantisce inoltre che i dati non possano essere accessibili con una vecchia chiave che potrebbe essere stata persa, decifrata o rubata. Aggiorna sempre le applicazioni dopo aver ruotato le chiavi di accesso.

Le chiavi di accesso sono composte da un ID chiave di accesso e una chiave di accesso segreta. Vengono utilizzate per firmare le richieste programmatiche inviate dall'utente. AWS Gli utenti hanno bisogno delle proprie chiavi di accesso per effettuare chiamate programmatiche AWS da Tools for Windows PowerShell, dagli AWS SDK o chiamate HTTP dirette utilizzando le operazioni API per singoli utenti. AWS CLI Servizi AWS

Se la tua organizzazione utilizza AWS IAM Identity Center (IAM Identity Center), i tuoi utenti possono accedere ad Active Directory, a una directory IAM Identity Center integrata o a [un altro provider di identità \(IdP\) connesso a IAM Identity Center](#). Possono quindi essere mappati su un ruolo IAM che consente loro di eseguire AWS CLI comandi o richiamare operazioni AWS API senza la necessità di chiavi di accesso. Per ulteriori informazioni, consulta [Configurazione dell'uso AWS IAM Identity Center nella Guida AWS CLI per l'AWS Command Line Interface utente](#).

Note

AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per ruotare le chiavi di accesso più vecchie di 90 giorni, consulta [Rotating access keys](#) nella IAM User Guide. Segui le istruzioni per qualsiasi utente con una chiave di accesso di età superiore a 90 giorni.

[IAM.4] La chiave di accesso utente root IAM non dovrebbe esistere

Requisiti correlati: benchmark CIS AWS Foundations versione 3.0.0/1.4, benchmark CIS Foundations versione 1.4.0/1.4, benchmark CIS AWS Foundations versione 1.2.0/1.12, PCI DSS versione 3.2.1/2.1, PCI DSS versione 3.2.1/2.2, PCI DSS versione 3.2.1/7.2.1, NIST.800-53.r5 AWS AC-2 (1),

NIST.800-53.r5 AC-3 (15)), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Categoria: Protezione > Gestione degli accessi sicuri

Severità: critica

Tipo di risorsa: AWS:::Account

Regola AWS Config : [iam-root-access-key-check](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se è presente la chiave di accesso dell'utente root.

L'utente root è l'utente con più privilegi in un Account AWS. AWS le chiavi di accesso forniscono l'accesso programmatico a un determinato account.

Security Hub consiglia di rimuovere tutte le chiavi di accesso associate all'utente root. Ciò limita i vettori che possono essere utilizzati per compromettere l'account. Incoraggia inoltre la creazione e l'utilizzo di account basati sul ruolo che dispongono di meno privilegi.

Correzione

Per eliminare la chiave di accesso dell'utente root, consulta [Eliminazione delle chiavi di accesso per l'utente root](#) nella IAM User Guide. Per eliminare le chiavi di accesso dell'utente root da un Account AWS ingresso AWS GovCloud (US), consulta [Eliminazione delle chiavi di accesso dell'utente root del mio AWS GovCloud \(US\) account nella Guida](#) per l'AWS GovCloud (US) utente.

[IAM.5] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console

Requisiti correlati: benchmark CIS AWS Foundations versione 3.0.0/1.10, benchmark CIS AWS Foundations versione 1.4.0/1.10, benchmark CIS AWS Foundations versione 1.2.0/1.2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (2)), NIST 800-53.r5 IA-2 (6), NIST 800-53.r5 IA-2 (8)

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS::IAM::User

Regola AWS Config : [mfa-enabled-for-iam-console-access](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se l'AWS autenticazione a più fattori (MFA) è abilitata per tutti gli utenti IAM che utilizzano una password della console.

L'autenticazione a più fattori (MFA) aggiunge un ulteriore livello di protezione al di sopra di nome utente e password. Con l'MFA abilitata, quando un utente accede a un AWS sito Web, gli vengono richiesti il nome utente e la password. Inoltre, viene richiesto loro un codice di autenticazione dal dispositivo AWS MFA.

Ti consigliamo di abilitare MFA per tutti gli account che dispongono di una password della console. MFA è progettato per fornire una maggiore sicurezza per l'accesso alla console. L'entità principal di autenticazione deve possedere un dispositivo che genera una chiave legata al fattore tempo e deve essere a conoscenza delle credenziali.

Note

AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per aggiungere MFA per gli utenti IAM, consulta [Using Multi-Factor Authentication \(MFA\) AWS nella IAM User Guide](#).

Offriamo una chiave di sicurezza MFA gratuita ai clienti idonei. [Verifica se sei idoneo e ordina la tua chiave gratuita](#).

[IAM.6] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root

Requisiti correlati: benchmark CIS AWS Foundations v3.0.0/1.6, benchmark CIS Foundations v1.4.0/1.6, benchmark CIS AWS Foundations v1.2.0/1.14, PCI DSS v3.2.1/8.3.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), nIST.800-53.r5 800-53.r5 IA-2 (2), NIST 800-53.r5 IA-2 (6), NIST 800-53.r5 IA-2 (8) AWS

Categoria: Protezione > Gestione degli accessi sicuri

Severità: critica

Tipo di risorsa: AWS :: Account

Regola AWS Config : [root-account-hardware-mfa-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se l'utente Account AWS è abilitato a utilizzare un dispositivo hardware di autenticazione a più fattori (MFA) per accedere con le credenziali dell'utente root. Il controllo fallisce se l'MFA non è abilitata o se alcuni dispositivi MFA virtuali sono autorizzati ad accedere con le credenziali dell'utente root.

Di conseguenza, un dispositivo MFA virtuale potrebbe non offrire lo stesso livello di sicurezza di un dispositivo hardware MFA. È consigliabile utilizzare solo un dispositivo MFA virtuale nell'attesa dell'approvazione di un acquisto hardware o della consegna del dispositivo hardware. Per saperne di più, consulta [Enabling a virtual multi-factor authentication \(MFA\) device \(console\)](#) nella IAM User Guide.

Sia i token Time-based One-Time Password (TOTP) che i token Universal 2nd Factor (U2F) sono validi come opzioni MFA hardware.

Correzione

Per aggiungere un dispositivo MFA hardware per l'utente root, consulta [Abilitare un dispositivo MFA hardware per l'utente Account AWS root \(console\)](#) nella Guida per l'utente IAM.

Offriamo una chiave di sicurezza MFA gratuita ai clienti idonei. [Verifica se sei idoneo e ordina la tua chiave gratuita.](#)

[IAM.7] Le politiche relative alle password per gli utenti IAM dovrebbero avere configurazioni solide

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-5 (1)

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS:::Account

Regola AWS Config : [iam-password-policy](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
RequireUppercaseCharacters	Richiede almeno un carattere maiuscolo nella password	Booleano	true o false	true
RequireLowercaseCharacters	Richiede almeno un carattere minuscolo nella password	Booleano	true o false	true
RequireSymbols	Richiede almeno un simbolo nella password	Booleano	true o false	true
RequireNumbers	Richiedi almeno un numero nella password	Booleano	true o false	true
MinimumPasswordLength	Numero minimo di caratteri nella password	Numero intero	8 Da a 128	8
PasswordReusePrevention	Numero di rotazioni della password prima che una vecchia password possa essere riutilizzata	Numero intero	12 Da a 24	Nessun valore predefinito
MaxPasswordAge	Numero di giorni prima della scadenza della password	Numero intero	1 Da a 90	Nessun valore predefinito

Questo controllo verifica se la politica sulle password degli account per gli utenti IAM utilizza configurazioni complesse. Il controllo fallisce se la politica delle password non utilizza configurazioni complesse. A meno che non si forniscano valori di parametro personalizzati, Security Hub utilizza i valori predefiniti menzionati nella tabella precedente. I `MaxPasswordAge` parametri `PasswordReusePrevention` and non hanno un valore predefinito, quindi se si escludono questi parametri, Security Hub ignora il numero di rotazioni della password e l'età della password durante la valutazione di questo controllo.

Per accedere a AWS Management Console, gli utenti IAM necessitano di password. Come best practice, Security Hub consiglia vivamente di utilizzare la federazione anziché creare utenti IAM. La federazione consente agli utenti di utilizzare le proprie credenziali aziendali esistenti per accedere a AWS Management Console Utilizza AWS IAM Identity Center (IAM Identity Center) per creare o federare l'utente, quindi assumi un ruolo IAM in un account.

Per ulteriori informazioni sui provider di identità e sulla federazione, consulta [Provider di identità e federazione](#) nella Guida per l'utente IAM. Per ulteriori informazioni su IAM Identity Center, consulta la [Guida AWS IAM Identity Center per l'utente](#).

Se devi utilizzare utenti IAM, Security Hub consiglia di imporre la creazione di password utente complesse. È possibile impostare una politica in materia di password Account AWS per specificare i requisiti di complessità e i periodi di rotazione obbligatori per le password. Quando si crea o si modifica una politica in materia di password, la maggior parte delle impostazioni relative alle password viene applicata alla successiva modifica delle password da parte degli utenti. Alcune impostazioni vengono applicate immediatamente.

Correzione

Per aggiornare la politica sulle password, consulta [Impostazione di una politica di password dell'account per gli utenti IAM](#) nella Guida per l'utente IAM.

[IAM.8] Le credenziali utente IAM non utilizzate devono essere rimosse

Requisiti correlati: PCI DSS versione 3.2.1/8.1.4, CIS AWS Foundations Benchmark versione 1.2.0/1.3, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-2 (3), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (15) R5 AC-3 (7), NIST.800-53R5 AC-6

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS::IAM::User

Regola AWS Config : [iam-user-unused-credentials-check](#)

Tipo di pianificazione: periodica

Parametri:

- `maxCredentialUsageAge: 90` (non personalizzabile)

Questo controllo verifica se gli utenti IAM dispongono di password o chiavi di accesso attive che non vengono utilizzate da 90 giorni.

Gli utenti IAM possono accedere alle AWS risorse utilizzando diversi tipi di credenziali, come password o chiavi di accesso.

Security Hub consiglia di rimuovere o disattivare tutte le credenziali che non sono state utilizzate per 90 giorni o più. La disabilitazione o la rimozione di credenziali non necessarie riduce la finestra di opportunità per le credenziali associate a un account compromesso o abbandonato da utilizzare.

Note

AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Quando visualizzi le informazioni sull'utente nella console IAM, ci sono colonne relative all'età della chiave di accesso, all'età della password e all'ultima attività. Se il valore in una di queste colonne è maggiore di 90 giorni, rendi inattive le credenziali per tali utenti.

Puoi anche utilizzare i [report sulle credenziali](#) per monitorare gli utenti e identificare quelli che non svolgono alcuna attività per 90 o più giorni. Puoi scaricare i report sulle credenziali in .csv formato dalla console IAM.

Dopo aver identificato gli account inattivi o le credenziali non utilizzate, disattivali. Per istruzioni, consulta [Creazione, modifica o eliminazione di una password utente IAM \(console\) nella Guida per l'utente IAM](#).

[IAM.9] L'MFA deve essere abilitata per l'utente root

Requisiti correlati: PCI DSS versione 3.2.1/8.3.1, benchmark CIS Foundations versione 3.0.0/1.5, benchmark CIS AWS Foundations versione 1.4.0/1.5, benchmark CIS AWS Foundations v1.2.0/1.13, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), nIST.800-53.r5 IA-2 (1), nIST.800-53.r5 800-53.r5 IA-2 (2), NIST 800-53.r5 IA-2 (6), NIST 800-53.r5 IA-2 (8) AWS

Categoria: Protezione > Gestione degli accessi sicuri

Severità: critica

Tipo di risorsa: AWS : : : Account

Regola AWS Config : [root-account-mfa-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

L'utente root ha accesso completo a tutti i servizi e le risorse di un Account AWS file. MFA aggiunge un ulteriore livello di protezione su nome utente e password. Con l'MFA abilitata, quando un utente accede a AWS Management Console, gli vengono richiesti il nome utente e la password e un codice di autenticazione dal dispositivo AWS MFA.

Quando si utilizza l'MFA virtuale per l'utente root, CIS consiglia che il dispositivo utilizzato non sia un dispositivo personale. Al contrario, utilizza un dispositivo mobile dedicato (tablet o telefono) che mantieni carico e protetto indipendentemente da qualsiasi dispositivo personale singolo. Questo diminuisce i rischi di perdita dell'accesso alla MFA a causa della perdita del dispositivo, permuta del dispositivo o se il proprietario del dispositivo non è più impiegato presso l'azienda.

Correzione

Per abilitare la MFA per l'utente root, consulta Attivare la [MFA sull'utente Account AWS root](#) nella Guida di riferimento per la gestione dell'AWS account.

[IAM.10] Le politiche relative alle password per gli utenti IAM dovrebbero avere durate elevate AWS Config

Requisiti correlati: PCI DSS v3.2.1/8.1.4, PCI DSS v3.2.1/8.2.3, PCI DSS v3.2.1/8.2.4, PCI DSS v3.2.1/8.2.5

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS:::Account

Regola AWS Config : [iam-password-policy](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la politica delle password degli account per gli utenti IAM utilizza le seguenti configurazioni PCI DSS minime.

- `RequireUppercaseCharacters`— Richiede almeno un carattere maiuscolo nella password. L'impostazione predefinita è `true`.
- `RequireLowercaseCharacters`— Richiede almeno un carattere minuscolo nella password. L'impostazione predefinita è `true`.
- `RequireNumbers`— Richiedi almeno un numero nella password. L'impostazione predefinita è `true`.
- `MinimumPasswordLength`— Lunghezza minima della password. (Impostazione predefinita = 7 o più)
- `PasswordReusePrevention`— Numero di password prima di consentirne il riutilizzo. (Impostazione predefinita = 4)
- `MaxPasswordAge` — Numero di giorni prima della scadenza della password. (Impostazione predefinita = 90)

Correzione

Per aggiornare la politica delle password per utilizzare la configurazione consigliata, consulta [Impostazione di una politica di password dell'account per gli utenti IAM](#) nella Guida per l'utente IAM.

[IAM.11] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola

Requisiti correlati: CIS Foundations Benchmark v1.2.0/1.5 AWS

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS:::Account

Regola AWS Config : [iam-password-policy](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Le policy sulle password applicano, in parte, requisiti di conformità delle password. Utilizza le politiche di gestione delle password di IAM per assicurarti che le password utilizzino set di caratteri diversi.

Il CIS consiglia che la politica delle password richieda almeno una lettera maiuscola. L'impostazione di una policy di complessità delle password aumenta la resilienza dell'account a fronte di tentativi di accesso di forza bruta.

Correzione

Per modificare la politica relativa alle password, consulta [Impostazione di una politica di password dell'account per gli utenti IAM nella Guida](#) per l'utente IAM. Per la sicurezza della password, seleziona Richiedi almeno una lettera maiuscola dell'alfabeto latino (A—Z).

[IAM.12] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola

Requisiti correlati: CIS Foundations Benchmark v1.2.0/1.6 AWS

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS:::Account

Regola AWS Config : [iam-password-policy](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Le policy sulle password applicano, in parte, requisiti di conformità delle password. Utilizza le politiche di gestione delle password di IAM per assicurarti che le password utilizzino set di caratteri diversi. Il CIS consiglia che la politica delle password richieda almeno una lettera minuscola. L'impostazione di una policy di complessità delle password aumenta la resilienza dell'account a fronte di tentativi di accesso di forza bruta.

Correzione

Per modificare la politica relativa alle password, consulta [Impostazione di una politica di password dell'account per gli utenti IAM nella Guida](#) per l'utente IAM. Per la sicurezza della password, seleziona Richiedi almeno una lettera minuscola dell'alfabeto latino (A—Z).

[IAM.13] Assicurati che la politica delle password IAM richieda almeno un simbolo

Requisiti correlati: CIS Foundations Benchmark AWS v1.2.0/1.7

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS :: Account

Regola AWS Config : [iam-password-policy](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Le policy sulle password applicano, in parte, requisiti di conformità delle password. Utilizza le politiche di gestione delle password di IAM per assicurarti che le password utilizzino set di caratteri diversi.

Il CIS raccomanda che la politica delle password richieda almeno un simbolo. L'impostazione di una policy di complessità delle password aumenta la resilienza dell'account a fronte di tentativi di accesso di forza bruta.

Correzione

Per modificare la politica relativa alle password, consulta [Impostazione di una politica di password dell'account per gli utenti IAM](#) nella Guida per l'utente IAM. Per la sicurezza della password, seleziona Richiedi almeno un carattere non alfanumerico.

[IAM.14] Assicurati che la politica delle password IAM richieda almeno un numero

Requisiti correlati: CIS Foundations Benchmark AWS v1.2.0/1.8

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS :: Account

Regola AWS Config : [iam-password-policy](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Le policy sulle password applicano, in parte, requisiti di conformità delle password. Utilizza le politiche di gestione delle password di IAM per assicurarti che le password utilizzino set di caratteri diversi.

Il CIS consiglia che la politica delle password richieda almeno un numero. L'impostazione di una policy di complessità delle password aumenta la resilienza dell'account a fronte di tentativi di accesso di forza bruta.

Correzione

Per modificare la politica relativa alle password, consulta [Impostazione di una politica di password dell'account per gli utenti IAM](#) nella Guida per l'utente IAM. Per la sicurezza della password, seleziona Richiedi almeno un numero.

[IAM.15] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14

Requisiti correlati: CIS Foundations Benchmark v3.0.0/1.8, CIS AWS Foundations Benchmark v1.4.0/1.8, CIS AWS Foundations Benchmark v1.2.0/1.9 AWS

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS :: Account

Regola AWS Config : [iam-password-policy](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Le policy sulle password applicano, in parte, requisiti di conformità delle password. Utilizza le politiche di gestione delle password di IAM per assicurarti che le password abbiano almeno una determinata lunghezza.

Il CIS raccomanda che la politica delle password richieda una lunghezza minima della password di 14 caratteri. L'impostazione di una policy di complessità delle password aumenta la resilienza dell'account a fronte di tentativi di accesso di forza bruta.

Correzione

Per modificare la politica relativa alle password, consulta [Impostazione di una politica di password dell'account per gli utenti IAM](#) nella Guida per l'utente IAM. Per la lunghezza minima della password, inserisci **14** o un numero maggiore.

[IAM.16] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password

Requisiti correlati: CIS Foundations Benchmark v3.0.0/1.9, CIS AWS Foundations Benchmark v1.4.0/1.9, CIS Foundations Benchmark v1.2.0/1.10 AWS AWS

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: bassa

Tipo di risorsa: AWS:::Account

Regola AWS Config : [iam-password-policy](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se il numero di password da ricordare è impostato su 24. Il controllo ha esito negativo se il valore non è 24.

Le policy di gestione delle password di IAM possono impedire il riutilizzo di una determinata password da parte dello stesso utente.

Il CIS raccomanda che la politica in materia di password impedisca il riutilizzo delle password. Impedire il riutilizzo delle password consente di incrementare la resilienza dell'account rispetto a tentativi di accesso di forza bruta.

Correzione

Per modificare la politica relativa alle password, consulta [Impostazione di una politica di password dell'account per gli utenti IAM nella Guida](#) per l'utente IAM. Per impedire il riutilizzo della password, inserisci `24`.

[IAM.17] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno

Requisiti correlati: CIS Foundations Benchmark v1.2.0/1.11 AWS

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: bassa

Tipo di risorsa: AWS :: Account

Regola AWS Config : [iam-password-policy](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Le policy relative alle password di IAM possono richiedere che le password vengano ruotate o scadute dopo un determinato numero di giorni.

Il CIS consiglia che la politica in materia di password faccia scadere le password dopo 90 giorni o meno. La riduzione della durata della password aumenta la resilienza dell'account contro tentativi di accesso di forza bruta. Richiedere le modifiche regolari delle password è utile nelle seguenti situazioni:

- Le password possono essere rubate o compromesse senza saperlo. Questo può accadere tramite compromissione del sistema, vulnerabilità del software o minacce interne.

- Alcuni filtri Web aziendali e governativi o server proxy sono in grado di intercettare e registrare il traffico anche se è criptato.
- Molte persone utilizzano la stessa password per molti sistemi diversi come lavoro, e-mail e personale.
- Workstation dell'utente finale compromesse potrebbero includere un keystroke logger.

Correzione

Per modificare la politica relativa alle password, consulta [Impostazione di una politica di password dell'account per gli utenti IAM nella Guida](#) per l'utente IAM. Per attivare la scadenza della password, inserisci **90** o un numero inferiore.

[IAM.18] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support

Requisiti correlati: CIS Foundations Benchmark v3.0.0/1.17, CIS AWS Foundations Benchmark v1.4.0/1.17, CIS Foundations Benchmark v1.2.0/1.20 AWS AWS

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: bassa

Tipo di risorsa: AWS:::Account

Regola AWS Config : [iam-policy-in-use](#)

Tipo di pianificazione: periodica

Parametri:

- policyARN: arn:*partition*:iam::aws:policy/AWSSupportAccess (non personalizzabile)
- policyUsageType: ANY (non personalizzabile)

AWS fornisce un centro di supporto che può essere utilizzato per la notifica e la risposta agli incidenti, nonché per il supporto tecnico e il servizio clienti.

Crea un ruolo IAM per consentire agli utenti autorizzati di gestire gli incidenti con AWS Support. Implementando il privilegio minimo per il controllo degli accessi, un ruolo IAM richiederà una policy

IAM appropriata per consentire l'accesso al centro di supporto per gestire gli incidenti con. AWS Support

Note

AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per risolvere questo problema, crea un ruolo che consenta agli utenti autorizzati di gestire gli AWS Support incidenti.

Per creare il ruolo da utilizzare per l'accesso AWS Support

1. Aprire la console IAM all'indirizzo <https://console.aws.amazon.com/iam/>.
2. Nel riquadro di navigazione IAM, scegli Ruoli, quindi scegli Crea ruolo.
3. Per Tipo di ruolo, scegli Altro Account AWS.
4. Per ID account, inserisci l' Account AWS ID Account AWS a cui desideri concedere l'accesso alle tue risorse.

Se gli utenti o i gruppi che assumeranno questo ruolo si trovano nello stesso account, immettere il numero di account locale.

Note

L'amministratore dell'account specificato può concedere l'autorizzazione di assumere questo ruolo a qualsiasi utente in tale account. Per eseguire questa operazione, l'amministratore collega una policy all'utente o al gruppo che garantisce l'autorizzazione per l'operazione `sts:AssumeRole`. In tale policy, la risorsa deve essere l'ARN del ruolo.

5. Scegli Successivo: autorizzazioni.
6. Cercare la policy gestita `AWSSupportAccess`.
7. Selezionare la casella di controllo per la policy gestita `AWSSupportAccess`.

8. Scegli Successivo: Tag.
9. (Facoltativo) Per aggiungere metadati al ruolo, allega i tag come coppie chiave-valore.

Per ulteriori informazioni sull'utilizzo dei tag in IAM, vedere [Tagging di utenti e ruoli IAM](#) nella Guida per l'utente di IAM.

10. Scegli Prossimo: Rivedi.
11. In Nome ruolo, immetti un nome per il ruolo.

I nomi dei ruoli devono essere univoci all'interno del tuo Account AWS. Non rispettano la distinzione tra maiuscole e minuscole.

12. (Facoltativo) In Descrizione ruolo, immettere una descrizione per il nuovo ruolo.
13. Verificare il ruolo e scegliere Create role (Crea ruolo).

[IAM.19] L'MFA deve essere abilitata per tutti gli utenti IAM

Requisiti correlati: PCI DSS versione 3.2.1/8.3.1, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 IA-2 (1), NIST.800-53.r5 IA-2 (2), NIST.800-53.r5 IA-2 (6), NIST.800-53.r5 IA-2 (8)

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS::IAM::User

Regola AWS Config : [iam-user-mfa-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se gli utenti IAM hanno abilitato l'autenticazione a più fattori (MFA).

Note

AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per aggiungere MFA per gli utenti IAM, consulta [Enabling MFA devices for users AWS nella IAM User Guide](#).

[IAM.20] Evita l'uso dell'utente root

Important

Security Hub ha ritirato questo controllo nell'aprile 2024. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: CIS Foundations Benchmark AWS v1.2.0/1.1

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: bassa

Tipo di risorsa: AWS::IAM::User

AWS Config regola: use-of-root-account-test (regola Security Hub personalizzata)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un Account AWS ha restrizioni sull'utilizzo dell'utente root. Il controllo valuta le seguenti risorse:

- Argomenti su Amazon Simple Notification Service (Amazon SNS)
- AWS CloudTrail sentieri
- Filtri metrici associati ai sentieri CloudTrail
- CloudWatch Allarmi Amazon basati sui filtri

Questo controllo determina se FAILED una o più delle seguenti affermazioni sono vere:

- Non esistono CloudTrail percorsi nell'account.

- Un CloudTrail percorso è abilitato, ma non configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura.
- Un CloudTrail trail è abilitato, ma non è associato a un gruppo di CloudWatch log Logs.
- Il filtro metrico esatto prescritto dal Center for Internet Security (CIS) non viene utilizzato. Il filtro metrico prescritto è. `'{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent"}'`
- Nell' CloudWatch account non sono presenti allarmi basati sul filtro metrico.
- CloudWatch gli allarmi configurati per inviare notifiche all'argomento SNS associato non si attivano in base alla condizione di allarme.
- L'argomento SNS non è conforme ai [vincoli per l'invio di un messaggio a un argomento SNS](#).
- L'argomento SNS non ha almeno un sottoscrittore.

Questo controllo determina NO_DATA se una o più delle seguenti affermazioni sono vere:

- Un percorso multiregionale ha sede in una regione diversa. Security Hub può generare risultati solo nella regione in cui si trova il percorso.
- Un percorso multiregionale appartiene a un account diverso. Security Hub può generare risultati solo per l'account proprietario del percorso.

Questo controllo determina WARNING se una o più delle seguenti affermazioni sono vere:

- L'account corrente non possiede l'argomento SNS a cui si fa riferimento nell' CloudWatch avviso.
- L'account corrente non ha accesso all'argomento SNS quando richiama l'API SNS.
`ListSubscriptionsByTopic`

Note

Ti consigliamo di utilizzare gli itinerari organizzativi per registrare gli eventi di molti account di un'organizzazione. Gli itinerari organizzativi sono percorsi multiregionali per impostazione predefinita e possono essere gestiti solo dall'account di AWS Organizations gestione o dall'account amministratore CloudTrail delegato. L'utilizzo di un percorso organizzativo comporta lo stato di controllo NO_DATA per i controlli valutati negli account dei membri dell'organizzazione. Negli account dei membri, Security Hub genera risultati solo per le risorse di proprietà dei membri. I risultati relativi agli itinerari organizzativi vengono generati

nell'account del proprietario della risorsa. Puoi visualizzare questi risultati nel tuo account amministratore delegato di Security Hub utilizzando l'aggregazione tra regioni.

Come best practice, utilizzare le credenziali dell'utente root solo quando necessario per [eseguire attività di gestione degli account e](#) dei servizi. Applica le policy IAM direttamente ai gruppi e ai ruoli, ma non agli utenti. Per istruzioni sulla configurazione di un amministratore per l'uso quotidiano, consulta [Creazione del primo utente e gruppo di amministratori IAM](#) nella Guida per l'utente IAM.

Correzione

I passaggi per risolvere questo problema includono la configurazione di un argomento di Amazon SNS, CloudTrail un percorso, un filtro metrico e un allarme per il filtro metrico.

Come creare un argomento Amazon SNS

1. Apri la console Amazon SNS all'indirizzo <https://console.aws.amazon.com/sns/v3/home>.
2. Crea un argomento Amazon SNS che riceva tutti gli allarmi CIS.

Creare almeno un sottoscrittore all'argomento. Per ulteriori informazioni, consulta [Nozioni di base su Amazon SNS](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

Quindi, configura un attivo CloudTrail che si applichi a tutte le regioni. A questo scopo, seguire le fasi di correzione in [the section called “\[CloudTrail.1\] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura”](#).

Prendi nota del nome del gruppo di log CloudWatch Logs che associ al CloudTrail percorso. Crea il filtro metrico per quel gruppo di log.

Infine, crea il filtro metrico e l'allarme.

Per creare un filtro parametri e allarme

1. Apri la CloudWatch console all'indirizzo <https://console.aws.amazon.com/cloudwatch/>.
2. Nel pannello di navigazione, selezionare Log groups (Gruppi di log).
3. Seleziona la casella di controllo per il gruppo di log CloudWatch Logs associato al CloudTrail percorso che hai creato.
4. Da Azioni, scegli Crea filtro metrico.
5. In Definisci modello, procedi come segue:

- a. Copiare il seguente modello e incollarlo nel campo Filter Pattern (Modello di filtro).

```
{$.userIdentity.type="Root" && $.userIdentity.invokedBy NOT EXISTS && $.eventType != "AwsServiceEvent"}
```

- b. Seleziona Successivo.
6. In Assegna metrica, effettuate le seguenti operazioni:
 - a. In Nome filtro, inserisci un nome per il filtro metrico.
 - b. Per Metric Namespace, inserisci **LogMetrics**

Se utilizzi lo stesso namespace per tutti i filtri delle metriche dei log CIS, tutte le metriche di CIS Benchmark vengono raggruppate insieme.
 - c. Per Metric Name, inserisci un nome per la metrica. Ricorda il nome della metrica. Dovrai selezionare la metrica quando crei l'allarme.
 - d. In Metric value (Valore parametro), inserisci **1**.
 - e. Seleziona Successivo.
 7. In Rivedi e crea, verifica le informazioni che hai fornito per il nuovo filtro metrico. Quindi, scegli Crea filtro metrico.
 8. Nel riquadro di navigazione, scegli Gruppi di log, quindi scegli il filtro che hai creato in Filtri metrici.
 9. Seleziona la casella di controllo per il filtro. Scegli Crea allarme.
 10. In Specificare metriche e condizioni, procedi come segue:
 - a. In Condizioni, per Soglia, scegli Statico.
 - b. Per Definire la condizione di allarme, scegli Maggiore/Uguale.
 - c. Per Definire il valore di soglia, immettere **1**
 - d. Seleziona Successivo.
 11. In Configura azioni, procedi come segue:
 - a. In Attivazione dello stato di allarme, scegli In allarme.
 - b. In Select an SNS topic (Seleziona un argomento SNS), scegli Select an existing SNS topic (Seleziona un argomento SNS esistente).
 - c. In Invia una notifica a, inserisci il nome dell'argomento SNS creato nella procedura precedente.

- d. Seleziona Successivo.
12. In Aggiungi nome e descrizione, inserisci un nome e una descrizione per l'avviso, ad esempio **CIS-1.1-RootAccountUsage**. Quindi scegli Successivo.
13. In Anteprima e crea, rivedi la configurazione dell'allarme. Quindi scegli Crea allarme.

[IAM.21] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi

Requisiti correlati: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 R5 AC-6 (10), NIST.800-53R5 AC-6 (2), NIST.800-53.5 AC-6 (3)

Categoria: Rileva > Gestione sicura degli accessi

Gravità: bassa

Tipo di risorsa: AWS::IAM::Policy

Regola AWS Config : [iam-policy-no-statements-with-full-access](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `excludePermissionBoundaryPolicy`: True (non personalizzabile)

Questo controllo verifica se le policy basate sull'identità IAM che crei dispongono di istruzioni Allow che utilizzano la wildcard * per concedere le autorizzazioni per tutte le azioni su qualsiasi servizio.

Il controllo ha esito negativo se una dichiarazione di policy include with. "Effect": "Allow"
"Action": "Service:*"

Ad esempio, la seguente dichiarazione in una politica dà come risultato un risultato non riuscito.

```
"Statement": [  
  {  
    "Sid": "EC2-Wildcard",  
    "Effect": "Allow",  
    "Action": "ec2:*",  
    "Resource": "*"
```



```
}
```

Il controllo ha esito negativo anche se si utilizza "Effect": "Allow" con "NotAction": "**service**:*". In tal caso, l'NotAction elemento fornisce l'accesso a tutte le azioni di un Servizio AWS, ad eccezione delle azioni specificate in NotAction.

Questo controllo si applica solo alle politiche IAM gestite dal cliente. Non si applica alle policy IAM gestite da AWS.

Quando si assegnano le autorizzazioni a Servizi AWS, è importante definire l'ambito delle azioni IAM consentite nelle politiche IAM. È necessario limitare le azioni IAM solo alle azioni necessarie. Questo ti aiuta a fornire i permessi con privilegi minimi. Politiche eccessivamente permissive potrebbero portare a un aumento dei privilegi se le policy sono collegate a un principale IAM che potrebbe non richiedere l'autorizzazione.

In alcuni casi, potresti voler consentire azioni IAM con un prefisso simile, come e. DescribeFlowLogs DescribeAvailabilityZones In questi casi autorizzati, puoi aggiungere un carattere jolly con suffisso al prefisso comune. Ad esempio, ec2:Describe*.

Questo controllo passa se si utilizza un'azione IAM con prefisso e un carattere jolly con suffisso. Ad esempio, la seguente dichiarazione in una politica restituisce un risultato positivo.

```
"Statement": [  
  {  
    "Sid": "EC2-Wildcard",  
    "Effect": "Allow",  
    "Action": "ec2:Describe*",  
    "Resource": "*" } ]
```

Raggruppando le azioni IAM correlate in questo modo, puoi anche evitare di superare i limiti di dimensione delle policy IAM.

Note

AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub. Tuttavia, la registrazione globale delle risorse può essere abilitata in una singola regione. Se si registrano solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Per risolvere questo problema, aggiorna le policy IAM in modo che non consentano i privilegi amministrativi «*» completi. Per i dettagli su come modificare una policy IAM, consulta [Modifica delle policy IAM](#) nella IAM User Guide.

[IAM.22] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse

Requisiti correlati: CIS Foundations Benchmark v3.0.0/1.12, CIS AWS Foundations Benchmark v1.4.0/1.12 AWS

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS::IAM::User

AWS Config regola: [iam-user-unused-credentials-check](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se gli utenti IAM dispongono di password o chiavi di accesso attive che non vengono utilizzate da 45 giorni o più. A tal fine, verifica se il `maxCredentialUsageAge` parametro della AWS Config regola è uguale o superiore a 45.

Gli utenti possono accedere alle AWS risorse utilizzando diversi tipi di credenziali, come password o chiavi di accesso.

Il CIS consiglia di rimuovere o disattivare tutte le credenziali che non sono state utilizzate per 45 giorni o più. La disabilitazione o la rimozione di credenziali non necessarie riduce la finestra di opportunità per le credenziali associate a un account compromesso o abbandonato da utilizzare.

La AWS Config regola per questo controllo utilizza le operazioni [GetCredentialReport](#) e [GenerateCredentialReport](#) API, che vengono aggiornate solo ogni quattro ore. Le modifiche agli utenti IAM possono richiedere fino a quattro ore per essere visibili a questo controllo.

Note

AWS Config deve essere abilitato in tutte le regioni in cui si utilizza Security Hub. Tuttavia, è possibile abilitare la registrazione delle risorse globali in una singola regione. Se si registrano

solo risorse globali in una singola area, è possibile disabilitare questo controllo in tutte le aree, ad eccezione dell'area in cui si registrano le risorse globali.

Correzione

Quando visualizzi le informazioni sull'utente nella console IAM, ci sono colonne relative all'età della chiave di accesso, all'età della password e all'ultima attività. Se il valore in una di queste colonne è superiore a 45 giorni, rendi inattive le credenziali di tali utenti.

Puoi anche utilizzare i [report sulle credenziali](#) per monitorare gli utenti e identificare quelli che non svolgono alcuna attività per 45 o più giorni. Puoi scaricare i report sulle credenziali in .csv formato dalla console IAM.

Dopo aver identificato gli account inattivi o le credenziali non utilizzate, disattivali. Per istruzioni, consulta [Creazione, modifica o eliminazione di una password utente IAM \(console\) nella Guida per l'utente IAM](#).

[IAM.23] Gli analizzatori IAM Access Analyzer devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::AccessAnalyzer::Analyzer

AWS Config regola: tagged-accessanalyzer-analyzer (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	una distinzione tra lettere maiuscole e minuscole.			

Questo controllo verifica se un analizzatore gestito da AWS Identity and Access Management Access Analyzer (IAM Access Analyzer) dispone di tag con le chiavi specifiche definite nel parametro.

`requiredTagKeys` Il controllo fallisce se l'analizzatore non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'analizzatore non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un analizzatore, consulta [TagResourceAWS](#) IAM Access Analyzer API Reference.

[IAM.24] I ruoli IAM devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::IAM::Role

AWS Config regola: tagged-iam-role (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un ruolo AWS Identity and Access Management (IAM) ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il ruolo non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il ruolo non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una

singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un ruolo IAM, consulta [Tagging IAM resources nella IAM](#) User Guide.

[IAM.25] Gli utenti IAM devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::IAM::User

AWS Config regola: tagged-iam-user (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un utente AWS Identity and Access Management (IAM) dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se l'utente non dispone di alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'utente non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un utente IAM, consulta [Tagging IAM resources nella IAM](#) User Guide.

[IAM.26] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi

Requisiti correlati: CIS Foundations Benchmark v3.0.0/1.19 AWS

Categoria: Identificazione > Conformità

Gravità: media

Tipo di risorsa: `AWS::IAM::ServerCertificate`

AWS Config regola: [iam-server-certificate-expiration-check](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un certificato del server SSL/TLS attivo gestito in IAM è scaduto. Il controllo fallisce se il certificato del server SSL/TLS scaduto non viene rimosso.

Per abilitare le connessioni HTTPS al sito Web o all'applicazione in AWS, è necessario un certificato del server SSL/TLS. Puoi utilizzare IAM o AWS Certificate Manager (ACM) per archiviare e distribuire i certificati del server. Utilizza IAM come gestore di certificati solo quando devi supportare connessioni HTTPS in un ambiente Regione AWS non supportato da ACM. IAM crittografa in modo sicuro le chiavi private e archivia la versione crittografata nella memoria dei certificati SSL di IAM. IAM supporta la distribuzione di certificati server in tutte le regioni, ma è necessario ottenere il certificato da un provider esterno per utilizzarlo con. AWS Non puoi caricare un certificato ACM su IAM. Inoltre, non puoi gestire i tuoi certificati dalla console IAM. La rimozione dei certificati SSL/TLS scaduti elimina il rischio che un certificato non valido venga distribuito accidentalmente su una risorsa, il che può danneggiare la credibilità dell'applicazione o del sito Web sottostanti.

Correzione

Per rimuovere un certificato server da IAM, consulta [Managing server certificates in IAM](#) nella IAM User Guide.

[IAM.27] Le identità IAM non devono avere la policy allegata
AWSCloudShellFullAccess

Requisiti correlati: CIS AWS Foundations Benchmark v3.0.0/1.22

Categoria: Protezione > Gestione sicura degli accessi > Policy IAM sicure

Gravità: media

Tipo di risorsa:AWS::IAM::Role,AWS::IAM::User,AWS::IAM::Group

AWS Config regola: [iam-policy-blacklisted-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

- «Policyarns»: «arn:aws:iam: :aws:policy/, arn:aws-cn:iam: :aws:policy/, arn :iam: AWSCloudShellFullAccess :aws:policy/» AWSCloudShellFullAccess aws-us-gov AWSCloudShellFullAccess

Questo controllo verifica se a un'identità IAM (utente, ruolo o gruppo) è associata la policy gestita. `AWS AWSCloudShellFullAccess` Il controllo fallisce se a un'identità IAM è associata la `AWSCloudShellFullAccess` policy.

AWS CloudShell fornisce un modo conveniente per eseguire i comandi CLI. Servizi AWS La policy `AWS AWSCloudShellFullAccess` fornisce l'accesso completo a CloudShell, che consente la funzionalità di caricamento e download di file tra il sistema locale dell'utente e l' CloudShell ambiente. All'interno dell' CloudShell ambiente, un utente dispone delle autorizzazioni `sudo` e può accedere a Internet. Di conseguenza, l'associazione di questa policy gestita a un'identità IAM offre loro la possibilità di installare software per il trasferimento di file e spostare i dati CloudShell da server Internet esterni. Ti consigliamo di seguire il principio del privilegio minimo e di assegnare autorizzazioni più limitate alle tue identità IAM.

Correzione

Per scollegare la `AWSCloudShellFullAccess` policy da un'identità IAM, consulta [Aggiungere e rimuovere le autorizzazioni di identità IAM nella Guida per l'utente IAM](#).

[IAM.28] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato

Requisiti correlati: CIS Foundations Benchmark v3.0.0/1.20 AWS

Categoria: Rileva > Servizi di rilevamento > Monitoraggio dell'utilizzo privilegiato

Gravità: alta

Tipo di risorsa: `AWS::AccessAnalyzer::Analyzer`

AWS Config regola: [iam-external-access-analyzer-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un Account AWS ha un analizzatore di accesso esterno IAM Access Analyzer abilitato. Il controllo fallisce se l'account non ha un analizzatore di accesso esterno abilitato nell'area attualmente selezionata. Regione AWS

Gli analizzatori di accesso esterni IAM Access Analyzer aiutano a identificare le risorse dell'organizzazione e degli account, come i bucket Amazon Simple Storage Service (Amazon S3) o i ruoli IAM, che sono condivisi con un'entità esterna. Questo ti aiuta a evitare l'accesso involontario

alle tue risorse e ai tuoi dati. IAM Access Analyzer è regionale e deve essere abilitato in ogni regione. Per identificare le risorse condivise con responsabili esterni, un analizzatore di accessi utilizza un ragionamento basato sulla logica per analizzare le politiche basate sulle risorse nel tuo ambiente. AWS Quando abiliti un analizzatore di accesso esterno, crei un analizzatore per l'intera organizzazione o l'account.

Correzione

Per abilitare un analizzatore di accesso esterno in una regione specifica, consulta [Enabling IAM Access Analyzer nella IAM User Guide](#). È necessario abilitare un analizzatore in ogni regione in cui si desidera monitorare l'accesso alle risorse.

AWS IoT controlli

Questi controlli sono correlati alle AWS IoT risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[IoT.1] i profili di AWS IoT Core sicurezza devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::IoT::SecurityProfile

AWS Config regola: tagged-iot-securityprofile (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfan	No default value

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se un profilo di AWS IoT Core sicurezza ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il profilo di sicurezza non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il profilo di sicurezza non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un profilo di AWS IoT Core sicurezza, consulta [Tagging your AWS IoT resources](#) nella Developer Guide.AWS IoT

[IoT.2] le azioni di AWS IoT Core mitigazione devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoT::MitigationAction`

AWS Config regola: `tagged-iot-mitigationaction` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un' AWS IoT Core azione di mitigazione ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se l'azione di mitigazione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'azione di mitigazione non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'azione di AWS IoT Core mitigazione, consulta [Tagging your AWS IoT resources](#) nella Developer Guide.AWS IoT

[IoT.3] le AWS IoT Core dimensioni devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::IoT::Dimension

AWS Config regola: tagged-iot-dimension (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfan	No default value

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se una AWS IoT Core dimensione ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se la dimensione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la dimensione non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una AWS IoT Core dimensione, consulta [Tagging your AWS IoT resources](#) nella Developer Guide.AWS IoT

gli AWS IoT Core autorizzatori [IoT.4] devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoT::Authorizer`

AWS Config regola: `tagged-iot-authorizer` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un AWS IoT Core autorizzatore dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se l'autorizzatore non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'autorizzatore non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un programma di AWS IoT Core autorizzazione, consulta [Tagging your AWS IoT resources](#) nella Developer Guide.AWS IoT

[IoT.5] gli alias dei AWS IoT Core ruoli devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::IoT::RoleAlias

AWS Config regola: tagged-iot-rolealias (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfan	No default value

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se un alias di AWS IoT Core ruolo ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo ha esito negativo se l'alias del ruolo non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'alias del ruolo non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un alias di AWS IoT Core ruolo, consulta [Tagging your AWS IoT resources](#) nella Developer Guide.AWS IoT

[IoT.6] AWS IoT Core le politiche devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::IoT::Policy`

AWS Config regola: `tagged-iot-policy` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se una AWS IoT Core politica ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se la policy non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la policy non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una AWS IoT Core politica, consulta [Tagging your AWS IoT resources](#) nella Developer Guide.AWS IoT

Controlli Amazon Kinesis

Questi controlli sono correlati alle risorse Kinesis.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[Kinesis.1] Gli stream Kinesis devono essere crittografati quando sono inattivi

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::Kinesis::Stream

Regola AWS Config : [kinesis-stream-encrypted](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i Kinesis Data Streams sono crittografati a riposo con la crittografia lato server. Questo controllo fallisce se un flusso Kinesis non è crittografato a riposo con la crittografia lato server.

La crittografia lato server è una funzionalità di Amazon Kinesis Data Streams che crittografa automaticamente i dati prima che siano inattivi utilizzando un. AWS KMS key I dati vengono crittografati prima di essere scritti sul livello di archiviazione del flusso Kinesis e vengono decrittografati dopo essere stati recuperati dall'archiviazione. Di conseguenza, i tuoi dati vengono crittografati quando sono inattivi all'interno del servizio Amazon Kinesis Data Streams.

Correzione

Per informazioni sull'attivazione della crittografia lato server per gli stream Kinesis, vedi [Come posso iniziare con la crittografia lato server?](#) nella Amazon Kinesis Developer Guide.

[Kinesis.2] Gli stream Kinesis devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Kinesis::Stream`

AWS Config regola: `tagged-kinesis-stream` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un flusso di dati di Amazon Kinesis contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il flusso di dati non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il flusso di dati non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un flusso di dati Kinesis, consulta [Tagging your stream in Amazon Kinesis Data Streams nella Amazon Kinesis Developer Guide](#).

AWS Key Management Service controlli

Questi controlli sono correlati alle AWS KMS risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[KMS.1] Le politiche gestite dai clienti di IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS

Requisiti correlati: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 R5 AC-6 (3)

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS::IAM::Policy

Regola AWS Config : [iam-customer-policy-blocked-kms-actions](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `blockedActionsPatterns`: `kms:ReEncryptFrom`, `kms:Decrypt`(non personalizzabile)
- `excludePermissionBoundaryPolicy`: `True` (non personalizzabile)

Verifica se la versione predefinita delle policy gestite dai clienti di IAM consente ai responsabili di utilizzare le azioni di AWS KMS decrittografia su tutte le risorse. Il controllo fallisce se la policy è sufficientemente aperta da consentire `kms:ReEncryptFrom` azioni `kms:Decrypt` o azioni su tutte le chiavi KMS.

Il controllo controlla solo le chiavi KMS nell'elemento Resource e non tiene conto di eventuali condizioni nell'elemento Condition di una politica. Inoltre, il controllo valuta le politiche gestite dal cliente sia allegate che non collegate. Non verifica le politiche in linea o AWS le politiche gestite.

Con AWS KMS, puoi controllare chi può utilizzare le tue chiavi KMS e accedere ai tuoi dati crittografati. Le policy IAM definiscono quali azioni un'identità (utente, gruppo o ruolo) può eseguire su quali risorse. Seguendo le migliori pratiche di sicurezza, AWS consiglia di concedere il privilegio minimo. In altre parole, è necessario concedere alle identità solo le `kms:ReEncryptFrom` autorizzazioni `kms:Decrypt` o e solo le chiavi necessarie per eseguire un'operazione. In caso contrario, l'utente potrebbe utilizzare chiavi non appropriate per i dati.

Invece di concedere le autorizzazioni per tutte le chiavi, stabilisci il set minimo di chiavi di cui gli utenti hanno bisogno per accedere ai dati crittografati. Quindi progetta politiche che consentano agli utenti

di utilizzare solo quelle chiavi. Ad esempio, non consentite `kms:Decrypt` l'autorizzazione su tutte le chiavi KMS. Consenti invece `kms:Decrypt` solo le chiavi in una particolare regione per il tuo account. Adottando il principio del privilegio minimo, puoi ridurre il rischio di divulgazione involontaria dei tuoi dati.

Correzione

Per modificare una policy gestita dai clienti IAM, consulta [Modifica delle policy gestite dai clienti](#) nella Guida per l'utente IAM. Quando modifichi la tua policy, per il `Resource` campo, fornisci l'Amazon Resource Name (ARN) della chiave o delle chiavi specifiche su cui desideri consentire le azioni di decrittografia.

[KMS.2] I principali IAM non devono disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS

Requisiti correlati: NIST.800-53.r5 AC-2, NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6, NIST.800-53.r5 AC-6 R5 AC-6 (3)

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa:

- `AWS::IAM::Group`
- `AWS::IAM::Role`
- `AWS::IAM::User`

Regola AWS Config : [iam-inline-policy-blocked-kms-actions](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `blockedActionsPatterns: kms:ReEncryptFrom, kms:Decrypt(non personalizzabile)`

Questo controllo verifica se le politiche in linea incorporate nelle identità IAM (ruolo, utente o gruppo) consentono le azioni di AWS KMS decrittografia e ricrittografia su tutte le chiavi KMS.

Il controllo fallisce se la policy è sufficientemente aperta da consentire azioni `kms:Decrypt` o `kms:ReEncryptFrom` su tutte le chiavi KMS.

Il controllo controlla solo le chiavi KMS nell'elemento Resource e non tiene conto di eventuali condizioni nell'elemento Condition di una politica.

Con AWS KMS, puoi controllare chi può utilizzare le tue chiavi KMS e accedere ai tuoi dati crittografati. Le policy IAM definiscono quali azioni un'identità (utente, gruppo o ruolo) può eseguire su quali risorse. Seguendo le migliori pratiche di sicurezza, AWS consiglia di concedere il privilegio minimo. In altre parole, è necessario concedere alle identità solo le autorizzazioni necessarie e solo le chiavi necessarie per eseguire un'attività. In caso contrario, l'utente potrebbe utilizzare chiavi non appropriate per i dati.

Invece di concedere l'autorizzazione per tutte le chiavi, stabilisci il set minimo di chiavi di cui gli utenti hanno bisogno per accedere ai dati crittografati. Quindi progetta politiche che consentano agli utenti di utilizzare solo quelle chiavi. Ad esempio, non consentite `kms:Decrypt` l'autorizzazione su tutte le chiavi KMS. Consenti invece l'autorizzazione solo su chiavi specifiche in una regione specifica per il tuo account. Adottando il principio del privilegio minimo, puoi ridurre il rischio di divulgazione involontaria dei tuoi dati.

Correzione

Per modificare una policy in linea IAM, consulta [Modifica delle policy in linea nella IAM User Guide](#). Quando modifichi la tua policy, per il Resource campo, fornisci l'Amazon Resource Name (ARN) della chiave o delle chiavi specifiche su cui desideri consentire le azioni di decrittografia.

[KMS.3] AWS KMS keys non deve essere eliminato involontariamente

Requisiti correlati: NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12 (2)

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Severità: critica

Tipo di risorsa: AWS::KMS::Key

AWS Config regola: `kms-cmk-not-scheduled-for-deletion-2` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se è prevista l'eliminazione delle chiavi KMS. Il controllo ha esito negativo se è pianificata l'eliminazione di una chiave KMS.

Le chiavi KMS non possono essere recuperate una volta eliminate. I dati crittografati con una chiave KMS sono inoltre permanentemente irrecuperabili se la chiave KMS viene eliminata. Se i dati importanti sono stati crittografati con una chiave KMS pianificata per l'eliminazione, prendi in considerazione la possibilità di decrittografare i dati o di ricrittografarli con una nuova chiave KMS, a meno che tu non stia eseguendo intenzionalmente una cancellazione crittografica.

Quando si pianifica l'eliminazione di una chiave KMS, viene imposto un periodo di attesa obbligatorio per consentire di annullare l'eliminazione, se è stata pianificata per errore. Il periodo di attesa predefinito è di 30 giorni, ma può essere ridotto a soli 7 giorni se è pianificata l'eliminazione della chiave KMS. Durante il periodo di attesa, l'eliminazione pianificata può essere annullata e la chiave KMS non verrà eliminata.

Per ulteriori informazioni sull'eliminazione delle chiavi KMS, consulta [Eliminazione](#) delle chiavi KMS nella Guida per gli sviluppatori.AWS Key Management Service

Correzione

Per annullare l'eliminazione pianificata di una chiave KMS, consulta [Per annullare l'eliminazione di una chiave in Pianificazione e annullamento dell'eliminazione delle chiavi](#) (console) nella Guida per gli sviluppatori.AWS Key Management Service

[KMS.4] la rotazione dei tasti dovrebbe essere abilitata AWS KMS

Requisiti correlati: PCI DSS versione 3.2.1/3.6.4, benchmark CIS Foundations versione 3.0.0/3.6, benchmark CIS AWS Foundations versione 1.4.0/3.8, benchmark CIS AWS Foundations v1.2.0/2.8, NIST.800-53.r5 SC-12, NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 AWS SC-28 (3)

Categoria: Protezione > Protezione dei dati > Crittografia di data-at-rest

Gravità: media

Tipo di risorsa: AWS :: KMS :: Key

Regola AWS Config : [cmk-backing-key-rotation-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

AWS KMS consente ai clienti di ruotare la chiave di supporto, che è materiale chiave memorizzato AWS KMS ed è legato all'ID della chiave KMS. È la chiave di supporto utilizzata per eseguire operazioni di crittografia, ad esempio la crittografia e la decrittografia. Al momento, la rotazione automatica delle chiavi conserva tutte le chiavi di supporto precedenti, in modo che la decrittografia di dati crittografati possa essere eseguita in modo trasparente.

CIS consiglia di abilitare la rotazione delle chiavi KMS. La rotazione delle chiavi di crittografia consente di ridurre l'impatto potenziale di una chiave compromessa perché i dati crittografati con una nuova chiave non sono accessibili con una chiave precedente che potrebbe essere stata esposta.

Correzione

Per abilitare la rotazione delle chiavi KMS, vedi [Come abilitare e disabilitare la rotazione automatica delle chiavi nella Guida per gli AWS Key Management Service sviluppatori](#).

AWS Lambda controlli

Questi controlli sono correlati alle risorse Lambda.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[Lambda.1] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico

Requisiti correlati: PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.2, PCI DSS versione 3.2.1/1.3.4, PCI DSS versione 3.2.1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20) R5 SC-7 (21), NIS.800-53.r5 SC-7 (3), NIS.800-53.r5 SC-7 (4), NIT 800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: AWS::Lambda::Function

Regola AWS Config : [lambda-function-public-access-prohibited](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la politica basata sulle risorse della funzione Lambda proibisce l'accesso pubblico all'esterno dell'account. Il controllo fallisce se è consentito l'accesso pubblico. Il controllo fallisce anche se una funzione Lambda viene richiamata da Amazon S3 e la policy non include una condizione per limitare l'accesso pubblico, ad esempio. `AWS:SourceAccount` Ti consigliamo di utilizzare altre condizioni S3 oltre alla tua policy sui bucket per un accesso più preciso. `AWS:SourceAccount`

La funzione Lambda non dovrebbe essere accessibile al pubblico, in quanto ciò potrebbe consentire l'accesso involontario al codice della funzione.

Correzione

Per risolvere questo problema, è necessario aggiornare la politica basata sulle risorse della funzione per rimuovere le autorizzazioni o aggiungere la condizione. `AWS:SourceAccount` Puoi aggiornare la policy basata sulle risorse solo dall'API Lambda o. AWS CLI

Per iniziare, [consulta la policy basata sulle risorse sulla console](#) Lambda. Identifica la dichiarazione politica con valori di `Principal` campo che rendono pubblica la policy, ad esempio `"*"`

```
{ "AWS": "*" }
```

Non è possibile modificare la policy dalla console. Per rimuovere le autorizzazioni dalla funzione, esegui il [remove-permission](#) comando da. AWS CLI

```
$ aws lambda remove-permission --function-name <function-name> --statement-id <statement-id>
```

Sostituisci `<function-name>` con il nome della funzione Lambda e `<statement-id>` con l'istruzione ID (`Sid`) dell'istruzione che desideri rimuovere.

[Lambda.2] Le funzioni Lambda devono utilizzare runtime supportati

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoria: Protezione > Sviluppo protetto

Gravità: media

Tipo di risorsa: `AWS::Lambda::Function`

Regola AWS Config : [lambda-function-settings-check](#)

Categoria: Protezione > Configurazione di rete protetta

Gravità: bassa

Tipo di risorsa: AWS::Lambda::Function

AWS Config regola: [lambda-inside-vpc](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una funzione Lambda è implementata in un cloud privato virtuale (VPC). Il controllo fallisce se la funzione Lambda non è distribuita in un VPC. Security Hub non valuta la configurazione del routing della sottorete VPC per determinare la raggiungibilità pubblica. È possibile che vengano visualizzati risultati non riusciti per le risorse Lambda @Edge.

L'implementazione di risorse in un VPC rafforza la sicurezza e il controllo sulle configurazioni di rete. Tali implementazioni offrono anche scalabilità e un'elevata tolleranza agli errori in più zone di disponibilità. È possibile personalizzare le implementazioni VPC per soddisfare diversi requisiti applicativi.

Correzione

Per configurare una funzione esistente per la connessione a sottoreti private nel tuo VPC, consulta [Configuring VPC access](#) nella Developer Guide.AWS Lambda Consigliamo di scegliere almeno due sottoreti private per un'elevata disponibilità e almeno un gruppo di sicurezza che soddisfi i requisiti di connettività della funzione.

[Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::Lambda::Function

Regola AWS Config : [lambda-vpc-multi-az-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
availabilityZones	Numero minimo di zone di disponibilità	Enum	2, 3, 4, 5, 6	2

Questo controllo verifica se una AWS Lambda funzione che si connette a un cloud privato virtuale (VPC) opera almeno nel numero specificato di zone di disponibilità (AZ). Il controllo fallisce se la funzione non funziona almeno nel numero specificato di AZ. A meno che non si fornisca un valore di parametro personalizzato per il numero minimo di AZ, Security Hub utilizza un valore predefinito di due AZ.

La distribuzione di risorse su più AZ è una AWS best practice per garantire un'elevata disponibilità all'interno dell'architettura. La disponibilità è un pilastro fondamentale del modello di sicurezza della triade di riservatezza, integrità e disponibilità. Tutte le funzioni Lambda che si connettono a un VPC devono disporre di un'implementazione Multi-AZ per garantire che una singola zona di errore non provochi un'interruzione totale delle operazioni.

Correzione

Se configuri la funzione per la connessione a un VPC nel tuo account, specifica le sottoreti in più AZ per garantire un'elevata disponibilità. Per istruzioni, consulta [Configurazione dell'accesso al VPC](#) nella Guida per AWS Lambda gli sviluppatori.

Lambda esegue automaticamente altre funzioni in più AZ per garantire che sia disponibile per elaborare gli eventi in caso di interruzione del servizio in una singola zona.

[Lambda.6] Le funzioni Lambda devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::Lambda::Function

AWS Config regola: tagged-lambda-function (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se una AWS Lambda funzione ha tag con i tasti specifici definiti nel parametro `requiredTagKeys`. Il controllo fallisce se la funzione non ha alcuna chiave tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se la funzione non è etichettata con alcun tasto. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una funzione Lambda, consulta [Using tags on Lambda functions](#) nella Developer Guide.AWS Lambda

Controlli Amazon Macie

Questi controlli sono correlati alle risorse di Macie.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[Macie.1] Amazon Macie dovrebbe essere abilitato

Requisiti correlati: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SI-4

Categoria: Rilevamento > Servizi di rilevamento

Gravità: media

Tipo di risorsa: AWS:::Account

Regola AWS Config : [macie-status-check](#)

Tipo di pianificazione: periodica

Questo controllo verifica se Amazon Macie è abilitato per un account. Il controllo fallisce se Macie non è abilitato per l'account.

Amazon Macie rileva i dati sensibili utilizzando l'apprendimento automatico e il pattern matching, fornisce visibilità sui rischi per la sicurezza dei dati e abilita la protezione automatizzata contro tali rischi. Macie valuta automaticamente e continuamente i bucket Amazon Simple Storage Service (Amazon S3) per la sicurezza e il controllo degli accessi e genera risultati per informarti di potenziali problemi con la sicurezza o la privacy dei tuoi dati Amazon S3. Macie automatizza anche l'individuazione e la segnalazione di dati sensibili, come le informazioni di identificazione personale (PII), per fornirti una migliore comprensione dei dati archiviati in Amazon S3. Per ulteriori informazioni, consulta la Guida per l'[utente di Amazon Macie](#).

Correzione

Per abilitare Macie, consulta [Enable Macie nella Guida](#) per l'utente di Amazon Macie.

[Macie.2] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato

Requisiti correlati: NIST.800-53.r5 CA-7, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 RA-5, NIST.800-53.r5 SA-8 (19), NIST.800-53.r5 SI-4

Categoria: Rilevamento > Servizi di rilevamento

Gravità: alta

Tipo di risorsa: AWS :: Account

Regola AWS Config : [macie-auto-sensitive-data-discovery-check](#)

Tipo di pianificazione: periodica

Questo controllo verifica se il rilevamento automatico di dati sensibili è abilitato per un account amministratore di Amazon Macie. Il controllo fallisce se il rilevamento automatico di dati sensibili non è abilitato per un account amministratore Macie. Questo controllo si applica solo agli account amministratore.

Macie automatizza il rilevamento e il reporting di dati sensibili, come le informazioni di identificazione personale (PII), nei bucket Amazon Simple Storage Service (Amazon S3). Grazie al rilevamento automatico dei dati sensibili, Macie valuta continuamente l'inventario dei bucket e utilizza tecniche di campionamento per identificare e selezionare oggetti S3 rappresentativi dai bucket. Macie analizza quindi gli oggetti selezionati, ispezionandoli alla ricerca di dati sensibili. Man mano che l'analisi procede, Macie aggiorna le statistiche, i dati di inventario e altre informazioni che fornisce sui dati S3. Macie genera anche risultati per segnalare i dati sensibili che trova.

Correzione

Per creare e configurare processi automatici di rilevamento di dati sensibili per analizzare oggetti nei bucket S3, consulta [Configurazione del rilevamento automatico di dati sensibili per il tuo account nella Guida per l'utente di Amazon Macie](#).

Controlli Amazon MSK

Questi controlli sono correlati alle risorse Amazon Managed Streaming for Apache Kafka (Amazon MSK).

Questi controlli potrebbero non essere disponibili tutti. Regioni AWS Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[MSK.1] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker

Requisiti correlati: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (1) -53,5 SC-8 (2)

Categoria: Protezione > Protezione dei dati > Crittografia di data-in-transit

Gravità: media

Tipo di risorsa: AWS::MSK::Cluster

Regola AWS Config : [msk-in-cluster-node-require-tls](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon MSK è crittografato in transito con HTTPS (TLS) tra i nodi broker del cluster. Il controllo fallisce se è abilitata la comunicazione in testo semplice per una connessione al nodo del broker del cluster.

HTTPS offre un ulteriore livello di sicurezza in quanto utilizza TLS per spostare i dati e può essere utilizzato per impedire a potenziali aggressori di utilizzare person-in-the-middle o simili attacchi per intercettare o manipolare il traffico di rete. Per impostazione predefinita, Amazon MSK crittografa i dati in transito con TLS. Tuttavia, puoi ignorare questa impostazione predefinita al momento della creazione del cluster. Consigliamo di utilizzare connessioni crittografate tramite HTTPS (TLS) per le connessioni ai nodi del broker.

Correzione

Per aggiornare le impostazioni di crittografia per i cluster MSK, consulta [Aggiornamento delle impostazioni di sicurezza di un cluster](#) nella Amazon Managed Streaming for Apache Kafka Developer Guide.

[MSK.2] Per i cluster MSK dovrebbe essere configurato un monitoraggio avanzato

Requisiti correlati: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa: AWS::MSK::Cluster

Regola AWS Config : [msk-enhanced-monitoring-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon MSK ha configurato il monitoraggio avanzato, specificato da un livello di monitoraggio di almeno `PER_TOPIC_PER_BROKER`. Il controllo fallisce se il livello di monitoraggio per il cluster è impostato su `DEFAULT` o `PER_BROKER`.

Il livello di `PER_TOPIC_PER_BROKER` monitoraggio fornisce informazioni più dettagliate sulle prestazioni del cluster MSK e fornisce anche metriche relative all'utilizzo delle risorse, come l'utilizzo della CPU e della memoria. Ciò consente di identificare i punti deboli in termini di prestazioni e i modelli di utilizzo delle risorse per singoli argomenti e broker. Questa visibilità, a sua volta, può ottimizzare le prestazioni dei vostri broker Kafka.

Correzione

Per configurare il monitoraggio avanzato per un cluster MSK, completa i seguenti passaggi:

1. Apri la console Amazon MSK all'indirizzo <https://console.aws.amazon.com/msk/home?region=us-east-1#/home/>.
2. Nel pannello di navigazione scegliere Clusters (Cluster). Quindi, scegli un cluster.
3. Per Azione, seleziona Modifica monitoraggio.
4. Seleziona l'opzione per il monitoraggio avanzato a livello di argomento.
5. Seleziona Salvataggio delle modifiche.

Per ulteriori informazioni sui livelli di monitoraggio, consulta la sezione [Aggiornamento delle impostazioni di sicurezza di un cluster](#) nella Amazon Managed Streaming for Apache Kafka Developer Guide.

Controlli Amazon MQ

Questi controlli sono correlati alle risorse Amazon MQ.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch

Requisiti correlati: NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-12, NIST.800-53.r5 SI-4

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::AmazonMQ::Broker

Regola AWS Config : [mq-cloudwatch-audit-log-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un broker Amazon MQ ActiveMQ trasmette i log di audit ad Amazon Logs. CloudWatch Il controllo fallisce se il broker non trasmette i log di audit a Logs. CloudWatch

Pubblicando i log del broker ActiveMQ su Logs CloudWatch , puoi CloudWatch creare allarmi e metriche che aumentano la visibilità delle informazioni relative alla sicurezza.

Correzione

Per trasmettere i log del broker ActiveMQ CloudWatch a Logs, consulta [Configuring Amazon MQ for ActiveMQ logs nella Amazon MQ Developer Guide](#).

[MQ.3] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie

Requisiti correlati: NIST.800-53.r5 CM-3, NIST.800-53.r5 SI-2

Categoria: Identificazione > Gestione di vulnerabilità, patch e versioni

Gravità: bassa

Tipo di risorsa: AWS::AmazonMQ::Broker

Regola AWS Config : [mq-auto-minor-version-upgrade-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un broker Amazon MQ ha abilitato l'aggiornamento automatico delle versioni secondarie. Il controllo fallisce se il broker non ha abilitato l'aggiornamento automatico della versione secondaria.

Man mano che Amazon MQ rilascia e supporta nuove versioni del motore di brokeraggio, le modifiche sono retrocompatibili con un'applicazione esistente e non compromettono le funzionalità esistenti. Gli aggiornamenti automatici delle versioni del motore di brokeraggio ti proteggono dai rischi per la sicurezza, aiutano a correggere i bug e a migliorare la funzionalità.

Note

Quando il broker associato all'aggiornamento automatico delle versioni secondarie utilizza la patch più recente e non è più supportato, è necessario eseguire l'aggiornamento manualmente.

Correzione

Per abilitare l'aggiornamento automatico della versione secondaria per un broker MQ, consulta [Aggiornamento automatico della versione secondaria del motore](#) nella Amazon MQ Developer Guide.

[MQ.4] I broker Amazon MQ devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::AmazonMQ::Broker

AWS Config regola: tagged-amazonmq-broker (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un broker Amazon MQ dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il broker non dispone di chiavi di tag o se non dispone di tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il broker non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un broker Amazon MQ, consulta [Tagging resources](#) nella Amazon MQ Developer Guide.

[MQ.5] I broker ActiveMQ devono utilizzare la modalità di distribuzione attiva/standby

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: bassa

Tipo di risorsa: AWS::AmazonMQ::Broker

Regola AWS Config : [mq-active-deployment-mode](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la modalità di distribuzione per un broker Amazon MQ ActiveMQ è impostata su active/standby. Il controllo fallisce se come modalità di distribuzione è impostato un broker a istanza singola (abilitato per impostazione predefinita).

La distribuzione attiva/standby offre un'elevata disponibilità per i broker Amazon MQ ActiveMQ in un unico ambiente. Regione AWS La modalità di distribuzione attiva/standby include due istanze di broker in due diverse zone di disponibilità, configurate in una coppia ridondante. Questi broker comunicano in modo sincrono con l'applicazione, il che può ridurre i tempi di inattività e la perdita di dati in caso di guasto.

Correzione

Per creare un nuovo broker ActiveMQ con modalità di distribuzione attiva/standby, consulta [Creazione e configurazione di un broker ActiveMQ nella Amazon MQ Developer Guide](#). Per la modalità di distribuzione, scegli il broker Active/standby. Non è possibile modificare la modalità di distribuzione per un broker esistente. È invece necessario creare un nuovo broker e copiare le impostazioni dal vecchio broker.

[MQ.6] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: bassa

Tipo di risorsa: AWS::AmazonMQ::Broker

Regola AWS Config : [mq-rabbit-deployment-mode](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la modalità di distribuzione per un broker Amazon MQ RabbitMQ è impostata sulla distribuzione in cluster. Il controllo fallisce se come modalità di distribuzione è impostato un broker a istanza singola (abilitato per impostazione predefinita).

La distribuzione in cluster offre un'elevata disponibilità per i broker Amazon MQ RabbitMQ in un unico. Regione AWS L'implementazione del cluster è un raggruppamento logico di tre nodi broker RabbitMQ, ciascuno con il proprio volume Amazon Elastic Block Store (Amazon EBS) e uno stato condiviso. L'implementazione del cluster garantisce la replica dei dati su tutti i nodi del cluster, il che può ridurre i tempi di inattività e la perdita di dati in caso di guasto.

Correzione

Per creare un nuovo broker RabbitMQ con modalità di distribuzione cluster, consulta [Creazione e connessione a un broker RabbitMQ nella Amazon MQ Developer Guide](#). Per la modalità di distribuzione, scegli Distribuzione in cluster. Non è possibile modificare la modalità di distribuzione per un broker esistente. È invece necessario creare un nuovo broker e copiare le impostazioni dal vecchio broker.

Controlli Amazon Neptune

Questi controlli sono correlati alle risorse di Neptune.

Questi controlli potrebbero non essere disponibili in tutti. Regioni AWS Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[Neptune.1] I cluster Neptune DB devono essere crittografati a riposo

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [neptune-cluster-encrypted](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Neptune DB è crittografato a riposo. Il controllo fallisce se un cluster Neptune DB non è crittografato a riposo.

I dati inattivi si riferiscono a tutti i dati archiviati in uno storage persistente e non volatile per qualsiasi durata. La crittografia aiuta a proteggere la riservatezza di tali dati, riducendo il rischio che un utente non autorizzato possa accedervi. La crittografia dei cluster Neptune DB protegge i dati e i metadati dall'accesso non autorizzato. Soddisfa inoltre i requisiti di conformità per la crittografia dei file system di produzione. data-at-rest

Correzione

È possibile abilitare la crittografia a riposo quando si crea un cluster Neptune DB. Non è possibile modificare le impostazioni di crittografia dopo aver creato un cluster. Per ulteriori informazioni, [consulta *Encrypting Neptune resources at rest* nella Guida per l'utente di Neptune.](#)

[Neptune.2] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST.800-53.R5 AU-6 (3), NIST.800-53.R5 AU-6 (4), NIST.800-53.R5 AU-6 (5), NIST.800-53.R5 AU-7 (1), NIST.800-53.R5 AU-9 (7), NIST.800-53.R5 CA-7, NIST.800-53.R5 NITR5 SC-7 (9), NIS.800-53.r5 SI-20, NIS.800-53.r5 SI-3 (8), NIS.800-53.r5 SI-4 (20), NIS.800-53.R5 SI-4 (5), NIT.800-53.r5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [neptune-cluster-cloudwatch-log-export-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Neptune DB pubblica log di audit su Amazon Logs. CloudWatch Il controllo fallisce se un cluster Neptune DB non pubblica i log di controllo su Logs. CloudWatch EnableCloudWatchLogsExportdovrebbe essere impostato su. Audit

Amazon Neptune e CloudWatch Amazon sono integrati in modo da poter raccogliere e analizzare i parametri delle prestazioni. Neptune invia automaticamente le metriche e supporta anche gli CloudWatch allarmi. CloudWatch I log di controllo sono altamente personalizzabili. Quando si esegue l'audit di un database, ogni operazione sui dati può essere monitorata e registrata in una pista di controllo, incluse le informazioni su quale cluster di database si accede e in che modo. Ti consigliamo di inviare questi log per aiutarti CloudWatch a monitorare i cluster Neptune DB.

Correzione

Per pubblicare i log di controllo di Neptune su Logs CloudWatch , [consulta Pubblicazione dei log di Neptune su Amazon Logs nella Neptune User Guide. CloudWatch](#) Nella sezione Esportazioni dei log, scegli Audit.

[Neptune.3] Le istantanee del cluster Neptune DB non devono essere pubbliche

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Severità: critica

Tipo di risorsa: AWS::RDS::DBClusterSnapshot

Regola AWS Config : [neptune-cluster-snapshot-public-prohibited](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istantanea manuale del cluster DB di Neptune è pubblica. Il controllo fallisce se un'istantanea manuale del cluster DB di Neptune è pubblica.

Un'istantanea manuale del cluster Neptune DB non deve essere pubblica a meno che non sia prevista. Se condividi un'istantanea manuale non crittografata come pubblica, l'istantanea è disponibile per tutti. Account AWS Le istantanee pubbliche possono causare un'esposizione involontaria dei dati.

Correzione

Per rimuovere l'accesso pubblico alle istantanee manuali dei cluster DB di Neptune, [consulta Condivisione di un'istantanea del cluster DB](#) nella Guida per l'utente di Neptune.

[Neptune.4] I cluster Neptune DB devono avere la protezione da eliminazione abilitata

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoria: Proteggi > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: bassa

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [neptune-cluster-deletion-protection-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Neptune DB ha la protezione da eliminazione abilitata. Il controllo fallisce se un cluster Neptune DB non ha la protezione da eliminazione abilitata.

L'attivazione della protezione da eliminazione del cluster offre un ulteriore livello di protezione contro l'eliminazione accidentale del database o l'eliminazione da parte di un utente non autorizzato. Un cluster Neptune DB non può essere eliminato mentre la protezione da eliminazione è abilitata.

È necessario innanzitutto disabilitare la protezione da eliminazione prima che una richiesta di eliminazione possa avere successo.

Correzione

Per abilitare la protezione da eliminazione per un cluster Neptune DB esistente, [consulta Modificare il cluster DB utilizzando la console, la CLI e l'API nella Guida per l'utente di Amazon Aurora.](#)

[Neptune.5] I cluster Neptune DB devono avere i backup automatici abilitati

Requisiti correlati: NIST.800-53.R5 SI-12

Categoria: Ripristino > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [neptune-cluster-backup-retention-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
minimumBackupRetentionPeriod	Periodo minimo di conservazione dei backup in giorni	Numero intero	7 Da a 35	7

Questo controllo verifica se un cluster Neptune DB ha abilitato i backup automatici e un periodo di conservazione dei backup maggiore o uguale al periodo di tempo specificato. Il controllo fallisce se i backup non sono abilitati per il cluster Neptune DB o se il periodo di conservazione è inferiore al periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di conservazione del backup, Security Hub utilizza un valore predefinito di 7 giorni.

I backup aiutano a ripristinare più rapidamente un incidente di sicurezza e a rafforzare la resilienza dei sistemi. Automatizzando i backup per i cluster Neptune DB, sarete in grado di ripristinare i sistemi in un determinato momento e ridurre al minimo i tempi di inattività e la perdita di dati.

Correzione

Per abilitare i backup automatici e impostare un periodo di conservazione dei backup per i cluster Neptune DB, [consulta *Enabling automatic backup*](#) nella Amazon RDS User Guide. Per il periodo di conservazione del Backup, scegli un valore maggiore o uguale a 7.

[Neptune.6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SC-7 (18))

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::RDS::DBClusterSnapshot

Regola AWS Config : [neptune-cluster-snapshot-encrypted](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istantanea del cluster Neptune DB è crittografata quando è inattiva. Il controllo fallisce se un cluster Neptune DB non è crittografato a riposo.

I dati inattivi si riferiscono a tutti i dati archiviati in uno storage persistente e non volatile per qualsiasi durata. La crittografia consente di proteggere la riservatezza di tali dati, riducendo il rischio che un utente non autorizzato possa accedervi. I dati nelle istantanee dei cluster Neptune DB devono essere crittografati quando sono inattivi per un ulteriore livello di sicurezza.

Correzione

Non è possibile crittografare uno snapshot del cluster Neptune DB esistente. È invece necessario ripristinare lo snapshot in un nuovo cluster DB e abilitare la crittografia sul cluster. È possibile creare un'istantanea crittografata dal cluster crittografato. Per istruzioni, consulta [Ripristino da uno snapshot](#)

[del cluster DB e Creazione di uno snapshot del cluster DB in Neptune nella Guida per l'utente di Neptune.](#)

[Neptune.7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [neptune-cluster-iam-database-authentication](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Neptune DB ha l'autenticazione del database IAM abilitata. Il controllo fallisce se l'autenticazione del database IAM non è abilitata per un cluster Neptune DB.

L'autenticazione del database IAM per i cluster di database Amazon Neptune elimina la necessità di memorizzare le credenziali degli utenti all'interno della configurazione del database perché l'autenticazione viene gestita esternamente tramite IAM. Quando l'autenticazione del database IAM è abilitata, ogni richiesta deve essere firmata utilizzando Signature Version 4. AWS

Correzione

Per impostazione predefinita, l'autenticazione del database IAM è disabilitata quando si crea un cluster Neptune DB. Per abilitarlo, consulta [Enabling IAM database authentication in Neptune](#) nella Neptune User Guide.

[Neptune.8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : [neptune-cluster-copy-tags-to-snapshot-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Neptune DB è configurato per copiare tutti i tag nelle istantanee al momento della creazione delle istantanee. Il controllo fallisce se un cluster Neptune DB non è configurato per copiare i tag nelle istantanee.

L'identificazione e l'inventario delle risorse IT sono un aspetto cruciale della governance e della sicurezza. È necessario etichettare gli snapshot nello stesso modo dei relativi cluster di database Amazon RDS principali. La copia dei tag garantisce che i metadati per gli snapshot DB corrispondano a quelli dei cluster di database principali e che le politiche di accesso per lo snapshot DB corrispondano anche a quelle dell'istanza DB principale.

Correzione

Per copiare i tag nelle istantanee per i cluster Neptune DB, consulta [Copiare i tag in Neptune nella Guida per l'utente di Neptune](#).

[Neptune.9] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : [neptune-cluster-multi-az-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Neptune DB dispone di istanze di replica in lettura in più zone di disponibilità (AZ). Il controllo fallisce se il cluster viene distribuito in una sola AZ.

Se una AZ non è disponibile e durante gli eventi di manutenzione regolari, le repliche di lettura fungono da destinazioni di failover per l'istanza principale. Pertanto, se si verifica un errore nell'istanza primaria, Neptune promuove un'istanza di replica di lettura a diventare l'istanza primaria. Al contrario, se il cluster database non include istanze di replica di lettura, il cluster database rimane non disponibile quando l'istanza primaria ha esito negativo finché non viene ricreata. La ricreazione dell'istanza primaria richiede molto più tempo rispetto alla promozione di un'istanza di replica di lettura. Per garantire un'elevata disponibilità, si consiglia di creare una o più istanze di replica di lettura che abbiano la stessa classe di istanza DB dell'istanza principale e si trovino in AZ diverse rispetto all'istanza primaria.

Correzione

Per implementare un cluster Neptune DB in più AZ, [consulta Istanze DB Read-Replica in un cluster Neptune DB nella Guida per l'utente di Neptune](#).

AWS Network Firewall controlli

Questi controlli sono correlati alle risorse del Network Firewall.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[NetworkFirewall.1] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::NetworkFirewall::Firewall

Regola AWS Config : [netfw-multi-az-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo valuta se un firewall gestito tramite AWS Network Firewall è distribuito su più zone di disponibilità (AZ). Il controllo fallisce se un firewall viene distribuito in una sola AZ.

AWS l'infrastruttura globale ne include diverse Regioni AWS. Le AZ sono sedi fisicamente separate e isolate all'interno di ciascuna regione, collegate tramite reti a bassa latenza, ad alta velocità di trasmissione e altamente ridondanti. Implementando un firewall Network Firewall su più AZ, è possibile bilanciare e spostare il traffico tra le AZ, il che aiuta a progettare soluzioni ad alta disponibilità.

Correzione

Implementazione di un firewall Network Firewall su più AZ

1. Apri alla console Amazon VPC all'indirizzo <https://console.aws.amazon.com/vpc/>.
2. Nel riquadro di navigazione, in Network Firewall, scegli Firewall.
3. Nella pagina Firewall, seleziona il firewall che desideri modificare.
4. Nella pagina dei dettagli del firewall, scegli la scheda Dettagli del firewall.
5. Nella sezione Politica associata e VPC, scegli Modifica
6. Per aggiungere una nuova AZ, scegli Aggiungi nuova sottorete. Seleziona la AZ e la sottorete che desideri utilizzare. Assicurati di selezionare almeno due AZ.
7. Selezionare Salva.

[NetworkFirewall.2] La registrazione del Network Firewall deve essere abilitata

Requisiti correlati: NIST.800-53.r5 AC-2 (12), NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-9 (7), NIST.800-53.r5 CA-7, NIST.800-53.r5 SC-7 (9), NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4, NIST.800-53.R5 SI-4 (20), NIST.800-53.5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::NetworkFirewall::LoggingConfiguration

Regola AWS Config : [netfw-logging-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la registrazione è abilitata per un AWS Network Firewall firewall. Il controllo fallisce se la registrazione non è abilitata per almeno un tipo di registro o se la destinazione di registrazione non esiste.

La registrazione consente di mantenere l'affidabilità, la disponibilità e le prestazioni dei firewall. In Network Firewall, la registrazione fornisce informazioni dettagliate sul traffico di rete, tra cui l'ora in cui lo stateful engine ha ricevuto un flusso di pacchetti, informazioni dettagliate sul flusso di pacchetti e qualsiasi azione basata sullo stateful rule intrapresa contro il flusso di pacchetti.

Correzione

Per abilitare la registrazione per un firewall, consulta [Aggiornamento della configurazione di registrazione di un firewall nella Guida per gli sviluppatori](#).AWS Network Firewall

[NetworkFirewall.3] Le policy di Network Firewall devono avere almeno un gruppo di regole associato

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Configurazione di rete sicura

Gravità: media

Tipo di risorsa: AWS::NetworkFirewall::FirewallPolicy

Regola AWS Config : [netfw-policy-rule-group-associated](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se a una policy Network Firewall sono associati gruppi di regole stateful o stateless. Il controllo ha esito negativo se non vengono assegnati gruppi di regole stateless o stateful.

Una policy firewall definisce il modo in cui il firewall monitora e gestisce il traffico in Amazon Virtual Private Cloud (Amazon VPC). La configurazione di gruppi di regole stateless e stateful aiuta a filtrare pacchetti e flussi di traffico e definisce la gestione del traffico predefinita.

Correzione

Per aggiungere un gruppo di regole a una policy Network Firewall, vedere [Aggiornamento di una policy firewall](#) nella AWS Network Firewall Developer Guide. Per informazioni sulla creazione e la gestione dei gruppi di regole, consulta [Gruppi di regole in AWS Network Firewall](#).

[NetworkFirewall.4] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Configurazione di rete sicura

Gravità: media

Tipo di risorsa: AWS::NetworkFirewall::FirewallPolicy

Regola AWS Config : [netfw-policy-default-action-full-packets](#)

Tipo di pianificazione: modifica attivata

Parametri:

- statelessDefaultActions: aws:drop,aws:forward_to_sfe(non personalizzabile)

Questo controllo verifica se l'azione stateless predefinita per pacchetti completi per una policy Network Firewall è drop o forward. Il controllo passa se è selezionato Drop o Forward è selezionato e fallisce se Pass è selezionato.

Una policy firewall definisce il modo in cui il firewall monitora e gestisce il traffico in Amazon VPC. Puoi configurare gruppi di regole stateless e stateful per filtrare pacchetti e flussi di traffico. L'impostazione predefinita è in grado Pass di consentire il traffico non intenzionale.

Correzione

Per modificare la politica del firewall, consulta [Aggiornamento di una politica firewall](#) nella Guida per gli sviluppatori.AWS Network Firewall Per le azioni predefinite Stateless, scegli Modifica. Quindi, scegli Elimina o Inoltra ai gruppi di regole con stato come Azione.

[NetworkFirewall.5] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Configurazione di rete sicura

Gravità: media

Tipo di risorsa: AWS::NetworkFirewall::FirewallPolicy

Regola AWS Config : [netfw-policy-default-action-fragment-packets](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `statelessFragDefaultActions` (Required) : `aws:drop`, `aws:forward_to_sfe`(non personalizzabile)

Questo controllo verifica se l'azione `stateless` predefinita per i pacchetti frammentati per una policy Network Firewall è `drop` o `forward`. Il controllo passa se è selezionato `Drop` o `Forward` è selezionato e fallisce se `Pass` è selezionato.

Una policy firewall definisce il modo in cui il firewall monitora e gestisce il traffico in Amazon VPC. Puoi configurare gruppi di regole `stateless` e `stateful` per filtrare pacchetti e flussi di traffico. L'impostazione predefinita è in grado `Pass` di consentire il traffico non intenzionale.

Correzione

Per modificare la politica del firewall, consulta [Aggiornamento di una politica firewall](#) nella Guida per gli sviluppatori.AWS Network Firewall Per le azioni predefinite `Stateless`, scegli `Modifica`. Quindi, scegli `Elimina` o `Inoltra` ai gruppi di regole con stato come `Azione`.

[NetworkFirewall.6] Il gruppo di regole `Stateless` Network Firewall non deve essere vuoto

Requisiti correlati: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (5)

Categoria: Protezione > Configurazione di rete sicura

Gravità: media

Tipo di risorsa: `AWS::NetworkFirewall::RuleGroup`

Regola AWS Config : [netfw-stateless-rule-group-not-empty](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo di regole senza stato AWS Network Firewall contiene regole. Il controllo ha esito negativo se non ci sono regole nel gruppo di regole.

Un gruppo di regole contiene regole che definiscono il modo in cui il firewall elabora il traffico nel tuo VPC. Un gruppo di regole stateless vuoto, se presente in una policy firewall, potrebbe dare l'impressione che il gruppo di regole elabori il traffico. Tuttavia, quando il gruppo di regole stateless è vuoto, non elabora il traffico.

Correzione

Per aggiungere regole al gruppo di regole Network Firewall, consulta [Aggiornamento di un gruppo di regole stateful nella Guida](#) per gli AWS Network Firewall sviluppatori. Nella pagina dei dettagli del firewall, per il gruppo di regole Stateless, scegli Modifica per aggiungere regole.

[NetworkFirewall.7] I firewall Network Firewall devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::NetworkFirewall::Firewall

AWS Config regola: tagged-networkfirewall-firewall (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un AWS Network Firewall firewall dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il firewall non dispone di chiavi

di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il firewall non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in Riferimenti generali di AWS

Correzione

Per aggiungere tag a un firewall Network Firewall, consulta [Tagging AWS Network Firewall resources](#) nella AWS Network Firewall Developer Guide.

[NetworkFirewall.8] Le politiche firewall di Network Firewall devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::NetworkFirewall::FirewallPolicy`

AWS Config regola: `tagged-networkfirewall-firewallpolicy` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se una politica AWS Network Firewall firewall contiene tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se la politica del firewall non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la politica del firewall non è contrassegnata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori

best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una politica di Network Firewall, consulta [Tagging AWS Network Firewall resources](#) nella AWS Network Firewall Developer Guide.

[NetworkFirewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoria: Protezione > Sicurezza della rete > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::NetworkFirewall::Firewall

Regola AWS Config : [netfw-deletion-protection-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS Network Firewall firewall ha la protezione da eliminazione abilitata. Il controllo fallisce se la protezione da eliminazione non è abilitata per un firewall.

AWS Network Firewall è un firewall di rete gestito a stato e un servizio di rilevamento delle intrusioni che consente di ispezionare e filtrare il traffico da, verso o tra i Virtual Private Cloud (VPC). L'impostazione di protezione dall'eliminazione protegge dall'eliminazione accidentale del firewall.

Correzione

Per abilitare la protezione da eliminazione su un firewall Network Firewall esistente, vedere [Aggiornamento di un firewall](#) nella AWS Network Firewall Developer Guide. Per Modifica le protezioni, seleziona Abilita. Puoi anche abilitare la protezione dall'eliminazione richiamando l'[UpdateFirewallDeleteProtection](#) API e impostando il DeleteProtection campo su. true

Controlli OpenSearch di Amazon Service

Questi controlli sono correlati alle risorse OpenSearch del Servizio.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

I OpenSearch domini [Opensearch.1] devono avere la crittografia a riposo abilitata

Requisiti correlati: PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.4, PCI DSS versione 3.2.1/7.2.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, nIST.800-53.r5 SC-13, nIST.800-53.r5 NITS-28, NITS.800-53.R5 SC-28 (1), NIST.800-53.R5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::OpenSearch::Domain

Regola AWS Config : [opensearch-encrypted-at-rest](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la encryption-at-rest configurazione dei OpenSearch domini è abilitata. Il controllo non riesce se la crittografia dei dati inattivi non è abilitata.

Per un ulteriore livello di sicurezza per i dati sensibili, è necessario configurare il dominio di OpenSearch servizio in modo che venga crittografato quando è inattivo. Quando configuri la crittografia dei dati inattivi, AWS KMS archivia e gestisce le chiavi di crittografia. Per eseguire la crittografia, AWS KMS utilizza l'algoritmo Advanced Encryption Standard con chiavi a 256 bit (AES-256).

Per ulteriori informazioni sulla crittografia dei OpenSearch servizi a riposo, consulta [Encryption of data at rest for Amazon OpenSearch Service](#) nella Amazon OpenSearch Service Developer Guide.

Correzione

Per abilitare la crittografia a riposo per OpenSearch domini nuovi ed esistenti, consulta [Enabling encryption of data at rest](#) nella Amazon OpenSearch Service Developer Guide.

I OpenSearch domini [Opensearch.2] non devono essere accessibili al pubblico

Requisiti correlati: PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.2, PCI DSS versione 3.2.1/1.3.4, PCI DSS versione 3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20) 3.5 SC-7 (21), NIT 800-53.r5 SC-7 (3), NIT 800-53.5 SC-7 (4), NIT 800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete sicura > Risorse all'interno del VPC

Severità: critica

Tipo di risorsa: AWS::OpenSearch::Domain

Regola AWS Config : [opensearch-in-vpc-only](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i OpenSearch domini si trovano in un VPC. Non valuta la configurazione del routing della sottorete VPC per determinare l'accesso pubblico.

È necessario assicurarsi che i OpenSearch domini non siano collegati a sottoreti pubbliche. Consulta [le politiche basate sulle risorse](#) nella Amazon OpenSearch Service Developer Guide. È inoltre necessario assicurarsi che il VPC sia configurato in base alle procedure consigliate. Consulta [le best practice di sicurezza per il tuo VPC](#) nella Amazon VPC User Guide.

OpenSearch i domini distribuiti all'interno di un VPC possono comunicare con le risorse VPC sulla AWS rete privata, senza la necessità di attraversare la rete Internet pubblica. Questa configurazione aumenta il livello di sicurezza limitando l'accesso ai dati in transito. I VPC forniscono una serie di controlli di rete per proteggere l'accesso ai OpenSearch domini, inclusi l'ACL di rete e i gruppi di sicurezza. Security Hub consiglia di migrare OpenSearch i domini pubblici ai VPC per sfruttare questi controlli.

Correzione

Se si crea un dominio con un endpoint pubblico, non è possibile inserirlo in un VPC in un secondo momento. Devi invece creare un nuovo dominio ed eseguire la migrazione dei dati. È vero anche il

contrario. Se si crea un dominio all'interno di un VPC, non può avere un endpoint pubblico. È invece necessario [creare un altro dominio](#) o disabilitare questo controllo.

Per istruzioni, consulta [Launching your Amazon OpenSearch Service domain all'interno di un VPC nella Amazon OpenSearch Service Developer Guide](#).

I OpenSearch domini [Opensearch.3] devono crittografare i dati inviati tra i nodi

Requisiti correlati: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (1) -53,5 SC-8 (2)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: AWS::OpenSearch::Domain

Regola AWS Config : [opensearch-node-to-node-encryption-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i OpenSearch domini hanno la node-to-node crittografia abilitata. Questo controllo ha esito negativo se node-to-node la crittografia è disabilitata nel dominio.

HTTPS (TLS) può essere utilizzato per impedire a potenziali aggressori di intercettare o manipolare il traffico di rete utilizzando attacchi simili. person-in-the-middle Devono essere consentite solo le connessioni crittografate tramite HTTPS (TLS). L'abilitazione della node-to-node crittografia per i OpenSearch domini garantisce che le comunicazioni all'interno del cluster siano crittografate durante il transito.

Questa configurazione può comportare un calo delle prestazioni. È necessario conoscere e testare il compromesso in termini di prestazioni prima di attivare questa opzione.

Correzione

Per abilitare node-to-node la crittografia su un OpenSearch dominio, consulta [node-to-node Enabling encryption](#) nella Amazon OpenSearch Service Developer Guide.

La registrazione degli errori del OpenSearch dominio [Opensearch.4] nei log dovrebbe essere abilitata CloudWatch

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIS.800-53.R 5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::OpenSearch::Domain

Regola AWS Config : [opensearch-logs-to-cloudwatch](#)

Tipo di pianificazione: modifica attivata

Parametri:

- logtype = 'error'(non personalizzabile)

Questo controllo verifica se i OpenSearch domini sono configurati per inviare i log degli errori ai CloudWatch registri. Questo controllo ha esito negativo se la registrazione degli errori non CloudWatch è abilitata per un dominio.

È necessario abilitare i log degli errori per i OpenSearch domini e inviarli a Logs per la conservazione e la CloudWatch risposta. I log degli errori di dominio possono essere utili per gli audit di sicurezza e di accesso e per diagnosticare i problemi di disponibilità.

Correzione

Per abilitare la pubblicazione dei log, consulta [Enabling log publishing \(console\)](#) nella Amazon OpenSearch Service Developer Guide.

I OpenSearch domini [Opensearch.5] devono avere la registrazione di controllo abilitata

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3,

NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIS.800-53.R 5 SI-4 (20), NID 800-53.R 5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::OpenSearch::Domain

Regola AWS Config : [opensearch-audit-logging-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `cloudWatchLogsLogGroupArnList`(non personalizzabile): Security Hub non compila questo parametro. Elenco separato da virgole di gruppi di CloudWatch log che devono essere configurati per i log di controllo.

Questa regola si applica NON_COMPLIANT se il gruppo di log CloudWatch Logs del OpenSearch dominio non è specificato in questo elenco di parametri.

Questo controllo verifica se nei OpenSearch domini è abilitata la registrazione di controllo. Questo controllo ha esito negativo se in un OpenSearch dominio non è abilitata la registrazione di controllo.

I log di controllo sono altamente personalizzabili. Ti consentono di tenere traccia delle attività degli utenti sui tuoi OpenSearch cluster, compresi i successi e gli errori di autenticazione, le richieste, le modifiche all'indicizzazione e le OpenSearch query di ricerca in arrivo.

Correzione

Per istruzioni su come abilitare i log di controllo, consulta [Enabling audit logs](#) nella Amazon OpenSearch Service Developer Guide.

I OpenSearch domini [Opensearch.6] devono avere almeno tre nodi di dati

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::OpenSearch::Domain

Regola AWS Config : [opensearch-data-node-fault-tolerance](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i OpenSearch domini sono configurati con almeno tre nodi di dati e `zoneAwarenessEnabled` lo è. `true` Questo controllo ha esito negativo per un OpenSearch dominio se `instanceCount` è inferiore a 3 o lo `zoneAwarenessEnabled` è `false`.

Un OpenSearch dominio richiede almeno tre nodi di dati per un'elevata disponibilità e tolleranza agli errori. L'implementazione di un OpenSearch dominio con almeno tre nodi di dati garantisce le operazioni del cluster in caso di guasto di un nodo.

Correzione

Per modificare il numero di nodi di dati in un dominio OpenSearch

1. Accedi alla AWS console e apri la console Amazon OpenSearch Service all'[indirizzo https://console.aws.amazon.com/aos/](https://console.aws.amazon.com/aos/).
2. In I miei domini, scegli il nome del dominio da modificare e scegli Modifica.
3. In Nodi di dati imposta Numero di nodi su un numero maggiore di 3. Se esegui la distribuzione in tre zone di disponibilità, imposta il numero su un multiplo di tre per garantire una distribuzione equa tra le zone di disponibilità.
4. Scegli Invia.

I OpenSearch domini [Opensearch.7] devono avere un controllo degli accessi granulare abilitato

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-5, NIST.800-53.r5 AC-6

Categoria: Protezione > Gestione degli accessi sicuri > Azioni API sensibili limitate

Gravità: alta

Tipo di risorsa: AWS::OpenSearch::Domain

Regola AWS Config : [opensearch-access-control-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se nei OpenSearch domini è abilitato il controllo granulare degli accessi. Il controllo fallisce se il controllo di accesso a grana fine non è abilitato. Il controllo granulare degli accessi richiede `advanced-security-options` che il parametro sia abilitato. OpenSearch `update-domain-config`

Il controllo granulare degli accessi offre modi aggiuntivi per controllare l'accesso ai tuoi dati su Amazon Service. OpenSearch

Correzione

Per abilitare il controllo granulare degli accessi, consulta la sezione Controllo [granulare degli accessi in Amazon Service nella Amazon OpenSearch Service Developer](#) Guide. OpenSearch

[Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS

Requisiti correlati: NIST.800-53.r5 AC-17 (2), NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), NIST.800-53.r5 SC-12 (3), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia di data-in-transit

Gravità: media

Tipo di risorsa: AWS::OpenSearch::Domain

Regola AWS Config : [opensearch-https-required](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `tlsPolicies`: `Policy-Min-TLS-1-2-PFS-2023-10`(non personalizzabile)

Questo controllo verifica se un endpoint di dominio Amazon OpenSearch Service è configurato per utilizzare la politica di sicurezza TLS più recente. Il controllo fallisce se l'endpoint del OpenSearch dominio non è configurato per utilizzare la politica supportata più recente o se HTTPS non è abilitato.

HTTPS (TLS) può essere utilizzato per impedire a potenziali aggressori di utilizzare person-in-the-middle o attacchi simili per intercettare o manipolare il traffico di rete. Devono essere consentite solo le connessioni crittografate tramite HTTPS (TLS). La crittografia dei dati in transito può influire sulle prestazioni. È consigliabile testare l'applicazione con questa funzionalità per comprendere il profilo delle prestazioni e l'impatto del TLS. TLS 1.2 offre diversi miglioramenti della sicurezza rispetto alle versioni precedenti di TLS.

Correzione

Per abilitare la crittografia TLS, utilizza l'operazione API. [UpdateDomainConfig](#) Configura il [DomainEndpointOptions](#) campo per impostare il `TLSecurityPolicy`. Per ulteriori informazioni, consulta [Node-to-node encryption](#) nella Amazon OpenSearch Service Developer Guide.

I OpenSearch domini [Opensearch.9] devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::OpenSearch::Domain`

AWS Config regola: `tagged-opensearch-domain` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un dominio Amazon OpenSearch Service ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il dominio non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il dominio non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un dominio OpenSearch di servizio, consulta [Working with tags](#) nella Amazon OpenSearch Service Developer Guide.

Nei OpenSearch domini [Opensearch.10] deve essere installato l'ultimo aggiornamento software

Requisiti correlati: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoria: Rileva > Gestione di vulnerabilità, patch e versioni

Gravità: bassa

Tipo di risorsa: AWS::OpenSearch::Domain

Regola AWS Config : [opensearch-update-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se in un dominio Amazon OpenSearch Service è installato l'ultimo aggiornamento software. Il controllo fallisce se un aggiornamento software è disponibile ma non è installato per il dominio.

OpenSearch Gli aggiornamenti del software di servizio forniscono le correzioni, gli aggiornamenti e le funzionalità più recenti della piattaforma disponibili per l'ambiente. Mantenere up-to-date l'installazione delle patch aiuta a mantenere la sicurezza e la disponibilità del dominio. Se non viene intrapresa alcuna azione sugli aggiornamenti richiesti, il software di servizio viene aggiornato automaticamente (in genere dopo 2 settimane). Ti consigliamo di pianificare gli aggiornamenti in un periodo di scarso traffico verso il dominio per ridurre al minimo le interruzioni del servizio.

Correzione

Per installare gli aggiornamenti software per un OpenSearch dominio, consulta [Starting an update](#) nella Amazon OpenSearch Service Developer Guide.

I OpenSearch domini [Opensearch.11] devono avere almeno tre nodi primari dedicati

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-2, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36, NIST.800-53.r5 SI-13

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::OpenSearch::Domain

Regola AWS Config : [opensearch-primary-node-fault-tolerance](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un dominio Amazon OpenSearch Service è configurato con almeno tre nodi primari dedicati. Il controllo fallisce se il dominio ha meno di tre nodi primari dedicati.

OpenSearch Il servizio utilizza nodi primari dedicati per aumentare la stabilità del cluster. Un nodo primario dedicato esegue attività di gestione del cluster, ma non contiene dati né risponde alle richieste di caricamento dei dati. Si consiglia di utilizzare Multi-AZ con standby, che aggiunge tre nodi primari dedicati a ciascun dominio di produzione OpenSearch .

Correzione

Per modificare il numero di nodi primari per un OpenSearch dominio, consulta [Creazione e gestione dei domini Amazon OpenSearch Service](#) nella Amazon OpenSearch Service Developer Guide.

AWS Private Certificate Authority controlli

Questi controlli sono correlati alle AWS Private CA risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

L'autorità di certificazione AWS Private CA principale [PCA.1] deve essere disabilitata

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Configurazione di rete protetta

Gravità: bassa

Tipo di risorsa: AWS::ACMPCA::CertificateAuthority

Regola AWS Config : [acm-pca-root-ca-disabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se AWS Private CA dispone di un'autorità di certificazione (CA) principale disabilitata. Il controllo fallisce se la CA principale è abilitata.

Con AWS Private CA, è possibile creare una gerarchia di CA che include una CA radice e CA subordinate. È necessario ridurre al minimo l'uso della CA principale per le attività quotidiane,

specialmente negli ambienti di produzione. La CA principale deve essere utilizzata solo per emettere certificati per CA intermedie. Ciò consente alla CA root di essere archiviata in modo sicuro mentre le CA intermedie eseguono l'attività quotidiana di emissione di certificati di entità finale.

Correzione

Per disabilitare la CA principale, consulta la sezione [Aggiornamento dello stato della CA](#) nella Guida per l'AWS Private Certificate Authority utente.

Controlli di Amazon Relational Database Service

Questi controlli sono correlati alle risorse Amazon RDS.

Questi controlli potrebbero non essere disponibili in tutti le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[RDS.1] L'istanza RDS deve essere privata

Requisiti correlati: PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.4, PCI DSS versione 3.2.1/1.3.6, PCI DSS versione 3.2.1/7.2.1, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20) 3.5 SC-7 (21), NIT 800-53.r5 SC-7 (3), NIT 800-53.5 SC-7 (4), NIT 800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

Regola AWS Config : [rds-snapshots-public-prohibited](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se gli snapshot di Amazon RDS sono pubblici. Il controllo fallisce se le istanze RDS sono pubbliche. Questo controllo valuta le istanze RDS, le istanze Aurora DB, le istanze Neptune DB e i cluster Amazon DocumentDB.

Gli snapshot RDS vengono utilizzati per eseguire il backup dei dati nelle istanze RDS in un determinato momento. Possono essere utilizzati per ripristinare gli stati precedenti delle istanze RDS.

Uno snapshot RDS non deve essere pubblico a meno che non sia previsto. Se condividi uno snapshot manuale non crittografato come pubblico, questo rende lo snapshot disponibile a tutti. Account AWS Ciò potrebbe comportare l'esposizione non intenzionale dei dati dell'istanza RDS.

Tieni presente che se la configurazione viene modificata per consentire l'accesso pubblico, la AWS Config regola potrebbe non essere in grado di rilevare la modifica per un massimo di 12 ore. Finché la AWS Config regola non rileva la modifica, il controllo viene superato anche se la configurazione viola la regola.

Per ulteriori informazioni sulla condivisione di uno snapshot DB, consulta [Sharing a DB snapshot](#) nella Amazon RDS User Guide.

Correzione

Per rimuovere l'accesso pubblico dagli snapshot RDS, consulta [Sharing a snapshot](#) nella Amazon RDS User Guide. Per la visibilità degli snapshot DB, scegliamo Private.

[RDS.2] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, in base alla durata PubliclyAccessible AWS Config

Requisiti correlati: benchmark CIS AWS Foundations versione 3.0.0/2.3.3, PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.2, PCI DSS versione 3.2.1/1.3.4, PCI DSS versione 3.2.1/1.3.6, PCI DSS versione 3.2.1/7.2.1, NIST.800-53.r5 AC-4, nIST.IST 4 NIS.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (5)

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: AWS::RDS::DBInstance

Regola AWS Config : [rds-instance-public-access-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le istanze di Amazon RDS sono accessibili al pubblico valutando il `PubliclyAccessible` campo nell'elemento di configurazione dell'istanza.

Le istanze DB Neptune e i cluster Amazon DocumentDB non hanno il flag e non `PubliclyAccessible` possono essere valutati. Tuttavia, questo controllo può comunque generare risultati per queste risorse. È possibile sopprimere questi risultati.

Il valore `PubliclyAccessible` nella configurazione dell'istanza RDS indica se l'istanza database è accessibile pubblicamente. Quando l'istanza database è configurata con `PubliclyAccessible`, si tratta di un'istanza con connessione Internet con un nome DNS risolvibile pubblicamente, che si risolve in un indirizzo IP pubblico. Quando l'istanza database non è accessibile pubblicamente, è un'istanza interna con un nome DNS che si risolve in un indirizzo IP privato.

A meno che non si intenda rendere l'istanza RDS accessibile al pubblico, l'istanza RDS non deve essere configurata con valore. `PubliclyAccessible` In questo modo si potrebbe consentire un traffico non necessario verso l'istanza del database.

Correzione

Per rimuovere l'accesso pubblico dalle istanze DB RDS, consulta [Modificare un'istanza DB Amazon RDS nella](#) Amazon RDS User Guide. Per l'accesso pubblico, scegli No.

[RDS.3] Le istanze database RDS devono avere la crittografia dei dati inattivi abilitata

Requisiti correlati: CIS AWS Foundations Benchmark v3.0.0/2.3.1, CIS Foundations Benchmark v1.4.0/2.3.1, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), nIST.800-53.r5 SC-28 (1), nIST.800-53.r5 SC-28 IST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6) AWS

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::RDS::DBInstance

Regola AWS Config : [rds-storage-encrypted](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la crittografia dello storage è abilitata per le istanze database di Amazon RDS.

Questo controllo è destinato alle istanze DB RDS. Tuttavia, può anche generare risultati per le istanze Aurora DB, le istanze Neptune DB e i cluster Amazon DocumentDB. Se questi risultati non sono utili, puoi eliminarli.

Per un ulteriore livello di sicurezza per i dati sensibili nelle istanze database RDS è necessario configurare la crittografia dei dati inattivi delle istanze database RDS. Per crittografare i dati inattivi delle istanze database RDS e degli snapshot, abilita l'opzione di crittografia per le istanze database RDS. I dati che vengono crittografati quando sono inattivi includono lo storage sottostante per le istanze database, i backup automatici, le repliche di lettura e gli snapshot.

Le istanze database crittografate RDS utilizzano l'algoritmo di crittografia AES-256 standard aperto per crittografare i dati sul server che ospita l'istanza database RDS. Dopo la crittografia dei dati, Amazon RDS gestisce l'autenticazione dell'accesso e la decrittografia dei dati in modo trasparente con un impatto minimo sulle prestazioni. Non è quindi necessario modificare le applicazioni client di database per utilizzare la crittografia.

La crittografia Amazon RDS è attualmente disponibile per tutti i motori di database e i tipi di storage. La crittografia Amazon RDS è disponibile per la maggior parte delle classi di istanza database. Per informazioni sulle classi di istanze DB che non supportano la crittografia Amazon RDS, [consulta Encrypting Amazon RDS resources nella Amazon RDS](#) User Guide.

Correzione

Per informazioni sulla crittografia delle istanze DB in Amazon RDS, consulta [Encrypting Amazon RDS resources nella Amazon RDS](#) User Guide.

[RDS.4] Le istantanee dei cluster RDS e le istantanee del database devono essere crittografate quando sono inattive

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa:AWS::RDS::DBClusterSnapshot, AWS::RDS::DBSnapshot

Regola AWS Config : [rds-snapshot-encrypted](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istantanea di RDS DB è crittografata. Il controllo ha esito negativo se uno snapshot RDS DB non è crittografato.

Questo controllo è destinato alle istanze DB RDS. Tuttavia, può anche generare risultati per istantanee di istanze Aurora DB, istanze DB Neptune e cluster Amazon DocumentDB. Se questi risultati non sono utili, puoi eliminarli.

La crittografia dei dati inattivi riduce il rischio che un utente non autenticato acceda ai dati archiviati su disco. I dati nelle istantanee RDS devono essere crittografati quando sono inattivi per un ulteriore livello di sicurezza.

Correzione

Per crittografare uno snapshot RDS, consulta [Encrypting Amazon RDS resources nella Amazon RDS User Guide](#). Quando crittografi un'istanza DB RDS, i dati crittografati includono lo storage sottostante dell'istanza, i relativi backup automatici, le repliche di lettura e le istantanee.

È possibile crittografare un'istanza DB RDS solo al momento della creazione, non dopo la creazione dell'istanza DB. Tuttavia, poiché è possibile crittografare una copia di uno snapshot DB non crittografata, puoi aggiungere in modo efficace la crittografia a un'istanza database non crittografata. Ovvero, è possibile creare uno snapshot dell'istanza database e quindi creare una copia crittografata di quella snapshot. Puoi quindi ripristinare un'istanza database da uno snapshot crittografata e pertanto disporre di una copia crittografata dell'istanza database originale.

[RDS.5] Le istanze DB RDS devono essere configurate con più zone di disponibilità

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::RDS::DBInstance

Regola AWS Config : [rds-multi-az-support](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'alta disponibilità è abilitata per le istanze DB RDS.

Le istanze DB RDS devono essere configurate per più zone di disponibilità (AZ). Ciò garantisce la disponibilità dei dati archiviati. Le implementazioni Multi-AZ consentono il failover automatico in caso di problemi con la disponibilità della zona di disponibilità e durante la normale manutenzione RDS.

Correzione

Per distribuire le tue istanze DB in più AZ, [modifica di un'istanza DB per renderla un'istanza DB Multi-AZ nella Amazon RDS User Guide](#).

[RDS.6] Il monitoraggio avanzato deve essere configurato per le istanze DB RDS

Requisiti correlati: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoria: Rilevamento > Servizi di rilevamento

Gravità: bassa

Tipo di risorsa: AWS::RDS::DBInstance

Regola AWS Config : [rds-enhanced-monitoring-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
monitoringInterval	Numero di secondi tra gli intervalli di raccolta delle metriche di monitoraggio	Enum	1, 5, 10, 15, 30, 60	Nessun valore predefinito

Questo controllo verifica se il monitoraggio avanzato è abilitato per un'istanza DB di Amazon Relational Database Service (Amazon RDS). Il controllo fallisce se il monitoraggio avanzato non è abilitato per l'istanza. Se fornisci un valore personalizzato per il `monitoringInterval` parametro, il controllo passa solo se le metriche di monitoraggio avanzate vengono raccolte per l'istanza all'intervallo specificato.

In Amazon RDS, Enhanced Monitoring consente una risposta più rapida ai cambiamenti delle prestazioni nell'infrastruttura sottostante. Queste modifiche delle prestazioni potrebbero comportare una mancanza di disponibilità dei dati. Enhanced Monitoring fornisce metriche in tempo reale del sistema operativo su cui viene eseguita l'istanza DB RDS. Sull'istanza è installato un agente. L'agente può ottenere le metriche in modo più accurato di quanto sia possibile dal livello dell'hypervisor.

I parametri di monitoraggio avanzato sono utili quando si desidera vedere come viene utilizzata la CPU in un'istanza database dai diversi processi o thread. Per ulteriori informazioni, consulta la sezione [Enhanced Monitoring](#) (Monitoraggio avanzato) nella Guida per l'utente di Amazon RDS.

Correzione

Per istruzioni dettagliate sull'attivazione di Enhanced Monitoring per la tua istanza DB, consulta [Configurazione e attivazione di Enhanced Monitoring](#) nella Amazon RDS User Guide.

[RDS.7] I cluster RDS devono avere la protezione da eliminazione abilitata

Requisiti correlati: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBCluster`

Regola AWS Config : [rds-cluster-deletion-protection-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster RDS DB ha la protezione da eliminazione abilitata. Il controllo ha esito negativo se in un cluster RDS DB non è abilitata la protezione da eliminazione.

Questo controllo è destinato alle istanze DB RDS. Tuttavia, può anche generare risultati per le istanze Aurora DB, le istanze Neptune DB e i cluster Amazon DocumentDB. Se questi risultati non sono utili, puoi eliminarli.

L'attivazione della protezione dall'eliminazione del cluster è un ulteriore livello di protezione contro l'eliminazione accidentale del database o l'eliminazione da parte di un'entità non autorizzata.

Quando la protezione da eliminazione è abilitata, non è possibile eliminare un cluster RDS. Prima che una richiesta di eliminazione possa avere esito positivo, è necessario disabilitare la protezione dall'eliminazione.

Correzione

Per abilitare la protezione da eliminazione per un cluster RDS DB, consulta [Modificare il cluster DB utilizzando la console, la CLI e l'API nella Amazon RDS User Guide](#). Per la protezione da eliminazione, scegli Abilita protezione da eliminazione.

[RDS.8] Le istanze DB RDS devono avere la protezione da eliminazione abilitata

Requisiti correlati: NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: bassa

Tipo di risorsa: AWS::RDS::DBInstance

Regola AWS Config : [rds-instance-deletion-protection-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri:

- databaseEngines: mariadb,mysql,custom-oracle-ee,oracle-ee-cdb,oracle-se2-cdb,oracle-ee,oracle-se2,oracle-se1,oracle-se,postgres,sqlserver-ee,sqlserver-se,sqlserver-ex,sqlserver-web (non personalizzabile)

Questo controllo verifica se le istanze DB RDS che utilizzano uno dei motori di database elencati hanno la protezione dall'eliminazione abilitata. Il controllo ha esito negativo se per un'istanza RDS DB non è abilitata la protezione da eliminazione.

L'attivazione della protezione dall'eliminazione delle istanze è un ulteriore livello di protezione contro l'eliminazione accidentale del database o l'eliminazione da parte di un'entità non autorizzata.

Mentre la protezione dall'eliminazione è abilitata, un'istanza DB RDS non può essere eliminata. Prima che una richiesta di eliminazione possa avere esito positivo, è necessario disabilitare la protezione dall'eliminazione.

Correzione

Per abilitare la protezione da eliminazione per un'istanza DB RDS, consulta [Modificare un'istanza DB Amazon RDS](#) nella Amazon RDS User Guide. Per la protezione da eliminazione, scegli Abilita protezione da eliminazione.

[RDS.9] Le istanze DB RDS devono pubblicare i log nei registri CloudWatch

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (10), NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIT.800-53.R5 SI-4 (20), NIT.800-53.R R5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::RDS::DBInstance

Regola AWS Config : [rds-logging-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istanza DB di Amazon RDS è configurata per pubblicare i seguenti log su Amazon CloudWatch Logs. Il controllo fallisce se l'istanza non è configurata per pubblicare i seguenti log su Logs: CloudWatch

- Oracle: (Alert, Audit, Trace, Listener)
- PostgreSQL: (Postgresql, aggiornamento)
- MySQL: (Controllo, Errore, Generale,) SlowQuery

- MariaDB: (Controllo, Errore, Generale,) SlowQuery
- SQL Server: (Errore, agente)
- Aurora: (Controllo, Errore, Generale,) SlowQuery
- Aurora-MySQL: (Controllo, Errore, Generale,) SlowQuery
- Aurora-PostgreSQL: (Postgresql, aggiornamento).

I database RDS devono avere i registri pertinenti abilitati. La registrazione del database fornisce registrazioni dettagliate delle richieste effettuate a RDS. I log del database possono facilitare i controlli di sicurezza e accesso e possono aiutare a diagnosticare i problemi di disponibilità.

Correzione

Per pubblicare i log del database RDS su CloudWatch Logs, consulta [Specificare i log da pubblicare su Logs CloudWatch nella Amazon RDS User Guide](#).

[RDS.10] L'autenticazione IAM deve essere configurata per le istanze RDS

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: media

Tipo di risorsa: AWS::RDS::DBInstance

Regola AWS Config : [rds-instance-iam-authentication-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istanza DB RDS ha l'autenticazione del database IAM abilitata. Il controllo fallisce se l'autenticazione IAM non è configurata per le istanze DB RDS. Questo controllo valuta solo le istanze RDS con i seguenti tipi di motore:mysql,,postgres, aurora e. aurora-mysql aurora-postgresql mariadb Un'istanza RDS deve inoltre trovarsi in uno dei seguenti stati per generare un risultato:available,, backing-up o. storage-optimization storage-full

L'autenticazione del database IAM consente l'autenticazione delle istanze del database con un token di autenticazione anziché una password. Il traffico di rete da e verso il database viene crittografato tramite SSL. Per ulteriori informazioni, consulta [Autenticazione database IAM](#) nella Guida per l'utente di Amazon Aurora.

Correzione

Per attivare l'autenticazione del database IAM su un'istanza DB RDS, consulta [Abilitazione e disabilitazione dell'autenticazione del database IAM](#) nella Amazon RDS User Guide.

[RDS.11] Le istanze RDS devono avere i backup automatici abilitati

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST .800-53,5 SI-13 (5)

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: AWS::RDS::DBInstance

Regola AWS Config : [db-instance-backup-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personali zzati consentiti	Valore predefinito di Security Hub
backupRetentionMinimum	Periodo minimo di conservazione dei backup in giorni	Numero intero	7 Da a 35	7
checkReadReplicas	Verifica se le istanze DB RDS dispongono di	Booleano	Non personali zzabile	false

Parametro	Descrizione	Type	Valori personali zzati consentiti	Valore predefinito di Security Hub
	backup abilitati per le repliche di lettura			

Questo controllo verifica se un'istanza di Amazon Relational Database Service ha abilitato i backup automatici e un periodo di conservazione dei backup maggiore o uguale al periodo di tempo specificato. Le repliche di lettura sono escluse dalla valutazione. Il controllo fallisce se i backup non sono abilitati per l'istanza o se il periodo di conservazione è inferiore al periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di conservazione del backup, Security Hub utilizza un valore predefinito di 7 giorni.

I backup aiutano a ripristinare più rapidamente un incidente di sicurezza e rafforzano la resilienza dei sistemi. Amazon RDS consente di configurare istantanee giornaliere di volumi completi di istanze. Per ulteriori informazioni sui backup automatici di Amazon RDS, consulta [Working with Backups](#) nella Amazon RDS User Guide.

Correzione

Per abilitare i backup automatici su un'istanza DB RDS, consulta [Enabling automatized backup](#) nella Amazon RDS User Guide.

[RDS.12] L'autenticazione IAM deve essere configurata per i cluster RDS

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoria: Protezione > Gestione sicura degli accessi > Autenticazione senza password

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [rds-cluster-iam-authentication-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon RDS DB ha l'autenticazione del database IAM abilitata.

L'autenticazione del database IAM consente l'autenticazione senza password per le istanze di database. L'autenticazione utilizza un token di autenticazione. Il traffico di rete da e verso il database è crittografato tramite SSL. Per ulteriori informazioni, consulta [Autenticazione database IAM](#) nella Guida per l'utente di Amazon Aurora.

Correzione

Per abilitare l'autenticazione IAM per un cluster DB, consulta [Abilitazione e disabilitazione dell'autenticazione del database IAM](#) nella Guida per l'utente di Amazon Aurora.

[RDS.13] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati

Requisiti correlati: CIS AWS Foundations Benchmark v3.0.0/2.3.2, NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoria: Rileva > Gestione delle vulnerabilità e delle patch

Gravità: alta

Tipo di risorsa: AWS::RDS::DBInstance

Regola AWS Config : [rds-automatic-minor-version-upgrade-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se gli aggiornamenti automatici delle versioni secondarie sono abilitati per l'istanza del database RDS.

L'abilitazione degli aggiornamenti automatici delle versioni secondarie garantisce l'installazione degli ultimi aggiornamenti delle versioni secondarie del sistema di gestione del database relazionale (RDBMS). Questi aggiornamenti potrebbero includere patch di sicurezza e correzioni di bug. Mantenersi aggiornati sull'installazione delle patch è un passaggio importante per proteggere i sistemi.

Correzione

Per abilitare gli aggiornamenti automatici delle versioni secondarie per un'istanza DB esistente, consulta [Modificare un'istanza DB Amazon RDS](#) nella Amazon RDS User Guide. Per l'aggiornamento automatico delle versioni secondarie, seleziona Sì.

[RDS.14] I cluster Amazon Aurora devono avere il backtracking abilitato

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SI-13 (5)

Categoria: Ripristino > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [aurora-mysql-backtracking-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personali zzati consentiti	Valore predefinito di Security Hub
BacktrackWindowInHours	Numero di ore per il backtrack di un cluster Aurora MySQL	Doppio	0.1 Da a 72	Nessun valore predefinito

Questo controllo verifica se un cluster Amazon Aurora ha il backtracking abilitato. Il controllo fallisce se il backtracking non è abilitato nel cluster. Se si fornisce un valore personalizzato per il BacktrackWindowInHours parametro, il controllo passa solo se il cluster viene eseguito a ritroso per il periodo di tempo specificato.

I backup consentono di ripristinare più rapidamente un incidente di sicurezza. Inoltre, rafforzano la resilienza dei sistemi. Il backtracking di Aurora riduce il tempo necessario per ripristinare un database a un determinato punto nel tempo. A tale scopo, non è necessario ripristinare il database.

Correzione

Per abilitare il backtracking di Aurora, consulta [Configurazione del backtracking nella Guida per l'utente](#) di Amazon Aurora.

Tieni presente che non puoi abilitare il backtracking su un cluster esistente. Puoi invece creare un clone con il backtracking abilitato. Per ulteriori informazioni sulle limitazioni del backtracking di Aurora, consulta l'elenco delle limitazioni in [Panoramica](#) del backtracking.

[RDS.15] I cluster RDS DB devono essere configurati per più zone di disponibilità

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 SC-36, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [rds-cluster-multi-az-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'alta disponibilità è abilitata per i cluster DB RDS. Il controllo fallisce se un cluster RDS DB non è distribuito in più zone di disponibilità (AZ).

I cluster RDS DB devono essere configurati per più AZ per garantire la disponibilità dei dati archiviati. L'implementazione su più AZ consente il failover automatico in caso di problemi di disponibilità AZ e durante i normali eventi di manutenzione RDS.

Correzione

Per distribuire i tuoi cluster DB in più AZ, [modifica di un'istanza DB per renderla un'istanza DB Multi-AZ nella Amazon RDS User Guide](#).

I passaggi di riparazione sono diversi per i database globali di Aurora. Per configurare più zone di disponibilità per un database globale Aurora, seleziona il tuo cluster DB. Quindi, scegli Azioni e Aggiungi lettore e specifica più AZ. Per ulteriori informazioni, consulta [Aggiungere repliche Aurora a un cluster DB](#) nella Amazon Aurora User Guide.

[RDS.16] I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificazione > Inventario

Gravità: bassa

Tipo di risorsa: AWS::RDS::DBCluster

AWS Config regola: `rds-cluster-copy-tags-to-snapshots-enabled` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i cluster RDS DB sono configurati per copiare tutti i tag nelle istantanee al momento della creazione delle istantanee.

L'identificazione e l'inventario delle risorse IT sono un aspetto cruciale della governance e della sicurezza. È necessario disporre della visibilità di tutti i cluster DB RDS in modo da poterne valutare il livello di sicurezza e intervenire sulle potenziali aree di debolezza. Le istantanee devono essere etichettate nello stesso modo dei cluster di database RDS principali. L'attivazione di questa impostazione garantisce che le istantanee ereditino i tag dei cluster di database principali.

Correzione

Per copiare automaticamente i tag negli snapshot per un cluster RDS DB, consulta [Modificare il cluster DB utilizzando la console, la CLI e l'API nella Guida per l'utente](#) di Amazon Aurora. Seleziona Copia i tag negli snapshot.

[RDS.17] Le istanze DB RDS devono essere configurate per copiare i tag nelle istantanee

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2)

Categoria: Identificazione > Inventario

Gravità: bassa

Tipo di risorsa: AWS::RDS::DBInstance

AWS Config regola: `rds-instance-copy-tags-to-snapshots-enabled` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le istanze DB RDS sono configurate per copiare tutti i tag nelle istantanee al momento della creazione delle istantanee.

L'identificazione e l'inventario delle risorse IT sono un aspetto cruciale della governance e della sicurezza. È necessario disporre della visibilità di tutte le istanze DB RDS in modo da poterne valutare il livello di sicurezza e intervenire sulle potenziali aree di debolezza. Le istantanee devono essere etichettate nello stesso modo delle istanze del database RDS principale. L'attivazione di questa impostazione garantisce che le istantanee ereditino i tag delle istanze di database principali.

Correzione

Per copiare automaticamente i tag negli snapshot per un'istanza DB RDS, consulta [Modifying an Amazon RDS DB Instance nella Amazon RDS User Guide](#). Seleziona Copia i tag negli snapshot.

[RDS.18] Le istanze RDS devono essere distribuite in un VPC

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete sicura > Risorse all'interno del VPC

Gravità: alta

Tipo di risorsa: AWS::RDS::DBInstance

AWS Config regola: `rds-deployed-in-vpc` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istanza Amazon RDS è distribuita su un VPC EC2.

I VPC forniscono una serie di controlli di rete per proteggere l'accesso alle risorse RDS. Questi controlli includono endpoint VPC, ACL di rete e gruppi di sicurezza. Per sfruttare questi controlli, ti consigliamo di creare le tue istanze RDS su un EC2-VPC.

Correzione

Per istruzioni su come spostare le istanze RDS su un VPC, consulta Aggiornamento [del VPC per un'istanza DB nella](#) Amazon RDS User Guide.

[RDS.19] Le sottoscrizioni esistenti per le notifiche di eventi RDS devono essere configurate per gli eventi critici del cluster

Requisiti correlati: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoria: Rileva > Servizi di rilevamento > Monitoraggio delle applicazioni

Gravità: bassa

Tipo di risorsa: AWS::RDS::EventSubscription

AWS Config regola: `rds-cluster-event-notifications-configured` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un abbonamento a eventi Amazon RDS esistente per cluster di database ha le notifiche abilitate per le seguenti coppie chiave-valore del tipo di origine e della categoria di evento:

```
DBCluster: ["maintenance","failure"]
```

Il controllo passa se non ci sono abbonamenti a eventi esistenti nel tuo account.

Le notifiche degli eventi RDS utilizzano Amazon SNS per informarti dei cambiamenti nella disponibilità o nella configurazione delle tue risorse RDS. Queste notifiche consentono una risposta rapida. Per ulteriori informazioni sulle notifiche degli eventi RDS, consulta [Using Amazon RDS event notification](#) nella Amazon RDS User Guide.

Correzione

Per iscriverti alle notifiche degli eventi del cluster RDS, consulta la sezione [Sottoscrizione alla notifica degli eventi di Amazon RDS](#) nella Amazon RDS User Guide. Utilizzare i seguenti valori:

Campo	Valore
Tipo di origine	Cluster
Cluster da includere	Tutti i cluster
Categorie di eventi da includere	Seleziona categorie di eventi specifiche o Tutte le categorie di eventi

[RDS.20] Le sottoscrizioni di notifica degli eventi RDS esistenti devono essere configurate per gli eventi critici delle istanze di database

Requisiti correlati: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoria: Rileva > Servizi di rilevamento > Monitoraggio delle applicazioni

Gravità: bassa

Tipo di risorsa: AWS::RDS::EventSubscription

AWS Config regola: rds-instance-event-notifications-configured (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un abbonamento ad eventi Amazon RDS esistente per le istanze di database ha le notifiche abilitate per le seguenti coppie chiave-valore del tipo di origine e della categoria di evento:

```
DBInstance: ["maintenance","configuration change","failure"]
```

Il controllo passa se non ci sono abbonamenti a eventi esistenti nel tuo account.

Le notifiche degli eventi RDS utilizzano Amazon SNS per informarti dei cambiamenti nella disponibilità o nella configurazione delle tue risorse RDS. Queste notifiche consentono una risposta rapida. Per ulteriori informazioni sulle notifiche degli eventi RDS, consulta [Using Amazon RDS event notification](#) nella Amazon RDS User Guide.

Correzione

Per iscriverti alle notifiche degli eventi delle istanze RDS, consulta la sezione [Sottoscrizione alla notifica degli eventi di Amazon RDS](#) nella Amazon RDS User Guide. Utilizzare i seguenti valori:

Campo	Valore
Tipo di origine	Istanze
Istanze da includere	Tutte le istanze
Categorie di eventi da includere	Seleziona categorie di eventi specifiche o Tutte le categorie di eventi

[RDS.21] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici del gruppo di parametri del database

Requisiti correlati: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoria: Rileva > Servizi di rilevamento > Monitoraggio delle applicazioni

Gravità: bassa

Tipo di risorsa: AWS::RDS::EventSubscription

AWS Config regola: rds-pg-event-notifications-configured (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se esiste un abbonamento ad Amazon RDS per eventi con le notifiche abilitate per le seguenti coppie chiave-valore per tipo di sorgente, categoria di evento.

```
DBParameterGroup: ["configuration change"]
```

Le notifiche degli eventi RDS utilizzano Amazon SNS per informarti dei cambiamenti nella disponibilità o nella configurazione delle tue risorse RDS. Queste notifiche consentono una risposta rapida. Per ulteriori informazioni sulle notifiche degli eventi RDS, consulta [Using Amazon RDS event notification](#) nella Amazon RDS User Guide.

Correzione

Per iscriverti alle notifiche degli eventi dei gruppi di parametri del database RDS, consulta la sezione [Sottoscrizione alla notifica degli eventi di Amazon RDS](#) nella Amazon RDS User Guide. Utilizzare i seguenti valori:

Campo	Valore
Tipo di origine	Gruppi di parametri
Gruppi di parametri da includere	Tutti i gruppi di parametri
Categorie di eventi da includere	Seleziona categorie di eventi specifiche o Tutte le categorie di eventi

[RDS.22] È necessario configurare un abbonamento alle notifiche di eventi RDS per gli eventi critici dei gruppi di sicurezza del database

Requisiti correlati: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-2

Categoria: Rileva > Servizi di rilevamento > Monitoraggio delle applicazioni

Gravità: bassa

Tipo di risorsa: AWS::RDS::EventSubscription

AWS Config regola: rds-sg-event-notifications-configured (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se esiste un abbonamento ad Amazon RDS per eventi con le notifiche abilitate per le seguenti coppie chiave-valore per tipo di sorgente, categoria di evento.

```
DBSecurityGroup: ["configuration change","failure"]
```

Le notifiche degli eventi RDS utilizzano Amazon SNS per informarti dei cambiamenti nella disponibilità o nella configurazione delle tue risorse RDS. Queste notifiche consentono una risposta rapida. Per ulteriori informazioni sulle notifiche degli eventi RDS, consulta [Using Amazon RDS event notification](#) nella Amazon RDS User Guide.

Correzione

Per iscriverti alle notifiche degli eventi delle istanze RDS, consulta la sezione [Sottoscrizione alla notifica degli eventi di Amazon RDS](#) nella Amazon RDS User Guide. Utilizzare i seguenti valori:

Campo	Valore
Tipo di origine	Gruppi di sicurezza
Gruppi di sicurezza da includere	Tutti i gruppi di sicurezza
Categorie di eventi da includere	Seleziona categorie di eventi specifiche o Tutte le categorie di eventi

[RDS.23] Le istanze RDS non devono utilizzare una porta predefinita del motore di database

Requisiti correlati: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53,5 SC-7 (5)

Categoria: Protezione > Configurazione di rete protetta

Gravità: bassa

Tipo di risorsa: AWS::RDS::DBInstance

AWS Config regola: `rds-no-default-ports` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster o un'istanza RDS utilizza una porta diversa dalla porta predefinita del motore di database. Il controllo ha esito negativo se il cluster o l'istanza RDS utilizza la porta predefinita.

Se si utilizza una porta nota per distribuire un cluster o un'istanza RDS, un utente malintenzionato può indovinare le informazioni sul cluster o sull'istanza. L'utente malintenzionato può utilizzare queste informazioni insieme ad altre informazioni per connettersi a un cluster o a un'istanza RDS o ottenere informazioni aggiuntive sull'applicazione.

Quando si modifica la porta, è necessario aggiornare anche le stringhe di connessione esistenti utilizzate per connettersi alla porta precedente. È inoltre necessario controllare il gruppo di sicurezza dell'istanza DB per assicurarsi che includa una regola di ingresso che consenta la connettività sulla nuova porta.

Correzione

Per modificare la porta predefinita di un'istanza DB RDS esistente, consulta [Modifying an Amazon RDS DB](#) nella Amazon RDS User Guide. Per modificare la porta predefinita di un cluster RDS DB esistente, consulta [Modificare il cluster DB utilizzando la console, la CLI e l'API](#) nella Guida per l'utente di Amazon Aurora. Per la porta del database, modifica il valore della porta con un valore non predefinito.

[RDS.24] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Identifica > Configurazione delle risorse

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

Regola AWS Config : [rds-cluster-default-admin-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster di database Amazon RDS ha modificato il nome utente dell'amministratore rispetto al valore predefinito. Il controllo non si applica ai motori del tipo Neptune (Neptune DB) o docdb (DocumentDB). Questa regola avrà esito negativo se il nome utente dell'amministratore è impostato sul valore predefinito.

Quando crei un database Amazon RDS, devi modificare il nome utente amministratore predefinito con un valore univoco. I nomi utente predefiniti sono di dominio pubblico e devono essere modificati durante la creazione del database RDS. La modifica dei nomi utente predefiniti riduce il rischio di accessi involontari.

Correzione

Per modificare il nome utente di amministratore associato al cluster di database Amazon RDS, [crea un nuovo cluster di database RDS](#) e modifica il nome utente amministratore predefinito durante la creazione del database.

[RDS.25] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Identifica > Configurazione delle risorse

Gravità: media

Tipo di risorsa: AWS::RDS::DBInstance

Regola AWS Config : [rds-instance-default-admin-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se hai cambiato il nome utente amministrativo per le istanze di database Amazon Relational Database Service (Amazon RDS) rispetto al valore predefinito. Il controllo non si applica ai motori del tipo Neptune (Neptune DB) o docdb (DocumentDB). Il controllo ha esito negativo se il nome utente amministrativo è impostato sul valore predefinito.

I nomi utente amministrativi predefiniti sui database Amazon RDS sono di dominio pubblico. Quando crei un database Amazon RDS, devi modificare il nome utente amministrativo predefinito con un valore univoco per ridurre il rischio di accessi involontari.

Correzione

Per modificare il nome utente amministrativo associato a un'istanza di database RDS, [crea prima una nuova istanza di database RDS](#). Modifica il nome utente amministrativo predefinito durante la creazione del database.

[RDS.26] Le istanze DB RDS devono essere protette da un piano di backup

Categoria: Recover > Resilience > Backup abilitati

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-12, NIST .800-53,5 SI-13 (5)

Gravità: media

Tipo di risorsa: AWS::RDS::DBInstance

AWS Config regola: [rds-resources-protected-by-backup-plan](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personali zzati consentiti	Valore predefinito di Security Hub
backupVaultLockCheck	Il controllo restituisce un PASSED risultato se il parametro è impostato su true e la risorsa utilizza AWS Backup Vault Lock.	Booleano	true o false	Nessun valore predefinito

Questo controllo valuta se le istanze database di Amazon RDS sono coperte da un piano di backup. Questo controllo fallisce se l'istanza DB RDS non è coperta da un piano di backup. Se si imposta il backupVaultLockCheck parametro uguale a true, il controllo passa solo se l'istanza è sottoposta a backup in un vault AWS Backup bloccato.

AWS Backup è un servizio di backup completamente gestito che centralizza e automatizza il backup dei dati in tutto il mondo. Servizi AWS Con AWS Backup, è possibile creare politiche di backup denominate piani di backup. È possibile utilizzare questi piani per definire i requisiti di backup, ad esempio la frequenza con cui eseguire il backup dei dati e la durata di conservazione di tali backup. L'inclusione delle istanze DB RDS in un piano di backup consente di proteggere i dati da perdite o eliminazioni involontarie.

Correzione

Per aggiungere un'istanza DB RDS a un piano di AWS Backup backup, consulta [Assegnazione di risorse a un piano di backup nella Guida per gli sviluppatori.AWS Backup](#)

[RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

AWS Config regola: [rds-cluster-encrypted-at-rest](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster DB RDS è crittografato quando è inattivo. Il controllo ha esito negativo se un cluster RDS DB non è crittografato a riposo.

I dati inattivi si riferiscono a tutti i dati archiviati in uno spazio di archiviazione persistente e non volatile per qualsiasi durata. La crittografia aiuta a proteggere la riservatezza di tali dati, riducendo il rischio che un utente non autorizzato possa accedervi. La crittografia dei cluster RDS DB protegge i dati e i metadati dall'accesso non autorizzato. Soddisfa inoltre i requisiti di conformità per la crittografia dei file system di produzione. data-at-rest

Correzione

È possibile abilitare la crittografia a riposo quando si crea un cluster DB RDS. Non è possibile modificare le impostazioni di crittografia dopo aver creato un cluster. Per ulteriori informazioni, [consulta Encrypting an Amazon Aurora DB cluster](#) nella Amazon Aurora User Guide.

[RDS.28] I cluster RDS DB devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::RDS::DBCluster`

AWS Config regola: `tagged-rds-dbcuster` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un cluster Amazon RDS DB dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il cluster DB non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il cluster DB non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un cluster RDS DB, consulta [Tagging delle risorse Amazon RDS nella Amazon RDS User Guide](#).

[RDS.29] Gli snapshot del cluster RDS DB devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::RDS::DBClusterSnapshot

AWS Config regola: tagged-rds-dbcustersnapshot (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	una distinzione tra lettere maiuscole e minuscole.			

Questo controllo verifica se uno snapshot del cluster Amazon RDS DB contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se lo snapshot del cluster DB non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se lo snapshot del cluster DB non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a uno snapshot del cluster RDS DB, consulta [Tagging delle risorse Amazon RDS nella Amazon RDS User Guide](#).

[RDS.30] Le istanze DB RDS devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::RDS::DBInstance

AWS Config regola: tagged-rds-dbinstance (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un'istanza DB di Amazon RDS ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se l'istanza DB non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'istanza DB non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'istanza DB RDS, consulta [Tagging delle risorse Amazon RDS](#) nella Amazon RDS User Guide.

[RDS.31] I gruppi di sicurezza RDS DB devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::RDS::DBSecurityGroup

AWS Config regola: tagged-rds-dbsecuritygroup (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfan	Nessun valore predefinito

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se un gruppo di sicurezza Amazon RDS DB dispone di tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il gruppo di sicurezza DB non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di sicurezza DB non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un gruppo di sicurezza RDS DB, consulta [Tagging delle risorse Amazon RDS](#) nella Amazon RDS User Guide.

[RDS.32] Gli snapshot RDS DB devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS :: RDS :: DBSnapshot

AWS Config regola: tagged-rds-dbsnapshot (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se uno snapshot di Amazon RDS DB contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se lo snapshot DB non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se lo snapshot DB non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a uno snapshot DB RDS, consulta [Tagging delle risorse Amazon RDS nella Amazon RDS User Guide](#).

[RDS.33] I gruppi di sottoreti RDS DB devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::RDS::DBSubnetGroup

AWS Config regola: tagged-rds-dbsubnetgroups (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfan	Nessun valore predefinito

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se un gruppo di sottoreti Amazon RDS DB dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gruppo di sottoreti DB non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di sottorete DB non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un sottogruppo di database RDS, consulta [Tagging delle risorse Amazon RDS nella Amazon RDS User Guide](#).

[RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo nei registri CloudWatch

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIS.800-53.R 5 SI-4 (20), NIST.800-53.R5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

AWS Config regola: [rds-aurora-mysql-audit-logging-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Aurora MySQL DB è configurato per pubblicare log di audit su Amazon Logs. CloudWatch Il controllo fallisce se il cluster non è configurato per pubblicare i log di controllo su Logs. CloudWatch

I registri di controllo registrano le attività del database, inclusi i tentativi di accesso, le modifiche dei dati, le modifiche allo schema e altri eventi che possono essere verificati per scopi di sicurezza e conformità. Quando configuri un cluster Aurora MySQL DB per pubblicare i log di controllo in un gruppo di log in Amazon CloudWatch Logs, puoi eseguire analisi in tempo reale dei dati di log. CloudWatch Logs conserva i log in uno storage altamente durevole. Puoi anche creare allarmi e visualizzare le metriche in. CloudWatch

Note

Un modo alternativo per pubblicare i log di controllo su CloudWatch Logs consiste nell'abilitare il controllo avanzato e impostare il parametro DB a livello di cluster su. `server_audit_logs_upload 1` L'impostazione predefinita per è. `server_audit_logs_upload parameter 0` Tuttavia, per passare questo controllo, si consiglia di utilizzare le seguenti istruzioni di riparazione.

Correzione

Per pubblicare i log di audit del cluster Aurora MySQL DB su Logs, CloudWatch consulta [Pubblicazione dei log di Amazon Aurora MySQL su Amazon Logs nella Amazon Aurora User Guide](#).
CloudWatch

[RDS.35] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie

Requisiti correlati: NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.800-53.r5 SI-2 (5)

Categoria: Rileva > Gestione di vulnerabilità, patch e versioni

Gravità: media

Tipo di risorsa: AWS::RDS::DBCluster

AWS Config regola: [rds-cluster-auto-minor-version-upgrade-enable](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'aggiornamento automatico della versione secondaria è abilitato per un cluster Amazon RDS Multi-AZ DB. Il controllo fallisce se l'aggiornamento automatico della versione secondaria non è abilitato per il cluster DB Multi-AZ.

RDS fornisce l'aggiornamento automatico delle versioni secondarie in modo da poter mantenere aggiornato il cluster DB Multi-AZ. Le versioni minori possono introdurre nuove funzionalità software, correzioni di bug, patch di sicurezza e miglioramenti delle prestazioni. Abilitando l'aggiornamento automatico delle versioni secondarie sui cluster di database RDS, il cluster, insieme alle istanze del cluster, riceverà aggiornamenti automatici alla versione secondaria quando saranno disponibili nuove versioni. Gli aggiornamenti vengono applicati automaticamente durante la finestra di manutenzione.

Correzione

Per abilitare l'aggiornamento automatico delle versioni secondarie sui cluster DB Multi-AZ, consulta [Modificare un cluster DB Multi-AZ nella Amazon RDS User Guide](#).

Controlli Amazon Redshift

Questi controlli sono correlati alle risorse di Amazon Redshift.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[Redshift.1] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico

Requisiti correlati: PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.2, PCI DSS versione 3.2.1/1.3.4, PCI DSS versione 3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20) 3.5 SC-7 (21), NIT 800-53.r5 SC-7 (3), NIT 800-53.5 SC-7 (4), NIT 800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete sicura > Risorse non accessibili al pubblico

Severità: critica

Tipo di risorsa: AWS::Redshift::Cluster

Regola AWS Config : [redshift-cluster-public-access-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i cluster Amazon Redshift sono accessibili pubblicamente. Valuta il `PubliclyAccessible` campo nell'elemento di configurazione del cluster.

L'`PubliclyAccessible` attributo della configurazione del cluster Amazon Redshift indica se il cluster è accessibile pubblicamente. Quando il cluster è configurato con `PubliclyAccessible` set to `true`, si tratta di un'istanza connessa a Internet con un nome DNS risolvibile pubblicamente, che si risolve in un indirizzo IP pubblico.

Quando il cluster non è accessibile pubblicamente, si tratta di un'istanza interna con un nome DNS che si risolve in un indirizzo IP privato. A meno che non si intenda rendere il cluster accessibile pubblicamente, il cluster non deve essere configurato con `PubliclyAccessible` set to `true`.

Correzione

Per aggiornare un cluster Amazon Redshift per disabilitare l'accesso pubblico, consulta [Modifying a cluster](#) nella Amazon Redshift Management Guide. Imposta l'accesso pubblico su No.

[Redshift.2] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito

Requisiti correlati: NIST.800-53.r5 AC-4, NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (1) -53,5 SC-8 (2)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: AWS::Redshift::Cluster AWS::Redshift::ClusterParameterGroup

Regola AWS Config : [redshift-require-tls-ssl](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se le connessioni ai cluster Amazon Redshift sono necessarie per utilizzare la crittografia in transito. Il controllo ha esito negativo se il parametro del cluster Amazon Redshift `require_SSL` non è impostato su `True`

Il TLS può essere usato per impedire a potenziali aggressori di utilizzare person-in-the-middle o attacchi simili per intercettare o manipolare il traffico di rete. Dovrebbero essere consentite solo le connessioni crittografate tramite TLS. La crittografia dei dati in transito può influire sulle prestazioni. È consigliabile testare l'applicazione con questa funzionalità per comprendere il profilo delle prestazioni e l'impatto del TLS.

Correzione

Per aggiornare un gruppo di parametri Amazon Redshift per richiedere la crittografia, consulta [Modificare un gruppo di parametri](#) nella Amazon Redshift Management Guide. Impostato su **`require_ssl` True**.

[Redshift.3] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SC-7 (10), NIT. 800-53,5 SI-13 (5)

Categoria: Recupero > Resilienza > Backup abilitati

Gravità: media

Tipo di risorsa: AWS::Redshift::Cluster

Regola AWS Config : [redshift-backup-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personali zzati consentiti	Valore predefinito di Security Hub
MinRetentionPeriod	Periodo minimo di conservazione delle istantanee in giorni	Numero intero	7 Da a 35	7

Questo controllo verifica se un cluster Amazon Redshift ha abilitato le istantanee automatiche e un periodo di conservazione maggiore o uguale al periodo di tempo specificato. Il controllo fallisce se le istantanee automatiche non sono abilitate per il cluster o se il periodo di conservazione è inferiore al periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di conservazione delle istantanee, Security Hub utilizza un valore predefinito di 7 giorni.

I backup consentono di ripristinare più rapidamente un incidente di sicurezza. Rafforzano la resilienza dei sistemi. Amazon Redshift acquisisce istantanee periodiche per impostazione predefinita. Questo controllo verifica se le istantanee automatiche sono abilitate e conservate per almeno sette giorni. Per ulteriori dettagli sugli snapshot automatizzati di Amazon Redshift, consulta la sezione [Istantanee automatizzate](#) nella Amazon Redshift Management Guide.

Correzione

Per aggiornare il periodo di conservazione degli snapshot per un cluster Amazon Redshift, [consulta Modifying a](#) cluster nella Amazon Redshift Management Guide. Per Backup, imposta la conservazione delle istantanee su un valore pari o superiore a 7.

[Redshift.4] I cluster Amazon Redshift devono avere la registrazione di controllo abilitata

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIS.800-53.R 5 SI-4 (20), NID 800-53.R 5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::Redshift::Cluster

AWS Config regola: `redshift-cluster-audit-logging-enabled` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

- `loggingEnabled = true`(non personalizzabile)

Questo controllo verifica se in un cluster Amazon Redshift è abilitata la registrazione di audit.

La registrazione di controllo di Amazon Redshift fornisce informazioni aggiuntive sulle connessioni e sulle attività degli utenti nel cluster. Questi dati possono essere archiviati e protetti in Amazon S3 e possono essere utili per controlli e indagini di sicurezza. Per ulteriori informazioni, consulta [Database audit logging](#) nella Amazon Redshift Management Guide.

Correzione

Per configurare la registrazione di audit per un cluster Amazon Redshift, [consulta Configurazione del controllo con la](#) console nella Amazon Redshift Management Guide.

[Redshift.6] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-2, NIST.800-53.r5 SI-2 (2), NIST.800-53.r5 SI-2 (4), NIST.IST .800-53,5 SI-2 (5)

Categoria: Rileva > Gestione delle vulnerabilità e delle patch

Gravità: media

Tipo di risorsa: AWS::Redshift::Cluster

Regola AWS Config : [redshift-cluster-maintenancesettings-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `allowVersionUpgrade = true`(non personalizzabile)

Questo controllo verifica se gli upgrade automatici delle versioni principali sono abilitati per il cluster Amazon Redshift.

L'abilitazione degli aggiornamenti automatici delle versioni principali garantisce che gli ultimi aggiornamenti delle versioni principali dei cluster Amazon Redshift vengano installati durante la finestra di manutenzione. Questi aggiornamenti potrebbero includere patch di sicurezza e correzioni di bug. Mantenersi aggiornati sull'installazione delle patch è un passaggio importante per proteggere i sistemi.

Correzione

Per risolvere questo problema da AWS CLI, utilizza il comando `Amazon modify-cluster Redshift` per impostare `--allow-version-upgrade` l'attributo.

```
aws redshift modify-cluster --cluster-identifier clustername --allow-version-upgrade
```

clustername Dov'è il nome del tuo cluster Amazon Redshift.

[Redshift.7] I cluster Redshift devono utilizzare un routing VPC avanzato

Requisiti correlati: NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (4), NIST.800-53,5 SC-7 (9)

Categoria: Protezione > Configurazione di rete sicura > Accesso privato alle API

Gravità: media

Tipo di risorsa: AWS::Redshift::Cluster

Regola AWS Config : [redshift-enhanced-vpc-routing-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Redshift è EnhancedVpcRouting abilitato.

Il routing VPC migliorato impone a tutto il UNLOAD traffico tra il cluster COPY e gli archivi di dati di passare attraverso il tuo VPC. Puoi quindi utilizzare funzionalità VPC come gruppi di sicurezza e liste di controllo degli accessi alla rete per proteggere il traffico di rete. Puoi anche utilizzare VPC Flow Logs per monitorare il traffico di rete.

Correzione

Per istruzioni dettagliate sulla riparazione, consulta Enhancing [Enhanced VPC](#) routing nella Amazon Redshift Management Guide.

[Redshift.8] I cluster Amazon Redshift non devono utilizzare il nome utente predefinito di amministratore

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Identifica > Configurazione delle risorse

Gravità: media

Tipo di risorsa: AWS::Redshift::Cluster

Regola AWS Config : [redshift-default-admin-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Redshift ha modificato il nome utente dell'amministratore rispetto al valore predefinito. Questo controllo avrà esito negativo se il nome utente di amministratore per un cluster Redshift è impostato su. `awsuser`

Quando si crea un cluster Redshift, è necessario modificare il nome utente amministratore predefinito con un valore univoco. I nomi utente predefiniti sono di dominio pubblico e devono essere modificati al momento della configurazione. La modifica dei nomi utente predefiniti riduce il rischio di accessi involontari.

Correzione

Non puoi modificare il nome utente di amministratore per il tuo cluster Amazon Redshift dopo che è stato creato. Per creare un nuovo cluster, segui le istruzioni riportate [qui](#).

[Redshift.9] I cluster Redshift non devono utilizzare il nome di database predefinito

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Identifica > Configurazione delle risorse

Gravità: media

Tipo di risorsa: `AWS::Redshift::Cluster`

Regola AWS Config : [redshift-default-db-name-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un cluster Amazon Redshift ha modificato il nome del database rispetto al valore predefinito. Il controllo avrà esito negativo se il nome del database per un cluster Redshift è impostato su. `dev`

Quando si crea un cluster Redshift, è necessario modificare il nome del database predefinito con un valore univoco. I nomi predefiniti sono di dominio pubblico e devono essere modificati al momento

della configurazione. Ad esempio, un nome noto potrebbe portare ad un accesso involontario se utilizzato in condizioni di policy IAM.

Correzione

Non puoi modificare il nome del database per il tuo cluster Amazon Redshift dopo la sua creazione. Per istruzioni sulla creazione di un nuovo cluster, consulta [Getting started with Amazon Redshift nella Amazon Redshift Getting Started Guide](#).

[Redshift.10] I cluster Redshift devono essere crittografati a riposo

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::Redshift::Cluster

Regola AWS Config : [redshift-cluster-kms-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se i cluster Amazon Redshift sono crittografati quando sono inattivi. Il controllo fallisce se un cluster Redshift non è crittografato a riposo o se la chiave di crittografia è diversa dalla chiave fornita nel parametro della regola.

In Amazon Redshift è possibile attivare la crittografia del database per i cluster per proteggere ulteriormente i dati a riposo. Quando si attiva la crittografia per un cluster, i blocchi di dati e i metadati di sistema vengono crittografati per il cluster e i relativi snapshot. La crittografia dei dati inattivi è una best practice consigliata perché aggiunge un livello di gestione degli accessi ai dati. La crittografia dei cluster Redshift a riposo riduce il rischio che un utente non autorizzato possa accedere ai dati archiviati su disco.

Correzione

Per modificare un cluster Redshift per utilizzare la crittografia KMS, consulta [Changing cluster encryption](#) nella Amazon Redshift Management Guide.

[Redshift.11] I cluster Redshift devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Redshift::Cluster`

AWS Config regola: `tagged-redshift-cluster` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un cluster Amazon Redshift dispone di tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il cluster non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il cluster non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una

singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui, AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un cluster Redshift, consulta [Tagging resources in Amazon Redshift nella Amazon Redshift Management Guide](#).

[Redshift.12] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::Redshift::EventSubscription

AWS Config regola: tagged-redshift-eventsubscription (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfano	No default value

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se uno snapshot del cluster Amazon Redshift contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se lo snapshot del cluster non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se lo snapshot del cluster non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un abbonamento di notifica di eventi Redshift, consulta [Tagging resources in Amazon Redshift nella Amazon Redshift Management Guide](#).

[Redshift.13] Le istantanee del cluster Redshift devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Redshift::ClusterSnapshot`

AWS Config regola: `tagged-redshift-clustersnapshot` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se uno snapshot del cluster Amazon Redshift contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se lo snapshot del cluster non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se lo snapshot del cluster non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a uno snapshot del cluster Redshift, consulta [Tagging resources in Amazon Redshift nella Amazon Redshift Management Guide](#).

[Redshift.14] I gruppi di sottoreti del cluster Redshift devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::Redshift::ClusterSubnetGroup

AWS Config regola: tagged-redshift-clustersubnetgroup (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfan	No default value

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se un sottogruppo di cluster Amazon Redshift ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se il gruppo di sottoreti del cluster non dispone di chiavi di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il gruppo di sottorete del cluster non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un sottogruppo di cluster Redshift, consulta [Tagging resources in Amazon Redshift nella Amazon Redshift Management Guide](#).

[Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate

Categoria: Protezione > Configurazione di rete sicura > Configurazione del gruppo di sicurezza

Gravità: alta

Tipo di risorsa: AWS::Redshift::Cluster

Regola AWS Config : [redshift-unrestricted-port-access](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un gruppo di sicurezza associato a un cluster Amazon Redshift ha regole di ingresso che consentono l'accesso alla porta del cluster da Internet (0.0.0.0/0 o :/0). Il controllo fallisce se le regole di ingresso del gruppo di sicurezza consentono l'accesso alla porta del cluster da Internet.

Consentire l'accesso in entrata senza restrizioni alla porta del cluster Redshift (indirizzo IP con suffisso /0) può causare accessi non autorizzati o incidenti di sicurezza. Si consiglia di applicare il principio dell'accesso con privilegi minimi durante la creazione di gruppi di sicurezza e la configurazione delle regole in entrata.

Correzione

Per limitare l'ingresso sulla porta del cluster Redshift a origini limitate, [consulta Work with security group](#) rules nella Amazon VPC User Guide. Aggiorna le regole in cui l'intervallo di porte corrisponde alla porta del cluster Redshift e l'intervallo di porte IP è 0.0.0.0/0.

Controlli Amazon Route 53

Questi controlli sono correlati alle risorse della Route 53.

Questi controlli potrebbero non essere disponibili in tutti le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[Route53.1] I controlli sanitari della Route 53 devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::Route53::HealthCheck`

AWS Config regola: `tagged-route53-healthcheck` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un controllo dello stato di Amazon Route 53 contiene tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il controllo dello stato non contiene alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il controllo di integrità non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un controllo di integrità della Route 53, consulta i [controlli di integrità di denominazione e etichettatura](#) nella Amazon Route 53 Developer Guide.

[Route53.2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIS.800-53.R 5 SI-4 (20), NID 800-53.R 5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::Route53::HostedZone

Regola AWS Config : [route53-query-logging-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la registrazione delle query DNS è abilitata per una zona ospitata pubblica di Amazon Route 53. Il controllo fallisce se la registrazione delle query DNS non è abilitata per una zona ospitata pubblicamente su Route 53.

La registrazione delle query DNS per una zona ospitata su Route 53 soddisfa i requisiti di sicurezza e conformità DNS e garantisce la visibilità. I log includono informazioni quali il dominio o il sottodominio su cui è stata eseguita la query, la data e l'ora della query, il tipo di record DNS (ad esempio, A o AAAA) e il codice di risposta DNS (ad esempio o). NoError ServFail Quando la registrazione delle query DNS è abilitata, Route 53 pubblica i file di registro su Amazon Logs. CloudWatch

Correzione

Per registrare le query DNS per le zone ospitate pubbliche di Route 53, consulta [Configurazione della registrazione per le query DNS nella Amazon Route 53 Developer Guide](#).

Controlli di Amazon Simple Storage Service

Questi controlli sono correlati alle risorse Amazon S3.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[S3.1] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate

Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: benchmark CIS AWS Foundations versione 3.0.0/2.1.4, benchmark CIS AWS Foundations versione 1.4.0/2.1.5, PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.2, PCI DSS v3.2.1/1.3.4, PCI DSS v3.2.1/1.3.6, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIS.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9))

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: AWS :: Account

Regola AWS Config : [s3-account-level-public-access-blocks-periodic](#)

Tipo di pianificazione: periodica

Parametri:

- `ignorePublicAcls: true` (non personalizzabile)
- `blockPublicPolicy: true` (non personalizzabile)
- `blockPublicAcls: true` (non personalizzabile)
- `restrictPublicBuckets: true` (non personalizzabile)

Questo controllo verifica se le precedenti impostazioni di accesso pubblico a blocchi di Amazon S3 sono configurate a livello di account per un bucket S3 generico. Il controllo fallisce se una o più impostazioni di accesso pubblico a blocchi sono impostate su `false`.

Il controllo ha esito negativo se una delle impostazioni è impostata su `o` se una delle impostazioni non è configurata su `false`.

Il blocco di accesso pubblico di Amazon S3 è progettato per fornire controlli su un intero bucket S3 Account AWS o a livello di singolo bucket S3 per garantire che gli oggetti non abbiano mai accesso pubblico. L'accesso pubblico viene concesso a bucket e oggetti tramite liste di controllo accessi (ACL), policy di bucket o entrambi.

A meno che tu non intenda rendere i tuoi bucket S3 accessibili al pubblico, devi configurare la funzionalità Amazon S3 Block Public Access a livello di account.

Per ulteriori informazioni, consulta [Using Amazon S3 Block Public Access](#) nella Guida per l'utente di Amazon Simple Storage Service.

Correzione

Per abilitare Amazon S3 Block Public Access per il tuo account Account AWS, consulta [Configurazione delle impostazioni di accesso pubblico a blocchi per il tuo account nella Guida per l'utente](#) di Amazon Simple Storage Service.

[S3.2] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura

Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.2, PCI DSS versione 3.2.1/1.3.6, PCI DSS versione 3.2.1/7.2.1, NIST.800-53.r5 AC-21,

NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20) 3.5 SC-7 (21), NIT 800-53.r5 SC-7 (3), NIT 800-53.5 SC-7 (4), NIT 800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: AWS :: S3 :: Bucket

Regola AWS Config : [s3-bucket-public-read-prohibited](#)

Tipo di pianificazione: periodica e con attivazione di modifiche

Parametri: nessuno


Questo controllo verifica se un bucket Amazon S3 per uso generico consente l'accesso pubblico in lettura. Esamina le impostazioni di blocco dell'accesso pubblico, la policy del bucket e la lista di controllo accessi (ACL) del bucket. Il controllo fallisce se il bucket consente l'accesso pubblico in lettura.

Alcuni casi d'uso potrebbero richiedere che tutti gli utenti di Internet siano in grado di leggere dal tuo bucket S3. Tuttavia, queste situazioni sono rare. Per garantire l'integrità e la sicurezza dei dati, il bucket S3 non deve essere leggibile pubblicamente.

Correzione

Per bloccare l'accesso pubblico in lettura sui tuoi bucket Amazon S3, consulta [Configurazione delle impostazioni di accesso pubblico a blocchi per i tuoi bucket S3 nella Guida per l'utente di Amazon Simple Storage Service](#).

[S3.3] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura

 Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.2, PCI DSS versione 3.2.1/1.3.4, PCI DSS versione 3.2.1/1.3.6, PCI DSS versione

3.2.1/7.2.1, NIST.800-53.r5 AC-21, nIST.800-53.r5 AC-3, nIST.800-53.r5 AC-3 800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.5 SC-7 (20), NIS.800-53.r5 SC-7 (21), NIS.800-53.r5 SC-7 (3), NIT.800-53.r5 SC-7 (4), NIT.800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete protetta

Severità: critica

Tipo di risorsa: AWS :: S3 :: Bucket

Regola AWS Config : [s3-bucket-public-write-prohibited](#)

Tipo di pianificazione: periodica e con attivazione di modifiche

Parametri: nessuno


Questo controllo verifica se un bucket Amazon S3 per uso generico consente l'accesso pubblico in scrittura. Esamina le impostazioni di blocco dell'accesso pubblico, la policy del bucket e la lista di controllo accessi (ACL) del bucket. Il controllo fallisce se il bucket consente l'accesso pubblico in scrittura.

Alcuni casi d'uso prevedono che chiunque su Internet sia in grado di scrivere nel bucket S3. Tuttavia, queste situazioni sono rare. Per garantire l'integrità e la sicurezza dei dati, il bucket S3 non deve essere scrivibile pubblicamente.

Correzione

Per bloccare l'accesso pubblico in scrittura sui tuoi bucket Amazon S3, consulta [Configurazione delle impostazioni di accesso pubblico a blocchi per i tuoi bucket S3 nella Guida per l'utente di Amazon Simple Storage Service](#).

[S3.5] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL

 Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: benchmark CIS AWS Foundations versione 3.0.0/2.1.1, benchmark CIS AWS Foundations versione 1.4.0/2.1.2, PCI DSS versione 3.2.1/4.1, NIST.800-53.r5 AC-17 (2),

NIST.800-53.r5 AC-4, NIST.800-53.r5 IA-5 (1), nIST.800-53.r5 SC-12 (3), nIST.800-53.r5 800-53.r5 SC-13, NIT.800-53.r5 SC-23, NIST.800-53.r5 SC-23 (3), NIT.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-8, NIST.800-53.r5 SC-8 (1), NIST.800-53.r5 SC-8 (2), NIST.800-53.r5 SC-8 (2) 5 SI-7 (6)

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS::S3::Bucket

Regola AWS Config : [s3-bucket-ssl-requests-only](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un bucket Amazon S3 per uso generico ha una politica che richiede richieste di utilizzo di SSL. Il controllo fallisce se la policy del bucket non richiede richieste di utilizzo di SSL.

I bucket S3 devono avere politiche che richiedono che tutte le richieste (Action: S3:*) accettino solo la trasmissione di dati tramite HTTPS nella politica delle risorse S3, indicata dalla chiave di condizione. aws:SecureTransport

Correzione

Per aggiornare una policy sui bucket di Amazon S3 per impedire il trasporto non sicuro, consulta [Aggiungere una policy sui bucket utilizzando la console Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service](#).


Aggiungi una dichiarazione di policy simile a quella riportata nella seguente policy. Sostituiscilo DOC-EXAMPLE-BUCKET con il nome del bucket che stai modificando.

```
{
  "Id": "ExamplePolicy",
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSSLRequestsOnly",
      "Action": "s3:*",
      "Effect": "Deny",
      "Resource": [
```

```
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET",
        "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*"
    ],
    "Condition": {
        "Bool": {
            "aws:SecureTransport": "false"
        }
    },
    "Principal": "*"
}
]
```

Per ulteriori informazioni, consulta [Quale policy sui bucket S3 devo usare per rispettare la AWS Config regola s3-? bucket-ssl-requests-only](#) nel Knowledge Center AWS ufficiale.

[S3.6] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS

 Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Gestione sicura degli accessi > Azioni operative API sensibili limitate

Gravità: alta

Tipo di risorsa: AWS::S3::Bucket

Regola AWS Config: [s3-bucket-blacklisted-actions-prohibited](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `blacklistedactionpatterns: s3:DeleteBucketPolicy, s3:PutBucketAcl, s3:PutBucketPolicy, s3:PutEncryptionConfiguration, s3:PutObjectAcl` (non personalizzabile)

Questo controllo verifica se una policy sui bucket generici di Amazon S3 impedisce ai principali di eseguire azioni negate sulle risorse nel bucket S3. Account AWS Il controllo fallisce se la bucket policy consente una o più delle azioni precedenti per un principale in un altro. Account AWS

L'implementazione dell'accesso con privilegi minimi è fondamentale per ridurre i rischi per la sicurezza e l'impatto di errori o intenzioni malevole. Se una policy S3 bucket consente l'accesso da account esterni, potrebbe causare l'esfiltrazione dei dati da parte di una minaccia interna o di un aggressore.

Il `blacklistedactionpatterns` parametro consente una valutazione corretta della regola per i bucket S3. Il parametro consente l'accesso agli account esterni per i modelli di azione che non sono inclusi nell'elenco. `blacklistedactionpatterns`

Correzione

Per aggiornare una policy sui bucket di Amazon S3 per rimuovere le autorizzazioni, consulta.

[Aggiungere una policy bucket utilizzando la console Amazon S3 nella Guida per l'utente di Amazon Simple Storage Service.](#)

Nella pagina Modifica policy bucket, nella casella di testo per la modifica della policy, esegui una delle seguenti azioni:

- Rimuovi le dichiarazioni che concedono ad altri Account AWS l'accesso alle azioni negate.
- Rimuovi le azioni negate consentite dalle dichiarazioni.

[S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni

Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: PCI DSS versione 3.2.1/2.2, NIST.800-53.r5 AU-9 (2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, nist.800-53.r5 SC-36 (2), NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: bassa

Tipo di risorsa: AWS::S3::Bucket

AWS Config regola: [s3-bucket-cross-region-replication-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se in un bucket Amazon S3 per uso generico è abilitata la replica tra regioni. Il controllo fallisce se nel bucket non è abilitata la replica tra regioni.

La replica è la copia automatica e asincrona di oggetti tra bucket uguali o diversi. Regioni AWS La replica copia gli oggetti appena creati e gli aggiornamenti degli oggetti da un bucket di origine a uno o più bucket di destinazione. AWS le migliori pratiche consigliano la replica per i bucket di origine e di destinazione di proprietà degli stessi. Account AWS Oltre alla disponibilità, è necessario prendere in considerazione altre impostazioni di protezione dei sistemi.

Correzione

Per abilitare la replica tra regioni su un bucket S3, consulta [Configurazione della replica per i bucket di origine e destinazione di proprietà dello stesso account nella Guida per l'utente di Amazon Simple Storage Service](#). Per Source bucket, scegli Applica a tutti gli oggetti nel bucket.

[S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico

Requisiti correlati: benchmark CIS AWS Foundations versione 3.0.0/2.1.4, benchmark CIS AWS Foundations versione 1.4.0/2.1.5, NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-4 (21) 3.5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.5 SC-7 (4), NIT. 800-53,5 SC-7 (9)

Categoria: Protezione > Gestione sicura degli accessi > Controllo degli accessi

Gravità: alta

Tipo di risorsa: AWS::S3::Bucket

Regola AWS Config : [s3-bucket-level-public-access-prohibited](#)

Tipo di pianificazione: modifica attivata

Parametri:

- `excludedPublicBuckets`(non personalizzabile): un elenco separato da virgole di nomi di bucket S3 pubblici e noti e consentiti

Questo controllo verifica se un bucket generico Amazon S3 blocca l'accesso pubblico a livello di bucket. Il controllo fallisce se una delle seguenti impostazioni è impostata su: `false`

- `ignorePublicAcls`
- `blockPublicPolicy`
- `blockPublicAcls`
- `restrictPublicBuckets`

Block Public Access a livello di bucket S3 fornisce controlli per garantire che gli oggetti non abbiano mai accesso pubblico. L'accesso pubblico viene concesso a bucket e oggetti tramite liste di controllo accessi (ACL), policy di bucket o entrambi.

A meno che tu non intenda rendere i tuoi bucket S3 accessibili al pubblico, devi configurare la funzionalità Amazon S3 Block Public Access a livello di bucket.

Correzione

Per informazioni su come rimuovere l'accesso pubblico a livello di bucket, consulta [Bloccare l'accesso pubblico allo storage Amazon S3 nella Amazon S3 User Guide](#).

[S3.9] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata

Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: NIST.800-53.r5 AC-2 (4), NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AC-6 (9), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-3, NIST.800-53.r5 NIST 5 AU-6 (3), NIS.800-53.R5 AU-6 (4), NIS.800-53.R5 CA-7, NIS.800-53.R5 SC-7 (9), NIS.800-53.R 5 SI-3 (8), NIS.800-53.R 5 SI-4 (20), NID 800-53.R 5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::S3::Bucket

Regola AWS Config : [s3-bucket-logging-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la registrazione degli accessi al server è abilitata per un bucket Amazon S3 per uso generico. Il controllo fallisce se la registrazione degli accessi al server non è abilitata. Quando la registrazione è abilitata, Amazon S3 fornisce i log di accesso per un bucket di origine a un bucket di destinazione scelto. Il bucket di destinazione deve trovarsi nello stesso Regione AWS del bucket di origine e non deve avere un periodo di conservazione predefinito configurato. Non è necessario che nel bucket di registrazione di destinazione sia abilitata la registrazione degli accessi al server ed è necessario eliminare i risultati relativi a questo bucket.

La registrazione degli accessi al server fornisce registrazioni dettagliate delle richieste effettuate a un bucket. I log di accesso al server possono aiutare nei controlli di sicurezza e di accesso. Per ulteriori informazioni, consulta [Best practice di sicurezza per Amazon S3: abilitare la registrazione degli accessi ai server Amazon S3](#).

Correzione

Per abilitare la registrazione degli accessi ai server Amazon S3, consulta [Enabling Amazon S3 server access logging nella Amazon S3 User Guide](#).

[S3.10] I bucket generici S3 con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita

 Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Security Hub ha ritirato questo controllo nell'aprile 2024 dallo standard AWS Foundational Security Best Practices, ma è ancora incluso nello standard NIST SP 800-53 Rev. 5. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::S3::Bucket

Regola AWS Config : [s3-version-lifecycle-policy-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno


Questo controllo verifica se un bucket con versione generica di Amazon S3 ha una configurazione del ciclo di vita. Il controllo fallisce se il bucket non ha una configurazione del ciclo di vita.

Ti consigliamo di creare una configurazione del ciclo di vita per il tuo bucket S3 per aiutarti a definire le azioni che desideri che Amazon S3 intraprenda durante la vita di un oggetto.

Correzione

[Per ulteriori informazioni sulla configurazione del ciclo di vita su un bucket Amazon S3, consulta Impostazione della configurazione del ciclo di vita su un bucket e Gestione del ciclo di vita dello storage.](#)

[S3.11] I bucket generici S3 devono avere le notifiche degli eventi abilitate

 Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Security Hub ha ritirato questo controllo nell'aprile 2024 dallo standard AWS Foundational Security Best Practices, ma è ancora incluso nello standard NIST SP 800-53 Rev. 5:. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: NIST.800-53.r5 CA-7, NIST.800-53.r5 SI-3 (8), NIST.800-53.r5 SI-4, NIST.800-53.r5 SI-4 (4)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::S3::Bucket

Regola AWS Config : [s3-event-notifications-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
eventTypes	Elenco dei tipi di eventi S3 preferiti	EnumList (massimo 28 articoli)	s3: IntelligentTiering, s3:LifecycleExpiration:*, s3:LifecycleExpiration:Delete, s3:LifecycleExpiration:DeleteMarkerCreated, s3:LifecycleTransition, s3:ObjectAcl:Put, s3:ObjectCreated:*, , s3:ObjectCreated:CompleteMu	Nessun valore predefinito

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
			ltipartUp load, s3:Object Created:C opy, s3:Object Created:P ost, s3:Object Created:P ut, s3:Object Removed:* , s3:Object Removed:D elete, s3:Object Removed:D eleteMark erCreated , s3:Object Restore:* , s3:Object Restore:C ompleted, s3:Object Restore:D elete, s3:Object	

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
			Restore:Post, s3:ObjectTagging:* , s3:ObjectTagging:Delete, s3:ObjectTagging:Put, s3:ReducedRedundancyLostObject, s3:Replication:*, s3:Replication:OperationFailedReplication, s3:Replication:OperationMissedThreshold, s3:Replication:OperationNotTracked, s3:Replic	

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
			ation:OperationReplicatedAfterThreshold, s3:TestEvent	

Questo controllo verifica se le notifiche degli eventi S3 sono abilitate su un bucket Amazon S3 per uso generico. Il controllo fallisce se le notifiche degli eventi S3 non sono abilitate nel bucket. Se fornisci valori personalizzati per il eventTypes parametro, il controllo passa solo se le notifiche degli eventi sono abilitate per i tipi di eventi specificati.

Quando abiliti le notifiche di eventi S3, ricevi avvisi quando si verificano eventi specifici che influiscono sui bucket S3. Ad esempio, puoi ricevere notifiche sulla creazione, la rimozione e il ripristino degli oggetti. Queste notifiche possono avvisare i team competenti in caso di modifiche accidentali o intenzionali che possono portare all'accesso non autorizzato ai dati.

Correzione

Per informazioni sul rilevamento delle modifiche ai bucket e agli oggetti S3, consulta [Amazon S3 Event Notifications nella Amazon S3 User Guide](#).

[S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3

Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6

Categoria: Proteggi > Gestione sicura degli accessi > Controllo degli accessi

Gravità: media

Tipo di risorsa: AWS::S3::Bucket

Regola AWS Config : [s3-bucket-acl-prohibited](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un bucket Amazon S3 per uso generico fornisce autorizzazioni utente con una lista di controllo degli accessi (ACL). Il controllo fallisce se un ACL è configurato per la gestione dell'accesso degli utenti al bucket.


Gli ACL sono meccanismi di controllo degli accessi legacy precedenti a IAM. Invece degli ACL, consigliamo di utilizzare le policy dei bucket S3 o le policy AWS Identity and Access Management (IAM) per gestire l'accesso ai bucket S3.

Correzione

Per passare questo controllo, devi disabilitare gli ACL per i tuoi bucket S3. Per istruzioni, consulta [Controllare la proprietà degli oggetti e disabilitare gli ACL per il tuo bucket nella Guida per l'utente di Amazon Simple Storage Service](#).

Per creare una policy per i bucket S3, consulta [Aggiungere una policy per i bucket utilizzando la console Amazon S3](#). Per creare una policy utente IAM su un bucket S3, consulta [Controllare l'accesso a un bucket con le policy utente](#).

[S3.13] I bucket generici S3 devono avere configurazioni del ciclo di vita

 Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST.800-53.r5 SI-13 (5)

Categoria: Proteggi > Protezione dei dati

Gravità: bassa

Tipo di risorsa: AWS::S3::Bucket

Regola AWS Config : [s3-lifecycle-policy-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
targetTransitionDays	Numero di giorni dopo la creazione dell'oggetto in cui gli oggetti vengono trasferiti a una classe di archiviazione specificata	Numero intero	1 Da a 36500	Nessun valore predefinito
targetExpirationDays	Numero di giorni dopo la creazione dell'oggetto in cui gli oggetti vengono eliminati	Numero intero	1 Da a 36500	Nessun valore predefinito
targetTransitionStorageClasses	Tipo di classe di archiviazione S3 di destinazione	Enum	STANDARD_IA, INTELLIGENT_TIERING, ONEZONE_IA, GLACIER, GLACIER_IR, DEEP_ARCHIVE	Nessun valore predefinito

Questo controllo verifica se un bucket Amazon S3 per uso generico ha una configurazione del ciclo di vita. Il controllo fallisce se il bucket non ha una configurazione del ciclo di vita. Se fornisci valori personalizzati per uno o più dei parametri precedenti, il controllo passa solo se la policy include la classe di archiviazione, il tempo di eliminazione o il tempo di transizione specificati.

La creazione di una configurazione del ciclo di vita per il tuo bucket S3 definisce le azioni che vuoi che Amazon S3 intraprenda durante la vita di un oggetto. Ad esempio, puoi trasferire oggetti in un'altra classe di storage, archivarli o eliminarli dopo un periodo di tempo specificato.

Correzione

Per informazioni sulla configurazione delle politiche del ciclo di vita su un bucket Amazon S3, consulta [Setting lifecycle configuration on a bucket e Managing your storage lifecycle](#) nella Amazon S3 User Guide.

[S3.14] I bucket generici S3 devono avere il controllo delle versioni abilitato

Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Requisiti correlati: NIST.800-53.r5 AU-9 (2), NIST.800-53.r5 CP-10, NIST.800-53.r5 CP-6, NIST.800-53.r5 CP-6 (1), NIST.800-53.r5 CP-6 (2), NIST.800-53.r5 CP-9, NIST.800-53.r5 SC-5 (2), NIST 800-53.R SI-12, NIT 800-53.R SI-13 (5)

Gravità: bassa

Tipo di risorsa: AWS::S3::Bucket


Regola AWS Config : [s3-bucket-versioning-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un bucket Amazon S3 per uso generico ha il controllo delle versioni abilitato. Il controllo fallisce se il controllo delle versioni è sospeso per il bucket.

Il controllo delle versioni mantiene più varianti di un oggetto nello stesso bucket S3. Puoi utilizzare il controllo delle versioni per conservare, recuperare e ripristinare versioni precedenti di un oggetto archiviato nel tuo bucket S3. Il controllo delle versioni ti aiuta a recuperare sia da azioni involontarie dell'utente che da errori delle applicazioni.


 Tip

Man mano che il numero di oggetti in un bucket aumenta a causa del controllo delle versioni, è possibile impostare una configurazione del ciclo di vita per archiviare o eliminare automaticamente gli oggetti con versioni in base a regole. Per ulteriori informazioni, consulta [Amazon S3 Lifecycle Management](#) for Versioned Objects.

Correzione

Per utilizzare il controllo delle versioni su un bucket S3, consulta [Enabling versioning on bucket nella Amazon S3 User Guide](#).

[S3.15] I bucket generici S3 devono avere Object Lock abilitato

 Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Requisiti correlati: NIST.800-53.R5 CP-6 (2)

Gravità: media

Tipo di risorsa: AWS::S3::Bucket

AWS Config regola: [s3-bucket-default-lock-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
mode	Modalità di conservazione di S3 Object Lock	Enum	GOVERNANCE, COMPLIANCE	Nessun valore predefinito

Questo controllo verifica se un bucket Amazon S3 per uso generico ha Object Lock abilitato. Il controllo fallisce se Object Lock non è abilitato per il bucket. Se fornite un valore personalizzato per il mode parametro, il controllo passa solo se S3 Object Lock utilizza la modalità di conservazione specificata.

È possibile utilizzare S3 Object Lock per memorizzare oggetti utilizzando un modello write-once-read-many (WORM). Object Lock può aiutare a impedire che gli oggetti nei bucket S3 vengano eliminati o sovrascritti per un periodo di tempo fisso o indefinitamente. Puoi utilizzare il blocco oggetti S3 per soddisfare i requisiti normativi che richiedono uno storage WORM o aggiungere un ulteriore livello di protezione contro le modifiche e l'eliminazione degli oggetti.

Correzione

Per configurare Object Lock per bucket S3 nuovi ed esistenti, consulta [Configuring S3 Object Lock nella Amazon S3 User Guide](#).

[S3.17] I bucket generici S3 devono essere crittografati quando sono inattivi con AWS KMS keys

Important

Il 12 marzo 2024, il titolo di questo controllo è cambiato in quello mostrato. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Requisiti correlati: NIST.800-53.r5 SC-12 (2), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 CA-9 1 (), NIST 800-53.R5 SI-7 (6), NIT 800-53.R5 AU-9

Gravità: media

Tipo di risorsa: AWS :: S3 :: Bucket

AWS Config regola: [s3-default-encryption-kms](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un bucket Amazon S3 per uso generico è crittografato con un AWS KMS key (SSE-KMS o DSSE-KMS). Il controllo fallisce se il bucket è crittografato con crittografia predefinita (SSE-S3).

La crittografia lato server (SSE) è la crittografia dei dati a destinazione da parte dell'applicazione o del servizio che li riceve. Se non diversamente specificato, i bucket S3 utilizzano le chiavi gestite di Amazon S3 (SSE-S3) per impostazione predefinita per la crittografia lato server. Tuttavia, per un maggiore controllo, puoi scegliere di configurare i bucket per utilizzare invece la crittografia lato server (SSE-KMS o DSSE-KMS). AWS KMS keys Amazon S3 crittografa i dati a livello di oggetto mentre li scrive su dischi nei data AWS center e li decrittografa per te quando vi accedi.

Correzione

Per crittografare un bucket S3 utilizzando SSE-KMS, consulta [Specificare la crittografia lato server con \(SSE-KMS\) nella Amazon AWS KMS S3 User Guide](#). Per crittografare un bucket S3 utilizzando DSSE-KMS, consulta [Specificare la crittografia lato server a doppio livello con \(AWS KMS keys DSSE-KMS\)](#) nella Guida per l'utente di Amazon S3.

[S3.19] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIS.800-53.r5 SC-7 (16), NIS.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Protezione > Gestione sicura degli accessi > Risorsa non accessibile al pubblico

Severità: critica

Tipo di risorsa: AWS::S3::AccessPoint

AWS Config regola: [s3-access-point-public-access-blocks](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un punto di accesso Amazon S3 ha abilitato le impostazioni di blocco dell'accesso pubblico. Il controllo fallisce se le impostazioni di blocco dell'accesso pubblico non sono abilitate per il punto di accesso.

La funzionalità Amazon S3 Block Public Access ti aiuta a gestire l'accesso alle tue risorse S3 a tre livelli: account, bucket e access point. Le impostazioni a ciascun livello possono essere configurate in modo indipendente, consentendoti di avere diversi livelli di restrizioni di accesso pubblico ai tuoi dati. Le impostazioni del punto di accesso non possono sovrascrivere individualmente le impostazioni più restrittive ai livelli superiori (livello di account o bucket assegnato al punto di accesso). Al contrario, le impostazioni a livello del punto di accesso sono additive, il che significa che completano e funzionano insieme alle impostazioni degli altri livelli. A meno che tu non voglia che un punto di accesso S3 sia accessibile al pubblico, devi abilitare le impostazioni di blocco dell'accesso pubblico.

Correzione

Amazon S3 attualmente non supporta la modifica delle impostazioni di blocco dell'accesso pubblico di un punto di accesso dopo la creazione del punto di accesso. Tutte le impostazioni di blocco dell'accesso pubblico sono abilitate per impostazione predefinita quando crei un nuovo punto di accesso. È consigliabile lasciare tutte le impostazioni abilitate, a meno che tu non debba necessariamente disabilitarne una specifica. Per ulteriori informazioni, consulta [la sezione Gestione dell'accesso pubblico agli access point](#) nella Guida per l'utente di Amazon Simple Storage Service.

[S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata

Requisiti correlati: CIS AWS Foundations Benchmark v3.0.0/2.1.2, CIS AWS Foundations Benchmark v1.4.0/2.1.3, NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2, NIST.800-53.r5 CM-2 (2), NIST.800-53.r5 CM-3, NIST.800-53.r5 SC-5 (2)

Categoria: Protezione > Protezione dei dati > Protezione dalla cancellazione dei dati

Gravità: bassa

Tipo di risorsa: AWS::S3::Bucket

AWS Config regola: [s3-bucket-mfa-delete-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'eliminazione dell'autenticazione a più fattori (MFA) è abilitata su un bucket con versione generica di Amazon S3. Il controllo fallisce se l'eliminazione MFA non è abilitata nel bucket. Il controllo non produce risultati per i bucket con una configurazione del ciclo di vita.

Quando lavori con S3 Versioning nei bucket Amazon S3, puoi facoltativamente aggiungere un altro livello di sicurezza configurando un bucket per abilitare l'eliminazione MFA. In tal caso, il proprietario del bucket deve includere due tipi di autenticazione in qualsiasi richiesta per eliminare una versione o modificare lo stato della funzione Controllo delle versioni del bucket. L'eliminazione MFA offre una maggiore sicurezza in caso di compromissione delle credenziali di sicurezza. L'eliminazione MFA può anche aiutare a prevenire le eliminazioni accidentali dei bucket richiedendo all'utente che avvia l'azione di eliminazione di dimostrare il possesso fisico di un dispositivo MFA con un codice MFA e aggiungendo un ulteriore livello di attrito e sicurezza all'azione di eliminazione.

Note

La funzionalità di eliminazione MFA richiede il controllo delle versioni del bucket come dipendenza. Il controllo delle versioni del bucket è un metodo per mantenere più varianti di un oggetto S3 nello stesso bucket. Inoltre, solo il proprietario del bucket che ha effettuato l'accesso come utente root può abilitare l'eliminazione MFA ed eseguire azioni di eliminazione sui bucket S3.

Correzione

Per abilitare S3 Versioning e configurare l'eliminazione MFA su un bucket, consulta [Configuring MFA delete](#) nella Amazon Simple Storage Service User Guide.

[S3.22] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto

Requisiti correlati: CIS Foundations Benchmark v3.0.0/3.8 AWS

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS:::Account

AWS Config regola: [cloudtrail-all-write-s3-data-event-check](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un utente Account AWS dispone di almeno un percorso AWS CloudTrail multiregionale che registra tutti gli eventi di scrittura dei dati per i bucket Amazon S3. Il controllo fallisce se l'account non dispone di un percorso multiregionale che registra gli eventi di scrittura dei dati per i bucket S3.

Le operazioni a livello di oggetto S3, ad esempio, `GetObject`, `deleteObject`, `PutObject` e `CopyObject`, sono chiamate eventi relativi ai dati. Per impostazione predefinita, CloudTrail non registra gli eventi relativi ai dati, ma puoi configurare percorsi per registrare gli eventi relativi ai dati per i bucket S3. Quando abiliti la registrazione a livello di oggetto per gli eventi di scrittura dei dati, puoi registrare l'accesso a ogni singolo oggetto (file) all'interno di un bucket S3. L'abilitazione della registrazione a livello di oggetto può aiutarti a soddisfare i requisiti di conformità dei dati, eseguire analisi di sicurezza complete, monitorare modelli specifici di comportamento degli utenti e intervenire sull'attività delle API a livello di oggetto all'interno dei tuoi bucket S3 utilizzando Amazon Events. Account AWS CloudWatch Questo controllo produce un PASSED risultato se configuri un percorso multiregionale che registra eventi di sola scrittura o tutti i tipi di dati per tutti i bucket S3.

Correzione

Per abilitare la registrazione a livello di oggetto per i bucket S3, consulta [Enabling CloudTrail event logging for S3 bucket and objects nella Amazon Simple Storage Service User Guide](#).

[S3.23] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto

Requisiti correlati: CIS Foundations Benchmark v3.0.0/3.9 AWS

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS:::Account

AWS Config regola: [cloudtrail-all-read-s3-data-event-check](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un utente Account AWS dispone di almeno un percorso AWS CloudTrail multiregionale che registra tutti gli eventi di lettura dei dati per i bucket Amazon S3. Il controllo fallisce se l'account non dispone di un percorso multiregionale che registra gli eventi dei dati di lettura per i bucket S3.

Le operazioni a livello di oggetto S3, ad esempio, `GetObject` e `DeleteObject`, sono chiamate eventi relativi ai dati. Per impostazione predefinita, CloudTrail non registra gli eventi relativi ai dati, ma puoi configurare percorsi per registrare gli eventi relativi ai dati per i bucket S3. Quando abiliti la registrazione a livello di oggetto per gli eventi di lettura dei dati, puoi registrare l'accesso a ogni singolo oggetto (file) all'interno di un bucket S3. L'abilitazione della registrazione a livello di oggetto può aiutarti a soddisfare i requisiti di conformità dei dati, eseguire analisi di sicurezza complete, monitorare modelli specifici di comportamento degli utenti e intervenire sull'attività delle API a livello di oggetto all'interno dei tuoi bucket S3 utilizzando Amazon Events. Account AWS CloudWatch Questo controllo produce PASSED risultati se configuri un percorso multiregionale che registra eventi di sola lettura o tutti i tipi di eventi relativi ai dati per tutti i bucket S3.

Correzione

Per abilitare la registrazione a livello di oggetto per i bucket S3, consulta [Enabling CloudTrail event logging for S3 bucket and objects nella Amazon Simple Storage Service User Guide](#).

SageMaker Controlli Amazon

Questi controlli sono correlati alle SageMaker risorse.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[SageMaker.1] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet

Requisiti correlati: PCI DSS versione 3.2.1/1.2.1, PCI DSS versione 3.2.1/1.3.1, PCI DSS versione 3.2.1/1.3.2, PCI DSS versione 3.2.1/1.3.4, PCI DSS versione 3.2.1/1.3.6, NIST.800-53.r5 AC-21,

NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.R5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (20) 3.5 SC-7 (21), NIT 800-53.r5 SC-7 (3), NIT 800-53.5 SC-7 (4), NIT 800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete protetta

Gravità: alta

Tipo di risorsa: AWS :: SageMaker :: NotebookInstance

Regola AWS Config : [sagemaker-notebook-no-direct-internet-access](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se l'accesso diretto a Internet è disabilitato per un'istanza di SageMaker notebook. Il controllo fallisce se il `DirectInternetAccess` campo è abilitato per l'istanza del notebook.

Se configuri l' SageMaker istanza senza un VPC, per impostazione predefinita è abilitato l'accesso diretto a Internet sull'istanza. È necessario configurare l'istanza con un VPC e modificare l'impostazione predefinita su `Disabilita: accedi a Internet tramite un VPC`. Per addestrare o ospitare modelli da un notebook, è necessario l'accesso a Internet. Per abilitare l'accesso a Internet, il VPC deve disporre di un endpoint di interfaccia (AWS PrivateLink) o di un gateway NAT e di un gruppo di sicurezza che consenta le connessioni in uscita. Per ulteriori informazioni su come connettere un'istanza di notebook alle risorse in un VPC, consulta [Connettere un'istanza di notebook alle risorse in un VPC nella Amazon Developer Guide](#). SageMaker Dovresti inoltre assicurarti che l'accesso alla tua SageMaker configurazione sia limitato ai soli utenti autorizzati. Limita le autorizzazioni IAM che consentono agli utenti di modificare SageMaker impostazioni e risorse.

Correzione

Non è possibile modificare l'impostazione di accesso a Internet dopo aver creato un'istanza di notebook. È invece possibile interrompere, eliminare e ricreare l'istanza con accesso a Internet bloccato. Per eliminare un'istanza di notebook che consente l'accesso diretto a Internet, consulta [Use notebook instances to build models: Clean up](#) nella Amazon SageMaker Developer Guide. Per ricreare un'istanza di notebook che nega l'accesso a Internet, consulta [Creare un'istanza notebook](#). Per Rete, accesso diretto a Internet, scegli `Disabilita: accedi a Internet tramite un VPC`.

[SageMaker.2] Le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato

Requisiti correlati: NIST.800-53.r5 AC-21, NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 AC-6, NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (20), NIST.800-53.r5 SC-7 (21), NIST.800-53.r5 SC-7 (3), NIST.800-53.r5 SC-7 (4), NIST.800-53.r5 SC-7 (9)

Categoria: Protezione > Configurazione di rete sicura > Risorse all'interno del VPC

Gravità: alta

Tipo di risorsa: AWS::SageMaker::NotebookInstance

Regola AWS Config : [sagemaker-notebook-instance-inside-vpc](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un'istanza di Amazon SageMaker Notebook viene avviata all'interno di un cloud privato virtuale (VPC) personalizzato. Questo controllo fallisce se un'istanza del SageMaker notebook non viene avviata all'interno di un VPC personalizzato o se viene avviata nel servizio SageMaker VPC.

Le sottoreti sono un intervallo di indirizzi IP all'interno di un VPC. Ti consigliamo di mantenere le tue risorse all'interno di un VPC personalizzato ogni volta che è possibile per garantire una protezione di rete sicura della tua infrastruttura. Un Amazon VPC è una rete virtuale dedicata al tuo Account AWS. Con Amazon VPC, puoi controllare l'accesso alla rete e la connettività Internet delle tue istanze SageMaker Studio e notebook.

Correzione

Non è possibile modificare l'impostazione del VPC dopo aver creato un'istanza del notebook. Puoi invece interrompere, eliminare e ricreare l'istanza. Per istruzioni, consulta [Usare le istanze di notebook per creare modelli: pulisci](#) nell'Amazon SageMaker Developer Guide.

[SageMaker.3] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15), NIST.800-53.r5 AC-3 (7), NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (10), NIST.800-53.r5 AC-6 (2)

Categoria: Protezione > Gestione sicura degli accessi > Restrizioni all'accesso degli utenti root

Gravità: alta

Tipo di risorsa: AWS::SageMaker::NotebookInstance

Regola AWS Config : [sagemaker-notebook-instance-root-access-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se l'accesso root è attivato per un'istanza di SageMaker notebook Amazon. Il controllo fallisce se l'accesso root è attivato per un'istanza di SageMaker notebook.

In conformità al principio del privilegio minimo, è consigliabile limitare l'accesso root alle risorse dell'istanza per evitare il sovraassegnamento involontario delle autorizzazioni.

Correzione

Per limitare l'accesso root alle istanze di SageMaker notebook, consulta [Controllare l'accesso root a un'istanza di SageMaker notebook](#) nella Amazon SageMaker Developer Guide.

[SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1

Requisiti correlati: NIST.800-53.r5 CP-10, NIST.800-53.r5 SC-5, NIST.800-53.r5 SC-36, NIST.800-53.r5 SA-13

Categoria: Recupero > Resilienza > Alta disponibilità

Gravità: media

Tipo di risorsa: AWS::SageMaker::EndpointConfig

Regola AWS Config : [sagemaker-endpoint-config-prod-instance-count](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se le varianti di produzione di un SageMaker endpoint Amazon hanno un numero iniziale di istanze superiore a 1. Il controllo fallisce se le varianti di produzione dell'endpoint hanno solo 1 istanza iniziale.

Le varianti di produzione eseguite con un numero di istanze superiore a 1 consentono la ridondanza delle istanze Multi-AZ gestita da SageMaker. L'implementazione di risorse su più zone di disponibilità è una AWS best practice per fornire un'elevata disponibilità all'interno dell'architettura. L'elevata disponibilità consente di riprendersi dagli incidenti di sicurezza.

Note

Questo controllo si applica solo alla configurazione degli endpoint basata sull'istanza.

Correzione

Per ulteriori informazioni sui parametri di configurazione degli endpoint, consulta [Create an endpoint configuration](#) nella Amazon SageMaker Developer Guide.

AWS Secrets Manager controlli

Questi controlli sono correlati alle risorse di Secrets Manager.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[SecretsManager.1] I segreti di Secrets Manager devono avere la rotazione automatica abilitata

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15)

Categoria: Protezione > Sviluppo protetto

Gravità: media

Tipo di risorsa: AWS::SecretsManager::Secret

Regola AWS Config : [secretsmanager-rotation-enabled-check](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
maximumAllowedRotationFrequency	Numero massimo di giorni consentito per la frequenza di rotazione segreta	Numero intero	1 Da a 365	Nessun valore predefinito

Questo controllo verifica se un segreto memorizzato in AWS Secrets Manager è configurato con rotazione automatica. Il controllo fallisce se il segreto non è configurato con la rotazione automatica. Se fornite un valore personalizzato per il `maximumAllowedRotationFrequency` parametro, il controllo passa solo se il segreto viene ruotato automaticamente all'interno della finestra temporale specificata.

Secrets Manager ti aiuta a migliorare il livello di sicurezza della tua organizzazione. I segreti includono credenziali del database, password e chiavi API di terze parti. È possibile utilizzare Secrets Manager per archiviare i segreti centralmente, crittografarli automaticamente, controllare l'accesso ai segreti e ruotare i segreti in modo sicuro e automatico.

Secrets Manager può ruotare i segreti. È possibile utilizzare la rotazione per sostituire i segreti a lungo termine con segreti a breve termine. La rotazione dei segreti limita il tempo per cui un utente non autorizzato può utilizzare un segreto compromesso. Per questo motivo, dovresti ruotare frequentemente i tuoi segreti. Per saperne di più sulla rotazione, consulta [Ruotare AWS Secrets Manager i tuoi segreti nella Guida](#) per l'AWS Secrets Manager utente.

Correzione

Per attivare la rotazione automatica per i segreti di Secrets Manager, consulta [Configurare la rotazione automatica per AWS Secrets Manager i segreti utilizzando la console](#) nella Guida per l'AWS Secrets Manager utente. È necessario scegliere e configurare una AWS Lambda funzione per la rotazione.

[SecretsManager.2] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15)

Categoria: Protezione > Sviluppo protetto

Gravità: media

Tipo di risorsa: AWS::SecretsManager::Secret

Regola AWS Config : [secretsmanager-scheduled-rotation-success-check](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un AWS Secrets Manager segreto è stato ruotato correttamente in base al programma di rotazione. Se lo `RotationOccurringAsScheduled` è `false`, il controllo fallisce. Il controllo valuta solo i segreti per i quali la rotazione è attivata.

Secrets Manager ti aiuta a migliorare il livello di sicurezza della tua organizzazione. I segreti includono credenziali del database, password e chiavi API di terze parti. È possibile utilizzare Secrets Manager per archiviare i segreti centralmente, crittografarli automaticamente, controllare l'accesso ai segreti e ruotare i segreti in modo sicuro e automatico.

Secrets Manager può ruotare i segreti. È possibile utilizzare la rotazione per sostituire i segreti a lungo termine con segreti a breve termine. La rotazione dei segreti limita il tempo per cui un utente non autorizzato può utilizzare un segreto compromesso. Per questo motivo, dovresti ruotare frequentemente i tuoi segreti.

Oltre a configurare i segreti in modo che ruotino automaticamente, è necessario assicurarsi che tali segreti ruotino correttamente in base alla pianificazione di rotazione.

Per ulteriori informazioni sulla rotazione, consulta [Rotating your AWS Secrets Manager secret](#) nella Guida per l'utente.AWS Secrets Manager

Correzione

Se la rotazione automatica fallisce, Secrets Manager potrebbe aver riscontrato errori nella configurazione. Per ruotare i segreti in Secrets Manager, si utilizza una funzione Lambda che definisce come interagire con il database o il servizio proprietario del segreto.

Per facilitare la diagnosi e la correzione degli errori comuni relativi alla rotazione dei segreti, consulta [Risoluzione dei problemi relativi alla AWS Secrets Manager rotazione dei segreti](#) nella Guida per l'AWS Secrets Manager utente.

[SecretsManager.3] Rimuovi i segreti inutilizzati di Secrets Manager

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15)

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS::SecretsManager::Secret

Regola AWS Config : [secretsmanager-secret-unused](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
unusedFor Days	Numero massimo di giorni in cui un segreto può rimanere inutilizzato	Numero intero	1 Da a 365	90

Questo controllo verifica se è stato effettuato l'accesso a un AWS Secrets Manager segreto entro il periodo di tempo specificato. Il controllo ha esito negativo se un segreto non viene utilizzato oltre il periodo di tempo specificato. A meno che non si fornisca un valore di parametro personalizzato per il periodo di accesso, Security Hub utilizza un valore predefinito di 90 giorni.

L'eliminazione dei segreti inutilizzati è importante tanto quanto la rotazione dei segreti. I segreti non utilizzati possono essere sfruttati in modo improprio dai precedenti utenti, che non hanno più bisogno di accedere a questi segreti. Inoltre, man mano che sempre più utenti accedono a un segreto, qualcuno potrebbe averlo gestito male e divulgato a un'entità non autorizzata, il che aumenta il rischio di abuso. L'eliminazione di segreti inutilizzati aiuta a revocare l'accesso segreto agli utenti che non ne hanno più bisogno. Inoltre aiuta a ridurre i costi di utilizzo di Secrets Manager. Pertanto, è essenziale eliminare regolarmente i segreti non utilizzati.

Correzione

Per eliminare i segreti inattivi di Secrets Manager, consulta [Eliminare un AWS Secrets Manager segreto](#) nella Guida per l'AWS Secrets Manager utente.

[SecretsManager.4] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni

Requisiti correlati: NIST.800-53.r5 AC-2 (1), NIST.800-53.r5 AC-3 (15)

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: media

Tipo di risorsa: AWS::SecretsManager::Secret

Regola AWS Config : [secretsmanager-secret-periodic-rotation](#)

Tipo di pianificazione: periodica

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
maxDaysSinceRotation	Numero massimo di giorni in cui un segreto può rimanere invariato	Numero intero	1 Da a 180	90

Questo controllo verifica se un AWS Secrets Manager segreto viene ruotato almeno una volta nell'intervallo di tempo specificato. Il controllo fallisce se un segreto non viene ruotato almeno così frequentemente. A meno che non si fornisca un valore di parametro personalizzato per il periodo di rotazione, Security Hub utilizza un valore predefinito di 90 giorni.

La rotazione dei segreti può aiutarti a ridurre il rischio di un uso non autorizzato dei tuoi segreti al tuo interno. Account AWS Gli esempi includono credenziali di database, password, chiavi API di terze parti e persino testo arbitrario. Se non modifichi i tuoi segreti per un lungo periodo di tempo, è più probabile che i segreti vengano compromessi.

Man mano che sempre più utenti accedono a un segreto, è più probabile che qualcuno lo abbia gestito male e lo abbia divulgato a un'entità non autorizzata. I segreti possono essere fatti trapelare attraverso i log e i dati della cache. Possono essere condivisi per scopi di debug e non modificati o revocati una volta completato il debug. Per tutti questi motivi, i segreti dovrebbero essere ruotati frequentemente.

È possibile configurare la rotazione automatica dei segreti in AWS Secrets Manager. Con la rotazione automatica, è possibile sostituire i segreti a lungo termine con quelli a breve termine, riducendo notevolmente il rischio di compromissione. Ti consigliamo di configurare la rotazione automatica per i tuoi segreti di Secrets Manager. Per ulteriori informazioni, consulta [Rotazione dei segreti AWS Secrets Manager](#) nella Guida per l'utente di AWS Secrets Manager.

Correzione

Per attivare la rotazione automatica per i segreti di Secrets Manager, consulta [Configurare la rotazione automatica per AWS Secrets Manager i segreti utilizzando la console](#) nella Guida per l'AWS Secrets Manager utente. È necessario scegliere e configurare una AWS Lambda funzione per la rotazione.

[SecretsManager.5] I segreti di Secrets Manager devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::SecretsManager::Secret

AWS Config regola: tagged-secretsmanager-secret (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere.	StringList	Elenco di tag che soddisfan	No default value

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.		o i requisiti AWS	

Questo controllo verifica se un AWS Secrets Manager segreto contiene tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il segreto non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il segreto non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un segreto di Secrets Manager, consulta [Tag AWS Secrets Manager secrets](#) nella Guida AWS Secrets Manager per l'utente.

AWS Service Catalog controlli

Questi controlli sono correlati alle risorse del Service Catalog.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[ServiceCatalog.1] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS

Requisiti correlati: NIST.800-53.r5 AC-3, NIST.800-53.r5 AC-4, NIST.800-53.r5 AC-6, NIST.800-53.r5 CM-8, NIST.800-53.r5 SC-7

Categoria: Protezione > Gestione degli accessi sicuri

Gravità: alta

Tipo di risorsa: AWS::ServiceCatalog::Portfolio

Regola AWS Config : [servicecatalog-shared-within-organization](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se AWS Service Catalog condivide i portafogli all'interno di un'organizzazione quando l'integrazione con AWS Organizations è abilitata. Il controllo fallisce se i portafogli non sono condivisi all'interno di un'organizzazione.

La condivisione del portafoglio solo all'interno di Organizations aiuta a garantire che un portafoglio non venga condiviso con persone errate Account AWS. Per condividere un portafoglio Service Catalog con un account in un'organizzazione, Security Hub consiglia di utilizzare ORGANIZATION_MEMBER_ACCOUNT invece di ACCOUNT. Ciò semplifica l'amministrazione regolando l'accesso concesso all'account in tutta l'organizzazione. Se hai l'esigenza aziendale di condividere i portafogli Service Catalog con un account esterno, puoi [eliminare automaticamente i risultati](#) da questo controllo o [disabilitarlo](#).

Correzione

Per abilitare la condivisione del portafoglio con Organizations, vedere [Sharing with AWS Organizations](#) nella Service Catalog Administrator Guide

Controlli di Amazon Simple Email Service

Questi controlli sono correlati alle risorse di Amazon SES.

Questi controlli potrebbero non essere disponibili in tutte le Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[SES.1] Gli elenchi di contatti SES devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: `AWS::SES::ContactList`

AWS Config regola: `tagged-ses-contactlist` (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un elenco di contatti di Amazon SES contiene tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se l'elenco dei contatti non ha alcuna chiave tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave tag e fallisce se l'elenco dei contatti non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in Riferimenti generali di AWS

Correzione

Per aggiungere tag a un elenco di contatti di Amazon SES, consulta [TagResource](#) Amazon SES API v2 Reference.

[SES.2] I set di configurazione SES devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::SES::ConfigurationSet

AWS Config regola: tagged-ses-configurationset (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un set di configurazione Amazon SES contiene tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se il set di configurazione non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il set di configurazione non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws :`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un set di configurazione Amazon SES, consulta [TagResource](#) Amazon SES API v2 Reference.

Controlli di Amazon Simple Notification Service

Questi controlli sono correlati alle risorse Amazon SNS.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[SNS.1] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS

Important

Security Hub ha ritirato questo controllo nell'aprile 2024 dallo standard AWS Foundational Security Best Practices, ma è ancora incluso nello standard NIST SP 800-53 Rev. 5. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::SNS::Topic

Regola AWS Config : [sns-encrypted-kms](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un argomento Amazon SNS è crittografato quando è inattivo utilizzando chiavi gestite in AWS Key Management Service (AWS KMS). I controlli falliscono se l'argomento SNS non utilizza una chiave KMS per la crittografia lato server (SSE). Per impostazione predefinita, SNS

archivia messaggi e file utilizzando la crittografia del disco. Per passare questo controllo, devi invece scegliere di utilizzare una chiave KMS per la crittografia. Ciò aggiunge un ulteriore livello di sicurezza e offre una maggiore flessibilità nel controllo degli accessi.

La crittografia dei dati inattivi riduce il rischio di accesso ai dati archiviati su disco da parte di un utente non autenticato. AWS Le autorizzazioni API sono necessarie per decrittografare i dati prima che possano essere letti. Ti consigliamo di crittografare gli argomenti SNS con chiavi KMS per un ulteriore livello di sicurezza.

Correzione

Per abilitare SSE per un argomento SNS, consulta [Enabling server-side encryption \(SSE\) per un argomento Amazon SNS nella Amazon Simple Notification Service Developer Guide](#). Prima di poter utilizzare SSE, devi anche configurare AWS KMS key le politiche per consentire la crittografia degli argomenti e la crittografia e la decrittografia dei messaggi. Per ulteriori informazioni, consulta [Configurazione delle AWS KMS autorizzazioni](#) nella Guida per gli sviluppatori di Amazon Simple Notification Service.

[SNS.2] La registrazione dello stato di consegna deve essere abilitata per i messaggi di notifica inviati a un argomento

Important

Security Hub ha ritirato questo controllo nell'aprile 2024. Per ulteriori informazioni, consulta [Registro delle modifiche per i controlli del Security Hub](#).

Requisiti correlati: NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::SNS::Topic

Regola AWS Config : [sns-topic-message-delivery-notification-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se la registrazione è abilitata per lo stato di consegna dei messaggi di notifica inviati a un argomento di Amazon SNS per gli endpoint. Questo controllo fallisce se la notifica dello stato di consegna dei messaggi non è abilitata.

La registrazione è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni dei servizi. La registrazione dello stato di consegna dei messaggi aiuta a fornire informazioni operative, come le seguenti:

- Sapere se un messaggio è stato consegnato all'endpoint Amazon SNS.
- Identificare la risposta inviata dall'endpoint Amazon SNS a Amazon SNS.
- Determinazione del tempo di permanenza del messaggio (il tempo tra il timestamp di pubblicazione e il trasferimento a un endpoint Amazon SNS).

Correzione

Per configurare la registrazione dello stato di consegna per un argomento, consulta lo stato di [consegna dei messaggi di Amazon SNS nella Amazon Simple Notification Service Developer Guide](#).

[SNS.3] Gli argomenti SNS devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::SNS::Topic

AWS Config regola: tagged-sns-topic (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa	StringList	Elenco di tag che soddisfano	No default value

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
	<p>valutata deve contenere.</p> <p>Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.</p>		<p>o i requisiti AWS</p>	

Questo controllo verifica se un argomento di Amazon SNS contiene tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se l'argomento non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'argomento non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un argomento SNS, consulta [Configurazione dei tag degli argomenti di Amazon SNS nella Amazon Simple Notification Service Developer Guide](#).

Controlli di Amazon Simple Queue Service

Questi controlli sono correlati alle risorse Amazon SQS.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[SQS.1] Le code di Amazon SQS devono essere crittografate quando sono inattive

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-3 (6), NIST.800-53.r5 SC-13, NIST.800-53.r5 SC-28, NIST.800-53.r5 SC-28 (1), NIST.800-53.r5 SC-7 (10), NIST.800-53.r5 SI-7 (6)

Categoria: Protezione > Protezione dei dati > Crittografia dei dati inattivi

Gravità: media

Tipo di risorsa: AWS::SQS::Queue

AWS Config regola: sqs-queue-encrypted (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una coda Amazon SQS è crittografata quando è inattiva. Il controllo fallisce se la coda non è crittografata con una chiave gestita da SQS (SSE-SQS) o una chiave (SSE-KMS). AWS Key Management Service AWS KMS

La crittografia dei dati inattivi riduce il rischio che un utente non autorizzato acceda ai dati archiviati su disco. La crittografia lato server (SSE) protegge il contenuto dei messaggi nelle code SQS utilizzando chiavi di crittografia gestite da SQL (SSE-SQS) o chiavi (SSE-KMS). AWS KMS

Correzione

Per configurare SSE per una coda SQS, consulta [Configurazione della crittografia lato server \(SSE\) per una coda \(console\) nella Amazon Simple Queue Service Developer Guide](#).

[SQS.2] Le code SQS devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS :: SQS :: Queue

AWS Config regola: tagged-sqs-queue (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se una coda Amazon SQS ha tag con le chiavi specifiche definite nel parametro. `requiredTagKeys` Il controllo fallisce se la coda non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro. `requiredTagKeys` Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se la coda non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni

in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta A [cosa serve ABAC?](#) AWS nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a una coda esistente utilizzando la console Amazon SQS, [consulta Configuring cost allocation tags for a Amazon SQS queue \(console\) nella Amazon Simple Queue Service Developer Guide.](#)

AWS Step Functions controlli

Questi controlli sono correlati alle risorse Step Functions.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione.](#)

[StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: `AWS::StepFunctions::StateMachine`

Regola AWS Config : [step-functions-state-machine-logging-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
LogLevel	Livello minimo di registrazione	Enum	ALL, ERROR, FATAL	Nessun valore predefinito

Questo controlla se una macchina a AWS Step Functions stati ha la registrazione attivata. Il controllo fallisce se una macchina a stati non ha la registrazione attivata. Se si fornisce un valore personalizzato per il LogLevel parametro, il controllo passa solo se la macchina a stati ha il livello di registrazione specificato attivato.

Il monitoraggio aiuta a mantenere l'affidabilità, la disponibilità e le prestazioni di Step Functions. È necessario raccogliere tutti i dati di monitoraggio Servizi AWS che si utilizzano in modo da poter eseguire più facilmente il debug degli errori multipunto. Avere una configurazione di registrazione definita per le tue macchine a stati Step Functions ti consente di tenere traccia della cronologia di esecuzione e dei risultati in Amazon CloudWatch Logs. Facoltativamente, puoi tenere traccia solo degli errori o degli eventi fatali.

Correzione

Per attivare la registrazione per una macchina a stati Step Functions, consulta [Configure logging](#) nella AWS Step Functions Developer Guide.

[StepFunctions.2] Le attività di Step Functions devono essere etichettate

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::StepFunctions::Activity

AWS Config regola: tagged-stepfunctions-activity (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
<code>requiredTagKeys</code>	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	Nessun valore predefinito

Questo controllo verifica se un' AWS Step Functions attività ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo fallisce se l'attività non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se l'attività non è etichettata con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui. AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in. Riferimenti generali di AWS

Correzione

Per aggiungere tag a un'attività di Step Functions, consulta [Tagging in Step Functions](#) nella AWS Step Functions Developer Guide.

AWS Transfer Family controlli

Questi controlli sono correlati alle risorse Transfer Family.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

I AWS Transfer Family flussi di lavoro [Transfer.1] devono essere etichettati

Categoria: Identificazione > Inventario > Etichettatura

Gravità: bassa

Tipo di risorsa: AWS::Transfer::Workflow

AWS Config regola: tagged-transfer-workflow (regola Security Hub personalizzata)

Tipo di pianificazione: modifica attivata

Parametri:

Parametro	Descrizione	Type	Valori personalizzati consentiti	Valore predefinito di Security Hub
requiredTagKeys	Elenco delle chiavi di tag non di sistema che la risorsa valutata deve contenere. Le chiavi dei tag prevedono una distinzione tra lettere maiuscole e minuscole.	StringList	Elenco di tag che soddisfano i requisiti AWS	No default value

Questo controllo verifica se un AWS Transfer Family flusso di lavoro ha tag con le chiavi specifiche definite nel parametro `requiredTagKeys`. Il controllo ha esito negativo se il flusso di lavoro non ha alcuna chiave di tag o se non ha tutte le chiavi specificate nel parametro `requiredTagKeys`. Se il

parametro `requiredTagKeys` non viene fornito, il controllo verifica solo l'esistenza di una chiave di tag e fallisce se il flusso di lavoro non è etichettato con alcuna chiave. I tag di sistema, che vengono applicati automaticamente e iniziano con `aws:`, vengono ignorati.

Un tag è un'etichetta che si assegna a una AWS risorsa e consiste in una chiave e un valore opzionale. È possibile creare tag per suddividere le risorse in categorie in base a scopo, proprietari, ambiente o ad altri criteri. I tag possono aiutarti a identificare, organizzare, cercare e filtrare le risorse. L'etichettatura consente inoltre di tenere traccia delle azioni e delle notifiche dei proprietari delle risorse responsabili. Quando si utilizza l'etichettatura, è possibile implementare il controllo degli accessi basato sugli attributi (ABAC) come strategia di autorizzazione, che definisce le autorizzazioni in base ai tag. Puoi allegare tag alle entità IAM (utenti o ruoli) e alle risorse. AWS Puoi creare una singola policy ABAC o un set separato di policy per i tuoi presidi IAM. Puoi progettare queste politiche ABAC per consentire le operazioni quando il tag del principale corrisponde al tag della risorsa. Per ulteriori informazioni, consulta [A cosa serve ABAC? AWS](#) nella Guida per l'utente di IAM.

Note

Non aggiungere informazioni di identificazione personale (PII) o altre informazioni riservate o sensibili nei tag. I tag sono accessibili a molti Servizi AWS, tra cui AWS Billing Per ulteriori best practice in materia di etichettatura, consulta [Taggare le AWS risorse](#) in Riferimenti generali di AWS

Correzione

Per aggiungere tag a un flusso di lavoro Transfer Family (console)

1. Apri la AWS Transfer Family console.
2. Nel riquadro di navigazione, scegli Flussi di lavoro. Quindi, seleziona il flusso di lavoro a cui desideri taggare.
3. Scegli Gestisci tag e aggiungi i tag.

[Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint

Requisiti correlati: NIST.800-53.r5 CM-7, NIST.800-53.r5 IA-5, NIST.800-53.r5 SC-8

Categoria: Protezione > Protezione dei dati > Crittografia dei dati in transito

Gravità: media

Tipo di risorsa: AWS::Transfer::Server

Regola AWS Config : [transfer-family-server-no-ftp](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se un AWS Transfer Family server utilizza un protocollo diverso dall'FTP per la connessione agli endpoint. Il controllo fallisce se il server utilizza il protocollo FTP per consentire a un client di connettersi all'endpoint del server.

L'FTP (File Transfer Protocol) stabilisce la connessione all'endpoint tramite canali non crittografati, rendendo i dati inviati su questi canali vulnerabili all'intercettazione. L'utilizzo di SFTP (SSH File Transfer Protocol), FTPS (File Transfer Protocol Secure) o AS2 (Applicability Statement 2) offre un ulteriore livello di sicurezza crittografando i dati in transito e può essere utilizzato per impedire a potenziali aggressori di utilizzare person-in-the-middle o attacchi simili per intercettare o manipolare il traffico di rete.

Correzione

Per modificare il protocollo per un server Transfer Family, vedere [Modifica i protocolli di trasferimento dei file](#) nella Guida per l'AWS Transfer Family utente.

AWS WAF controlli

Questi controlli sono correlati alle AWS WAF risorse.

Questi controlli potrebbero non essere disponibili in tutti Regioni AWS. Per ulteriori informazioni, consulta [Disponibilità dei controlli per regione](#).

[WAF.1] La registrazione AWS WAF classica Global Web ACL deve essere abilitata

Requisiti correlati: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (4) R5 CA-7, NIST. 800-53.R5 SC-7 (9), NIST. 800-53.5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::WAF::WebACL

Regola AWS Config : [waf-classic-logging-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la registrazione è abilitata per un ACL web AWS WAF globale. Questo controllo ha esito negativo se la registrazione non è abilitata per l'ACL Web.

La registrazione è un elemento importante per mantenere l'affidabilità, la disponibilità e le prestazioni a livello globale. AWS WAF È un requisito aziendale e di conformità in molte organizzazioni e consente di risolvere i problemi relativi al comportamento delle applicazioni. Fornisce inoltre informazioni dettagliate sul traffico analizzato dall'ACL Web a cui è allegato. AWS WAF

Correzione

Per abilitare la registrazione per un ACL AWS WAF Web, consulta la sezione [Registrazione delle informazioni sul traffico ACL Web](#) nella Developer Guide.AWS WAF

[WAF.2] Le regole regionali AWS WAF classiche devono avere almeno una condizione

Requisiti correlati: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: AWS::WAFRegional::Rule

Regola AWS Config : [waf-regional-rule-not-empty](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una regola AWS WAF regionale ha almeno una condizione. Il controllo ha esito negativo se non sono presenti condizioni all'interno di una regola.

Una regola regionale WAF può contenere più condizioni. Le condizioni della regola consentono l'ispezione del traffico e l'esecuzione di un'azione definita (consentire, bloccare o contare). Senza

alcuna condizione, il traffico scorre senza ispezioni. Una regola regionale WAF priva di condizioni, ma con un nome o tag che suggerisca di consentire, bloccare o contare, potrebbe indurre a supporre erroneamente che una di queste azioni si stia verificando.

Correzione

Per aggiungere una condizione a una regola vuota, consulta [Aggiungere e rimuovere condizioni in una regola nella Guida](#) per gli sviluppatori.AWS WAF

[WAF.3] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola

Requisiti correlati: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: AWS::WAFRegional::RuleGroup

Regola AWS Config : [waf-regional-rulegroup-not-empty](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo di regole AWS WAF regionali ha almeno una regola. Il controllo ha esito negativo se non è presente alcuna regola all'interno di un gruppo di regole.

Un gruppo di regole regionali WAF può contenere più regole. Le condizioni della regola consentono l'ispezione del traffico e l'esecuzione di un'azione definita (consentire, bloccare o contare). Senza regole, il traffico scorre senza ispezioni. Un gruppo di regole regionali WAF privo di regole, ma con un nome o un tag che suggerisce l'autorizzazione, il blocco o il numero, potrebbe indurre a supporre erroneamente che una di queste azioni sia in corso.

Correzione

Per aggiungere regole e condizioni di regole a un gruppo di regole vuoto, consulta [Aggiungere ed eliminare regole da un gruppo di regole AWS WAF classico e Aggiungere e rimuovere condizioni in una regola nella Guida](#) per gli sviluppatori.AWS WAF

[WAF.4] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: AWS::WAFRegional::WebACL

Regola AWS Config : [waf-regional-webacl-not-empty](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un ACL AWS WAF Classic regionale Web contiene regole WAF o gruppi di regole WAF. Questo controllo ha esito negativo se un ACL Web non contiene regole o gruppi di regole WAF.

Un ACL web WAF regionale può contenere una raccolta di regole e gruppi di regole che esaminano e controllano le richieste web. Se un ACL web è vuoto, il traffico web può passare senza essere rilevato o modificato da WAF, a seconda dell'azione predefinita.

Correzione

Per aggiungere regole o gruppi di regole a un ACL web regionale AWS WAF classico vuoto, consulta [Modifica di un ACL Web nella Guida per gli sviluppatori](#).AWS WAF

[WAF.6] Le regole globali AWS WAF classiche devono avere almeno una condizione

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: AWS::WAF::Rule

Regola AWS Config : [waf-global-rule-not-empty](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una regola AWS WAF globale contiene condizioni. Il controllo ha esito negativo se non sono presenti condizioni all'interno di una regola.

Una regola globale WAF può contenere più condizioni. Le condizioni di una regola consentono l'ispezione del traffico e l'esecuzione di un'azione definita (consentire, bloccare o contare). Senza alcuna condizione, il traffico scorre senza ispezioni. Una regola globale WAF priva di condizioni, ma con un nome o tag che suggerisca di consentire, bloccare o contare, potrebbe portare a supporre erroneamente che una di queste azioni sia in corso.

Correzione

Per istruzioni sulla creazione di una regola e sull'aggiunta di condizioni, consulta [Creazione di una regola e aggiunta di condizioni](#) nella Guida per gli sviluppatori AWS WAF

[WAF.7] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: AWS::WAF::RuleGroup

Regola AWS Config : [waf-global-rulegroup-not-empty](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un gruppo di regole AWS WAF globale ha almeno una regola. Il controllo ha esito negativo se non è presente alcuna regola all'interno di un gruppo di regole.

Un gruppo di regole globale WAF può contenere più regole. Le condizioni della regola consentono l'ispezione del traffico e l'esecuzione di un'azione definita (consentire, bloccare o contare). Senza regole, il traffico scorre senza ispezioni. Un gruppo di regole globale WAF senza regole, ma con un nome o un tag che suggerisce di consentire, bloccare o contare, potrebbe portare a supporre erroneamente che una di queste azioni sia in corso.

Correzione

Per istruzioni sull'aggiunta di una regola a un gruppo di regole, consulta [Creating an AWS WAF Classic rule group](#) nella Developer Guide.AWS WAF

[WAF.8] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole

Requisiti correlati: NIST.800-53.r5 AC-4 (21), NIST.800-53.r5 SC-7, NIST.800-53.r5 SC-7 (11), NIST.800-53.r5 SC-7 (16), NIST.800-53.r5 SC-7 (21)

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: AWS : :WAF : :WebACL

Regola AWS Config : [waf-global-webacl-not-empty](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un ACL web AWS WAF globale contiene almeno una regola WAF o un gruppo di regole WAF. Il controllo ha esito negativo se un ACL Web non contiene regole o gruppi di regole WAF.

Un ACL web globale WAF può contenere una raccolta di regole e gruppi di regole che esaminano e controllano le richieste web. Se un ACL Web è vuoto, il traffico Web può passare senza essere rilevato o modificato da WAF, a seconda dell'azione predefinita.

Correzione

Per aggiungere regole o gruppi di regole a un ACL web AWS WAF globale vuoto, consulta [Modifica di un ACL web nella Guida per gli sviluppatori](#).AWS WAF Per Filtro, scegliete Globale () CloudFront.

[WAF.10] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole

Requisiti correlati: NIST.800-53.r5 CA-9 (1), NIST.800-53.r5 CM-2

Categoria: Protezione > Configurazione di rete protetta

Gravità: media

Tipo di risorsa: AWS::WAFv2::WebACL

Regola AWS Config : [wafv2-webacl-not-empty](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se un elenco di controllo degli accessi Web AWS WAF V2 (Web ACL) contiene almeno una regola o un gruppo di regole. Il controllo ha esito negativo se un ACL Web non contiene regole o gruppi di regole.

Un ACL Web offre un controllo dettagliato su tutte le richieste Web HTTP (S) a cui risponde la risorsa protetta. Un ACL Web deve contenere una raccolta di regole e gruppi di regole che esaminano e controllano le richieste Web. Se un ACL Web è vuoto, il traffico Web può passare senza essere rilevato o modificato, AWS WAF a seconda dell'azione predefinita.

Correzione

Per aggiungere regole o gruppi di regole a un ACL web WAFV2 vuoto, vedere [Modifica di un ACL Web](#) nella Guida per gli sviluppatori.AWS WAF

[WAF.11] la registrazione ACL web deve essere abilitata AWS WAF

Requisiti correlati: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (4) R5 CA-7, NIS.800-53.r5 SC-7 (10), NIS.800-53.r5 SC-7 (9), NIS.800-53R5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: bassa

Tipo di risorsa: AWS::WAFv2::WebACL

AWS Config regola: [wafv2-logging-enabled](#)

Tipo di pianificazione: periodica

Parametri: nessuno

Questo controllo verifica se la registrazione è attivata per un elenco di controllo degli accessi Web AWS WAF V2 (Web ACL). Questo controllo ha esito negativo se la registrazione è disattivata per l'ACL Web.

La registrazione mantiene l'affidabilità, la disponibilità e le prestazioni di AWS WAF. Inoltre, la registrazione è un requisito aziendale e di conformità in molte organizzazioni. Registrando il traffico analizzato dall'ACL Web, è possibile risolvere i problemi relativi al comportamento delle applicazioni.

Correzione

Per attivare la registrazione per un ACL AWS WAF Web, consulta [Managing logging for a Web ACL](#) nella Developer Guide. AWS WAF

Le regole [WAF.12] devono avere le metriche abilitate AWS WAF CloudWatch

Requisiti correlati: NIST.800-53.r5 AC-4 (26), NIST.800-53.r5 AU-10, NIST.800-53.r5 AU-12, NIST.800-53.r5 AU-2, NIST.800-53.r5 AU-3, NIST.800-53.r5 AU-6 (3), NIST.800-53.r5 AU-6 (4), NIST.800-53.r5 AU-6 (4) R5 CA-7, NIS.800-53.r5 SC-7 (10), NIS.800-53.r5 SC-7 (9), NIS.800-53R5 SI-7 (8)

Categoria: Identificazione > Registrazione

Gravità: media

Tipo di risorsa: AWS::WAFv2::RuleGroup

AWS Config regola: [wafv2-rulegroup-logging-enabled](#)

Tipo di pianificazione: modifica attivata

Parametri: nessuno

Questo controllo verifica se una AWS WAF regola o un gruppo di regole ha le CloudWatch metriche Amazon abilitate. Il controllo fallisce se la regola o il gruppo di regole non ha le CloudWatch metriche abilitate.

La configurazione delle CloudWatch metriche su AWS WAF regole e gruppi di regole offre visibilità sul flusso di traffico. Puoi vedere quali regole ACL vengono attivate e quali richieste vengono accettate e bloccate. Questa visibilità può aiutarti a identificare attività dannose sulle risorse associate.

Correzione

Per abilitare le CloudWatch metriche su un gruppo di AWS WAF regole, richiama l'[UpdateRuleGroup](#) API. [Per abilitare le CloudWatch metriche su una AWS WAF regola, richiama l'API ACL. UpdateWeb](#) Imposta il campo su `CloudWatchMetricsEnabled true` Quando utilizzi la

AWS WAF console per creare regole o gruppi di regole, le CloudWatch metriche vengono abilitate automaticamente.

Visualizzazione e gestione dei controlli di sicurezza

Un controllo è una protezione all'interno di uno standard di sicurezza che aiuta un'organizzazione a proteggere la riservatezza, l'integrità e la disponibilità delle proprie informazioni. In Security Hub, un controllo è correlato a una AWS risorsa specifica.

Visualizzazione consolidata dei controlli

La pagina Controlli della console Security Hub mostra tutti i controlli disponibili nella versione corrente Regione AWS (è possibile visualizzare i controlli nel contesto di uno standard visitando la pagina degli standard di sicurezza e scegliendo uno standard abilitato). Security Hub assegna ai controlli un ID, un titolo e una descrizione di controllo di sicurezza coerenti tra gli standard. Gli ID dei controlli includono il numero pertinente Servizio AWS e un numero univoco (ad esempio, CodeBuild .3).

Le seguenti informazioni sono disponibili nella pagina Controlli della [console Security Hub](#):

- Un punteggio di sicurezza complessivo basato sulla percentuale di controlli approvati rispetto al numero totale di controlli abilitati con dati
- La percentuale di controlli di sicurezza non riusciti su tutti i controlli abilitati
- Il numero di controlli di sicurezza superati e non riusciti per controlli di diversa gravità
- Un elenco di controlli suddiviso in diverse schede in base allo stato di attivazione. I controlli disponibili che non si applicano a nessuno degli standard abilitati vengono visualizzati nella colonna Disabilitato. I controlli non elaborati, ad esempio quelli che non sono disponibili nella regione corrente, vengono visualizzati nella colonna Nessun dato. Il numero di controlli nella colonna Tutti è uguale alla somma dei controlli nelle colonne Failed, Unknown, Passed, Disabled e Nessun dato.

Dalla pagina Controlli, puoi scegliere un controllo per visualizzarne i dettagli e intervenire sui risultati generati dal controllo. Da questa pagina, puoi anche abilitare o disabilitare un controllo di sicurezza nel tuo sistema attuale Account AWS e Regione AWS. Le azioni di attivazione e disabilitazione della pagina Controlli si applicano a tutti gli standard. Per ulteriori informazioni, consulta [Abilitazione e disabilitazione dei controlli in tutti gli standard](#).

Per gli account amministratore, la pagina Controlli riflette lo stato dei controlli negli account dei membri. Se un controllo di controllo non riesce in almeno un account membro, il controllo viene

visualizzato nella scheda Non riuscito della pagina Controlli. Se hai impostato una [regione di aggregazione](#), la pagina Controlli riflette lo stato dei controlli in tutte le aree collegate. Se un controllo di controllo ha esito negativo in almeno una regione collegata, il controllo viene visualizzato nella scheda Non riuscito della pagina Controlli.

La visualizzazione dei controlli consolidati modifica i campi di ricerca dei controlli nel AWS Security Finding Format (ASFF) che possono influire sui flussi di lavoro. Per ulteriori informazioni, consulta [Visualizzazione dei controlli consolidati: modifiche ASFF](#).

Punteggio di sicurezza complessivo per i controlli

La pagina Controlli mostra un punteggio di sicurezza complessivo compreso tra 0 e 100 percento. Il punteggio di sicurezza complessivo viene calcolato in base alla percentuale di controlli approvati rispetto al numero totale di controlli abilitati con dati.

Note

Per visualizzare il punteggio di sicurezza complessivo per i controlli, devi aggiungere l'autorizzazione alla chiamata **BatchGetControlEvaluations** al ruolo IAM che utilizzi per accedere a Security Hub. Questa autorizzazione non è necessaria per visualizzare i punteggi di sicurezza per standard specifici.

Quando abiliti Security Hub, Security Hub calcola il punteggio di sicurezza iniziale entro 30 minuti dalla prima visita alla pagina di riepilogo o alla pagina degli standard di sicurezza sulla console Security Hub. Possono essere necessarie fino a 24 ore prima che i punteggi di sicurezza vengano generati per la prima volta nelle regioni cinesi e. AWS GovCloud (US) Region I punteggi vengono generati solo per gli standard abilitati quando visiti quelle pagine. Per visualizzare un elenco degli standard attualmente abilitati, utilizza l'operazione [GetEnabledStandardsAPI](#). Inoltre, la registrazione AWS Config delle risorse deve essere configurata per visualizzare gli spartiti. Il punteggio di sicurezza complessivo è la media dei [punteggi di sicurezza standard](#).

Dopo la prima generazione dei punteggi, Security Hub aggiorna i punteggi di sicurezza ogni 24 ore. Security Hub visualizza un timestamp per indicare quando un punteggio di sicurezza è stato aggiornato l'ultima volta.

Se hai impostato una [regione di aggregazione](#), il punteggio di sicurezza complessivo riflette i risultati del controllo nelle regioni collegate.

Argomenti

- [Categorie di controllo](#)
- [Abilitazione e disabilitazione dei controlli in tutti gli standard](#)
- [Abilitazione automatica di nuovi controlli negli standard abilitati](#)
- [Parametri di controllo personalizzati](#)
- [Controlli del Security Hub che potresti voler disabilitare](#)
- [Visualizzazione dei dettagli di un controllo](#)
- [Filtraggio e ordinamento dell'elenco dei controlli](#)
- [Visualizzazione e adozione di misure in base ai risultati del controllo](#)

Categorie di controllo

A ogni controllo viene assegnata una categoria. La categoria di un controllo riflette la funzione di protezione a cui si applica il controllo.

Il valore della categoria contiene la categoria, la sottocategoria all'interno della categoria e, facoltativamente, un classificatore all'interno della sottocategoria. Per esempio:

- Identifica > Inventario
- Proteggi > Protezione dei dati > Crittografia dei dati in transito

Di seguito sono riportate le descrizioni delle categorie, sottocategorie e classificatori disponibili.

Identificazione

Sviluppare le conoscenze organizzative per gestire i rischi di sicurezza informatica per sistemi, risorse, dati e funzionalità.

Inventario

Il servizio ha implementato le strategie di tagging delle risorse corrette? Le strategie di tagging includono il proprietario della risorsa?

Quali risorse utilizza il servizio? Sono risorse approvate per questo servizio?

Hai visibilità sull'inventario approvato? Ad esempio, utilizzi servizi come Amazon EC2 Systems Manager e Service Catalog?

Registrazione

Hai abilitato in modo sicuro tutte le registrazioni rilevanti per il servizio? Alcuni esempi di file di log includono:

- Registri di flusso di Amazon VPC
- Log di accesso per Elastic Load Balancing
- CloudFront Registri Amazon
- CloudWatch Registri Amazon
- Registrazione di Amazon Relational Database Service
- Log di indicizzazione lenti di Amazon OpenSearch Service
- Tracciamento X-Ray
- AWS Directory Service registri
- AWS Config articoli
- Snapshot

Protezione

Sviluppare e implementare le misure di sicurezza appropriate per garantire la fornitura di servizi di infrastruttura critica e procedure di codifica sicure.

Gestione sicura degli accessi

Il servizio utilizza pratiche con privilegi minimi nelle sue politiche IAM o in materia di risorse?

Le password e i segreti sono sufficientemente complessi? Sono ruotati in modo appropriato?

Il servizio utilizza l'autenticazione a più fattori (MFA)?

Il servizio evita l'utente root?

I criteri basati sulle risorse consentono l'accesso pubblico?

Configurazione di rete sicura

Il servizio evita l'accesso alla rete remota pubblico e non sicuro?

Il servizio utilizza correttamente i VPC? Ad esempio, i processi devono essere eseguiti in VPC?

Il servizio segmenta e isola correttamente le risorse sensibili?

Protezione dei dati

Crittografia dei dati inattivi: il servizio crittografa i dati inattivi?

Crittografia dei dati in transito: il servizio crittografa i dati in transito?

Integrità dei dati: il servizio convalida l'integrità dei dati?

Protezione dall'eliminazione dei dati: il servizio protegge i dati dall'eliminazione accidentale?

Gestione e utilizzo dei dati: utilizzi servizi come Amazon Macie per tracciare la posizione dei tuoi dati sensibili?

Protezione API

Il servizio viene utilizzato AWS PrivateLink per proteggere le operazioni dell'API del servizio?

Servizi di protezione

Sono in atto i servizi di protezione corretti? Forniscono la giusta quantità di copertura?

I servizi di protezione consentono di deviare gli attacchi e i compromessi diretti al servizio. Esempi di servizi di protezione AWS includono AWS Control Tower,, AWS WAF, Vanta AWS Shield Advanced, Secrets Manager, IAM Access Analyzer e AWS Resource Access Manager.

Sviluppo sicuro

Si utilizzano pratiche di codifica sicure?

Si evitano vulnerabilità quali la Top Ten Open Web Application Security Project (OWASP)?

Rilevamento

Sviluppare e implementare le attività appropriate per identificare il verificarsi di un evento di sicurezza informatica.

Servizi di rilevamento

Sono disponibili i servizi di rilevamento corretti?

Forniscono la giusta quantità di copertura?

Esempi di servizi di AWS rilevamento includono Amazon GuardDuty AWS Security Hub, Amazon Inspector, Amazon Detective, AWS IoT Device Defender Amazon CloudWatch Alarms e. AWS Trusted Advisor

Rispondi

Sviluppare e implementare le attività appropriate per intervenire in merito a un evento di sicurezza informatica rilevato.

Azioni di risposta

Rispondi rapidamente agli eventi di sicurezza?

Avete qualche risultato critico attivo o ad alta gravità?

Informatica forense

È possibile acquisire in modo sicuro i dati forensi per il servizio? Ad esempio, acquisisci istantanee di Amazon EBS associate a risultati realmente positivi?

Hai creato un account forense?

Ripristino

Sviluppare e implementare le attività appropriate per mantenere piani di resilienza e ripristinare eventuali funzionalità o servizi compromessi a causa di un evento di sicurezza informatica.

Resilienza

La configurazione del servizio supporta failover agevoli, scalabilità elastica e disponibilità elevata?

Sono stati stabiliti dei backup?

Abilitazione e disabilitazione dei controlli in tutti gli standard

AWS Security Hub genera risultati per i controlli abilitati e considera tutti i controlli abilitati nel calcolo dei punteggi di sicurezza. È possibile scegliere di abilitare e disabilitare i controlli in tutti gli standard di sicurezza o configurare lo stato di abilitazione in modo diverso a seconda degli standard. Consigliamo la prima opzione, in cui lo stato di attivazione di un controllo è allineato a tutti gli standard abilitati. Questa sezione spiega come abilitare e disabilitare i controlli tra gli standard. Per

abilitare o disabilitare un controllo in uno o più standard specifici, vedere [Abilitazione e disabilitazione dei controlli in standard specifici](#).

Se è stata impostata una regione di aggregazione, la console Security Hub mostra i controlli di tutte le regioni collegate. Se un controllo è disponibile in una regione collegata ma non nella regione di aggregazione, non è possibile abilitare o disabilitare tale controllo dalla regione di aggregazione.

Note

[Le istruzioni per abilitare e disabilitare i controlli variano a seconda che si utilizzi o meno la configurazione centrale.](#) Questa sezione descrive le differenze. La configurazione centrale è disponibile per gli utenti che integrano Security Hub e AWS Organizations. Si consiglia di utilizzare la configurazione centrale per semplificare il processo di attivazione e disabilitazione dei controlli in ambienti con più account e più regioni.

Abilitazione dei controlli

Quando abiliti un controllo in uno standard, Security Hub inizia a eseguire i controlli di sicurezza per il controllo e a generare i risultati del controllo.

Security Hub include lo [stato del controllo](#) nel calcolo del punteggio di sicurezza complessivo e dei punteggi di sicurezza standard. Se attivi i risultati del controllo consolidato, riceverai un unico risultato per un controllo di sicurezza anche se hai abilitato un controllo in più standard. Per ulteriori informazioni, consulta [Risultati dei controlli consolidati](#).

Abilitazione del controllo in tutti gli standard su più account e regioni

Per abilitare un controllo di sicurezza su più account e Regioni AWS, è necessario utilizzare la [configurazione centrale](#).

Quando si utilizza la configurazione centrale, l'amministratore delegato può creare politiche di configurazione del Security Hub che abilitano controlli specifici su tutti gli standard abilitati. È quindi possibile associare la politica di configurazione a account e unità organizzative (OU) specifici o alla radice. Una politica di configurazione ha effetto nella regione di origine (chiamata anche regione di aggregazione) e in tutte le regioni collegate.

Le politiche di configurazione offrono la personalizzazione. Ad esempio, puoi scegliere di abilitare tutti i controlli in un'unità organizzativa e puoi scegliere di abilitare solo i controlli Amazon Elastic Compute

Cloud (EC2) in un'altra unità organizzativa. Il livello di granularità dipende dagli obiettivi prefissati per la copertura di sicurezza nell'organizzazione. Per istruzioni sulla creazione di una politica di configurazione che abiliti controlli specifici tra gli standard, consulta. [Creazione e associazione dei criteri di configurazione del Security Hub](#)

Note

L'amministratore delegato può creare politiche di configurazione per gestire i controlli in tutti gli standard tranne il [Service-Managed](#) Standard:. AWS Control Tower I controlli per questo standard devono essere configurati nel servizio. AWS Control Tower

Se desideri che alcuni account configurino i propri controlli anziché l'amministratore delegato, l'amministratore delegato può designare tali account come autogestiti. Gli account autogestiti devono configurare i controlli separatamente in ciascuna regione.

Abilitare il controllo in tutti gli standard in un unico account e regione

Se non utilizzi la configurazione centrale o sei un account autogestito, non puoi utilizzare i criteri di configurazione per abilitare centralmente i controlli in più account e regioni. Tuttavia, puoi utilizzare i seguenti passaggi per abilitare un controllo in un singolo account e regione.

Security Hub console

Per abilitare un controllo su più standard in un account e in un'unica regione

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Scegli Controlli dal pannello di navigazione.
3. Scegli la scheda Disabilitato.
4. Scegli l'opzione accanto a un controllo.
5. Scegli Abilita controllo (questa opzione non viene visualizzata per un controllo già abilitato).
6. Ripeti l'operazione in ogni regione in cui desideri abilitare il controllo.

Security Hub API

Per abilitare il controllo su più standard in un account e in un'unica regione

1. Invoca l'[ListStandardsControlAssociations](#)API. Fornisci un ID di controllo di sicurezza.

Richiesta di esempio:

```
{
  "SecurityControlId": "IAM.1"
}
```

2. Richiama l'[BatchUpdateStandardsControlAssociations](#) API. Fornisci l'Amazon Resource Name (ARN) di tutti gli standard in cui il controllo non è abilitato. Per ottenere ARN standard, esegui [DescribeStandards](#).
3. Imposta il `AssociationStatus` parametro uguale a `ENABLED`. Se segui questi passaggi per un controllo già abilitato, l'API restituisce una risposta con codice di stato HTTP 200.

Richiesta di esempio:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/v/1.2.0",
    "AssociationStatus": "ENABLED"}, {"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-best-practices/v/1.0.0",
    "AssociationStatus": "ENABLED"}]
}
```

4. Ripetere l'operazione in ogni regione in cui si desidera abilitare il controllo.

AWS CLI

Per abilitare il controllo su più standard in un account e in un'unica regione

1. Esegui il comando [list-standards-control-associations](#). Fornisci un ID di controllo di sicurezza.

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Esegui il comando [batch-update-standards-control-associations](#). Fornisci l'Amazon Resource Name (ARN) di tutti gli standard in cui il controllo non è abilitato. Per ottenere ARN standard, esegui il `describe-standards` comando.
3. Imposta il `AssociationStatus` parametro uguale a `ENABLED`. Se segui questi passaggi per un controllo già abilitato, il comando restituisce una risposta con il codice di stato HTTP 200.

```
aws securityhub --region us-east-1 batch-update-standards-control-associations
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
"StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "ENABLED"}, {"SecurityControlId": "CloudTrail.1",
"StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/
v/1.4.0", "AssociationStatus": "ENABLED"}]'
```

4. Ripeti l'operazione in ogni regione in cui desideri abilitare il controllo.

Abilitazione automatica di nuovi controlli negli standard abilitati

Security Hub rilascia regolarmente nuovi controlli di sicurezza e li aggiunge a uno o più standard. Puoi scegliere se abilitare automaticamente i nuovi controlli negli standard abilitati.

Note

Ti consigliamo di utilizzare la configurazione centrale per abilitare automaticamente i nuovi controlli. Se la politica di configurazione include un elenco di controlli da disabilitare (a livello di codice, questo riflette il `DisabledSecurityControlIdentifiers` parametro), Security Hub abilita automaticamente tutti gli altri controlli tra gli standard, inclusi i controlli appena rilasciati. Se la tua politica include un elenco di controlli da abilitare (questo riflette il `EnabledSecurityControlIdentifiers` parametro), Security Hub disabilita automaticamente tutti gli altri controlli tra gli standard, compresi quelli appena rilasciati. Per ulteriori informazioni, consulta [Come funzionano le politiche di configurazione di Security Hub](#).

Scegli il metodo di accesso preferito e segui i passaggi per abilitare automaticamente i nuovi controlli negli standard abilitati. Le seguenti istruzioni si applicano solo se non utilizzi la configurazione centrale.

Security Hub console

Per abilitare automaticamente i nuovi controlli

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli la scheda Generale.
3. In Controlli, scegli Modifica.

4. Attiva l'attivazione automatica dei nuovi controlli negli standard abilitati.
5. Selezionare Salva.

Security Hub API

Per abilitare automaticamente i nuovi controlli

1. Invoca l'[UpdateSecurityHubConfiguration](#) API.
2. Per abilitare automaticamente nuovi controlli per gli standard abilitati, imposta su `AutoEnableControls` `true`. Se non desideri abilitare automaticamente i nuovi controlli, imposta `AutoEnableControls` su `false`.

AWS CLI

Per abilitare automaticamente i nuovi controlli

1. Esegui il comando [update-security-hub-configuration](#).
2. Per abilitare automaticamente nuovi controlli per gli standard abilitati, specificare `--auto-enable-controls`. Se non desiderate abilitare automaticamente i nuovi controlli, specificate `--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Comando di esempio

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Disabilitazione dei controlli

Quando si disattiva un controllo in tutti gli standard, si verifica quanto segue:

- I controlli di sicurezza per il controllo non vengono più eseguiti.
- Non vengono generati ulteriori risultati per tale verifica.
- I risultati esistenti vengono archiviati automaticamente dopo 3-5 giorni (si noti che questa è la soluzione migliore).

- Tutte AWS Config le regole correlate create da Security Hub vengono rimosse.

Invece di disabilitare un controllo in tutti gli standard, puoi semplicemente disabilitarlo in uno o più standard specifici. In tal caso, Security Hub non esegue controlli di sicurezza per il controllo degli standard in cui l'hai disabilitato, quindi non influisce sul punteggio di sicurezza per tali standard. Tuttavia, Security Hub mantiene la AWS Config regola e continua a eseguire i controlli di sicurezza per il controllo se è abilitato in altri standard. Ciò può influire sul punteggio di sicurezza riepilogativo. Per istruzioni sulla configurazione dei controlli in standard specifici, consulta [Abilitazione e disabilitazione dei controlli in standard specifici](#).

Per ridurre i disturbi rilevati, può essere utile disabilitare i controlli non pertinenti all'ambiente in uso. Per consigli su quali controlli disabilitare, vedi [Controlli del Security Hub che potresti voler disabilitare](#).

Quando disabiliti uno standard, tutti i controlli che si applicano allo standard vengono disabilitati (tuttavia, tali controlli potrebbero rimanere abilitati in altri standard). Per informazioni sulla disabilitazione di uno standard, vedere [the section called “Abilitazione e disabilitazione degli standard”](#).

Quando disabiliti uno standard, Security Hub non tiene traccia dei controlli applicabili che sono stati disabilitati. Se successivamente riattivi lo stesso standard, tutti i controlli ad esso applicabili vengono abilitati automaticamente. Inoltre, la disabilitazione di un controllo non è un'azione permanente. Supponiamo di disabilitare un controllo e quindi di abilitare uno standard precedentemente disabilitato. Se lo standard include quel controllo, sarà abilitato in quello standard. Quando abiliti uno standard in Security Hub, tutti i controlli che si applicano a quello standard vengono abilitati automaticamente. Puoi scegliere di disabilitare controlli specifici.

Disattivazione di un controllo in tutti gli standard su più account e regioni

Per disabilitare un controllo di sicurezza su più account e Regioni AWS, è necessario utilizzare la [configurazione centrale](#).

Quando si utilizza la configurazione centrale, l'amministratore delegato può creare politiche di configurazione del Security Hub che disabilitano i controlli specifici tra gli standard abilitati. È quindi possibile associare la politica di configurazione a account, unità organizzative o root specifici. Una politica di configurazione ha effetto nella regione di origine (chiamata anche regione di aggregazione) e in tutte le regioni collegate.

Le politiche di configurazione offrono la personalizzazione. Ad esempio, puoi scegliere di disabilitare tutti i AWS CloudTrail controlli in un'unità organizzativa e puoi scegliere di disabilitare tutti i controlli

IAM in un'altra unità organizzativa. Il livello di granularità dipende dagli obiettivi prefissati per la copertura di sicurezza nell'organizzazione. Per istruzioni sulla creazione di una politica di configurazione che disabiliti controlli specifici tra gli standard, vedi. [Creazione e associazione dei criteri di configurazione del Security Hub](#)

Note

L'amministratore delegato può creare politiche di configurazione per gestire i controlli in tutti gli standard tranne il [Service-Managed](#) Standard. AWS Control Tower I controlli per questo standard devono essere configurati nel servizio. AWS Control Tower

Se desideri che alcuni account configurino i propri controlli anziché l'amministratore delegato, l'amministratore delegato può designare tali account come autogestiti. Gli account autogestiti devono configurare i controlli separatamente in ciascuna regione.

Disattivazione di un controllo in tutti gli standard in un unico account e regione

Se non utilizzi la configurazione centrale o sei un account autogestito, non puoi utilizzare i criteri di configurazione per disabilitare centralmente i controlli in più account e regioni. Tuttavia, puoi utilizzare i seguenti passaggi per disabilitare un controllo in un singolo account e regione.

Security Hub console

Per disabilitare un controllo su più standard in un account e in un'unica regione

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Scegli Controlli dal pannello di navigazione.
3. Scegli l'opzione accanto a un controllo.
4. Scegli Disabilita controllo (questa opzione non viene visualizzata per un controllo già disabilitato).
5. Seleziona un motivo per disabilitare il controllo e conferma scegliendo Disabilita.
6. Ripetere l'operazione in ogni regione in cui si desidera disattivare il controllo.

Security Hub API

Per disabilitare un controllo su più standard in un account e in una regione

1. Invoca l'[ListStandardsControlAssociations](#) API. Fornisci un ID di controllo di sicurezza.

Richiesta di esempio:

```
{
  "SecurityControlId": "IAM.1"
}
```

2. Richiama l'[BatchUpdateStandardsControlAssociations](#) API. Fornisci l'ARN di tutti gli standard in cui è abilitato il controllo. Per ottenere ARN standard, esegui [DescribeStandards](#)
3. Imposta il `AssociationStatus` parametro uguale a `DISABLED`. Se segui questi passaggi per un controllo già disabilitato, l'API restituisce una risposta con codice di stato HTTP 200.

Richiesta di esempio:

```
{
  "StandardsControlAssociationUpdates": [{"SecurityControlId": "IAM.1",
    "StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-
    benchmark/v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not
    applicable to environment"}, {"SecurityControlId": "IAM.1", "StandardsArn":
    "arn:aws:securityhub::standards/aws-foundational-security-best-practices/
    v/1.0.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
    environment"}]}
}
```

4. Ripetere l'operazione in ogni regione in cui si desidera disattivare il controllo.

AWS CLI

Per disabilitare un controllo su più standard in un account e in una regione

1. Esegui il comando [list-standards-control-associations](#). Fornisci un ID di controllo di sicurezza.

```
aws securityhub --region us-east-1 list-standards-control-associations --
security-control-id CloudTrail.1
```

2. Esegui il comando [batch-update-standards-control-associations](#). Fornisci l'ARN di tutti gli standard in cui è abilitato il controllo. Per ottenere ARN standard, esegui il `describe-standards` comando.
3. Imposta il `AssociationStatus` parametro uguale a `DISABLED`. Se segui questi passaggi per un controllo già disabilitato, il comando restituisce una risposta con il codice di stato HTTP 200.

```
aws securityhub --region us-east-1 batch-update-standards-control-associations
--standards-control-association-updates '[{"SecurityControlId": "CloudTrail.1",
"StandardsArn": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/
v/1.2.0", "AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable
to environment"}, {"SecurityControlId": "CloudTrail.1", "StandardsArn":
"arn:aws:securityhub::standards/cis-aws-foundations-benchmark/v/1.4.0",
"AssociationStatus": "DISABLED", "UpdatedReason": "Not applicable to
environment"}]'
```

4. Ripeti l'operazione in ogni regione in cui desideri disattivare il controllo.

Abilitazione automatica di nuovi controlli negli standard abilitati

AWS Security Hub rilascia regolarmente nuovi controlli e li aggiunge a uno o più standard. Puoi scegliere se abilitare automaticamente i nuovi controlli negli standard abilitati.

Note

Se utilizzi la configurazione centrale e includi un elenco di controlli specifici da disabilitare nella tua politica di configurazione (a livello di codice, questo riflette il `DisabledSecurityControlIdentifiers` parametro), Security Hub abilita automaticamente tutti gli altri controlli tra gli standard, inclusi i controlli appena rilasciati. Per ulteriori informazioni, consulta [Come funzionano le politiche di configurazione di Security Hub](#).

Ti consigliamo di utilizzare la configurazione centrale di Security Hub per abilitare automaticamente nuovi controlli di sicurezza. È possibile creare policy di configurazione che includano un elenco di controlli da disabilitare in tutti gli standard. Tutti gli altri controlli, compresi quelli appena rilasciati, sono abilitati per impostazione predefinita. In alternativa, è possibile creare policy che includono un elenco di controlli da abilitare in tutti gli standard. Tutti gli altri controlli, compresi quelli appena

rilasciati, sono disabilitati per impostazione predefinita. Per ulteriori informazioni, consulta [Come funziona la configurazione centrale](#).

Security Hub non abilita nuovi controlli quando vengono aggiunti a uno standard che non hai abilitato.

Le seguenti istruzioni si applicano solo se non si utilizza la configurazione centrale.

Scegli il metodo di accesso preferito e segui i passaggi per abilitare automaticamente i nuovi controlli negli standard abilitati.

Security Hub console

Per abilitare automaticamente i nuovi controlli

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, scegli Impostazioni, quindi scegli la scheda Generale.
3. In Controlli, scegli Modifica.
4. Attiva l'attivazione automatica dei nuovi controlli negli standard abilitati.
5. Selezionare Salva.

Security Hub API

Per abilitare automaticamente i nuovi controlli

1. Esegui [UpdateSecurityHubConfiguration](#).
2. Per abilitare automaticamente nuovi controlli per gli standard abilitati, imposta `AutoEnableControls` su `true`. Se non desideri abilitare automaticamente i nuovi controlli, imposta `AutoEnableControls` su `false`.

AWS CLI

Per abilitare automaticamente i nuovi controlli

1. Esegui il comando [update-security-hub-configuration](#).
2. Per abilitare automaticamente nuovi controlli per gli standard abilitati, specificare `--auto-enable-controls`. Se non desiderate abilitare automaticamente i nuovi controlli, specificate `--no-auto-enable-controls`.

```
aws securityhub update-security-hub-configuration --auto-enable-controls | --no-auto-enable-controls
```

Comando di esempio

```
aws securityhub update-security-hub-configuration --auto-enable-controls
```

Se non abiliti automaticamente i nuovi controlli, devi abilitarli manualmente. Per istruzioni, consulta [the section called “Abilitazione e disabilitazione dei controlli in tutti gli standard”](#).

Parametri di controllo personalizzati

Alcuni controlli Security Hub utilizzano parametri che influiscono sul modo in cui il controllo viene valutato. In genere, tali controlli vengono valutati in base ai valori dei parametri predefiniti definiti da Security Hub. Tuttavia, per un sottoinsieme di questi controlli, è possibile personalizzare i valori dei parametri. Quando personalizzi il valore di un parametro per un controllo, Security Hub inizia a valutare il controllo rispetto al valore specificato. Se la risorsa alla base del controllo soddisfa il valore personalizzato, Security Hub genera un PASSED risultato. Se la risorsa non soddisfa il valore personalizzato, Security Hub genera un FAILED risultato.

Personalizzando i parametri di controllo, puoi affinare le best practice di sicurezza consigliate e monitorate da Security Hub per allinearle ai requisiti aziendali e alle aspettative di sicurezza. Invece di sopprimere i risultati di un controllo, puoi personalizzare uno o più dei relativi parametri per ottenere risultati adatti alle tue esigenze di sicurezza.

Ecco alcuni esempi di casi d'uso per parametri di controllo personalizzati:

- [CloudWatch.16] — i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato

È possibile specificare il periodo di conservazione.

- [IAM.7] — Le politiche relative alle password per gli utenti IAM devono avere configurazioni avanzate

È possibile specificare parametri relativi alla complessità della password.

- [EC2.18] — I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate

È possibile specificare quali porte sono autorizzate a consentire il traffico in entrata senza restrizioni.

- [Lambda.5] — Le funzioni VPC Lambda devono funzionare in più zone di disponibilità

È possibile specificare il numero minimo di zone di disponibilità che generano un risultato superato.

Questa sezione spiega come personalizzare e gestire i parametri di controllo.

Come funzionano i parametri di controllo personalizzati

Un controllo può avere uno o più parametri personalizzabili. I possibili tipi di dati per i singoli parametri di controllo includono:

- Booleano
- Doppio
- Enum
- EnumList
- Numero intero
- IntegerList
- Stringa
- StringList

Per alcuni controlli, i valori dei parametri accettabili devono inoltre rientrare in un intervallo specificato per essere validi. In questi casi, Security Hub fornisce l'intervallo accettabile.

Security Hub sceglie i valori dei parametri predefiniti e potrebbe occasionalmente aggiornarli. Dopo aver personalizzato un parametro di controllo, il suo valore continua a essere il valore specificato per il parametro, a meno che non lo si modifichi. Vale a dire, il parametro interrompe il tracciamento degli aggiornamenti al valore predefinito di Security Hub, anche se il valore personalizzato del parametro corrisponde al valore predefinito corrente definito da Security Hub. Ecco un esempio del controllo [ACM.1]: i certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato:

```
{  
  "SecurityControlId": "ACM.1",
```

```
"Parameters": {
  "daysToExpiration": {
    "ValueType": "CUSTOM",
    "Value": {
      "Integer": 30
    }
  }
}
```

Nell'esempio precedente, il `daysToExpiration` parametro ha un valore personalizzato di 30. Inoltre, il valore predefinito corrente per questo parametro è 30. Se Security Hub modifica il valore predefinito in 14, il parametro in questo esempio non terrà traccia di tale modifica. Manterrà il valore di 30.

Se desideri tenere traccia degli aggiornamenti al valore predefinito di Security Hub per un parametro, imposta il `ValueType` campo su `DEFAULT` invece di `CUSTOM`. Per ulteriori informazioni, consulta [Ripristino dei valori dei parametri predefiniti in un singolo account e regione](#).

Quando modifichi il valore di un parametro, attivi anche un nuovo controllo di sicurezza che valuta il controllo in base al nuovo valore. Security Hub genera quindi nuovi risultati di controllo in base al nuovo valore. Durante gli aggiornamenti periodici per controllare i risultati, Security Hub utilizza anche il nuovo valore del parametro. Se modifichi i valori dei parametri per un controllo, ma non hai abilitato nessuno standard che includa il controllo, Security Hub non esegue alcun controllo di sicurezza utilizzando i nuovi valori. È necessario abilitare almeno uno standard pertinente affinché Security Hub valuti il controllo in base al nuovo valore del parametro.

I valori dei parametri personalizzati si applicano a tutti gli standard abilitati. Non puoi personalizzare i parametri per un controllo che non è supportato nella tua regione attuale. Per un elenco dei limiti regionali per i singoli controlli, consulta [Limiti regionali sui controlli](#).

Personalizzazione dei parametri di controllo

Le istruzioni per personalizzare i parametri di controllo variano a seconda che si utilizzi o meno la configurazione [centrale](#). La configurazione centrale è una funzionalità che l'amministratore delegato di Security Hub può utilizzare per gestire le funzionalità del Security Hub tra Regioni AWS account e unità organizzative (OU) della propria organizzazione.

Se l'organizzazione utilizza la configurazione centrale, l'amministratore delegato può creare politiche di configurazione che includono parametri di controllo personalizzati. Queste politiche

possono essere associate agli account dei membri e alle unità organizzative gestite centralmente e hanno effetto nella regione di origine e in tutte le regioni collegate. L'amministratore delegato può anche designare uno o più account come autogestiti, il che consente al proprietario dell'account di configurare i propri parametri separatamente in ciascuna regione. Se l'organizzazione non utilizza la configurazione centrale, è necessario personalizzare i parametri di controllo separatamente in ogni account e regione.

Personalizzazione dei parametri di controllo su più account e regioni

Quando si utilizza la configurazione centrale, è possibile personalizzare i parametri di controllo per gli account e le unità organizzative gestiti centralmente su più account e regioni. Si consiglia di utilizzare la configurazione centrale perché consente di allineare i valori dei parametri di controllo tra le diverse parti dell'organizzazione. Ad esempio, tutti gli account di test potrebbero utilizzare determinati valori di parametro e tutti gli account di produzione potrebbero utilizzare valori diversi.

Se sei l'amministratore delegato di Security Hub di un'organizzazione che utilizza la configurazione centrale, scegli il metodo preferito e segui i passaggi per personalizzare i parametri di controllo su più account e regioni.

Security Hub console

Per personalizzare i parametri di controllo in più account e regioni

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).

Assicurati di aver effettuato l'accesso alla regione d'origine.

2. Nel riquadro di navigazione, scegli Impostazioni e configurazione.
3. Scegliere la scheda Policy.
4. Per creare una nuova politica di configurazione che includa parametri personalizzati, scegli Crea politica. Per specificare parametri personalizzati in una politica di configurazione esistente, seleziona la politica, quindi scegli Modifica.

Per creare una nuova politica di configurazione con parametri personalizzati

1. Nella sezione Politica personalizzata, scegli gli standard e i controlli di sicurezza che desideri abilitare.
2. Seleziona Personalizza i parametri di controllo.
3. Seleziona un controllo, quindi specifica i valori personalizzati per uno o più parametri.
4. Per personalizzare i parametri per più controlli, scegli Personalizza controllo aggiuntivo.

5. Nella sezione Account, seleziona gli account o le unità organizzative a cui desideri applicare la politica.
6. Seleziona Successivo.
7. Scegli Crea politica e applicala. Nella tua regione d'origine e in tutte le regioni collegate, questa azione sostituisce le impostazioni di configurazione esistenti degli account e delle unità organizzative associati a questa politica di configurazione. Gli account e le unità organizzative possono essere associati a una politica di configurazione tramite applicazione diretta o eredità da un genitore.

Per aggiungere o modificare parametri personalizzati in una politica di configurazione esistente

1. Nella sezione Controlli, in Criteri personalizzati, specificate i nuovi valori dei parametri personalizzati che desiderate.
2. Se è la prima volta che personalizzi i parametri di controllo in questa politica, seleziona Personalizza parametri di controllo, quindi seleziona un controllo da personalizzare. Per personalizzare i parametri per ulteriori controlli, scegli Personalizza controllo aggiuntivo.
3. Nella sezione Account, verifica gli account o le unità organizzative a cui desideri applicare la politica.
4. Seleziona Successivo.
5. Rivedi le modifiche e verifica che siano corrette. Al termine, scegli Salva politica e applica. Nella tua regione d'origine e in tutte le regioni collegate, questa azione sostituisce le impostazioni di configurazione esistenti degli account e delle unità organizzative associati a questa politica di configurazione. Gli account e le unità organizzative possono essere associati a una politica di configurazione tramite applicazione diretta o eredità da un genitore.

Security Hub API

Per personalizzare i parametri di controllo in più account e regioni

Per creare una nuova politica di configurazione con parametri personalizzati

1. Richiama l'[CreateConfigurationPolicy](#) API dall'account amministratore delegato nella regione di residenza.

2. Per l'`SecurityControlCustomParameters` oggetto, fornite l'identificatore di ogni controllo che desiderate personalizzare.
3. Per l'`Parameters` oggetto, fornite il nome di ogni parametro che desiderate personalizzare. Per ogni parametro che personalizzi, fornisci `CUSTOMValueType`. Per `Value`, fornisci il tipo di dati del parametro e il valore personalizzato. Il `Value` campo non può essere vuoto quando lo `ValueType` è `CUSTOM`. Se la richiesta omette un parametro supportato dal controllo, tale parametro mantiene il valore corrente. Puoi trovare parametri, tipi di dati e valori validi supportati per un controllo richiamando l'API. [GetSecurityControlDefinition](#)

Per aggiungere o modificare parametri personalizzati in una politica di configurazione esistente

1. Richiama l'[UpdateConfigurationPolicy](#) API dall'account amministratore delegato nella regione di residenza.
2. Per il `Identifier` campo, fornisci l'Amazon Resource Name (ARN) o l'ID della policy di configurazione che desideri aggiornare.
3. Per l'`SecurityControlCustomParameters` oggetto, fornisci l'identificatore di ogni controllo che desideri personalizzare.
4. Per l'`Parameters` oggetto, fornite il nome di ogni parametro che desiderate personalizzare. Per ogni parametro che personalizzi, fornisci `CUSTOMValueType`. Per `Value`, fornisci il tipo di dati del parametro e il valore personalizzato. Se la richiesta omette un parametro supportato dal controllo, tale parametro mantiene il valore corrente. Puoi trovare parametri, tipi di dati e valori validi supportati per un controllo richiamando l'API. [GetSecurityControlDefinition](#)

Esempio di richiesta API per creare una nuova politica di configurazione:

```
{
  "Name": "SampleConfigurationPolicy",
  "Description": "Configuration policy for production accounts",
  "ConfigurationPolicy": {
    "SecurityHub": {
      "ServiceEnabled": true,
      "EnabledStandardIdentifiers": [
        "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0"},
        "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"}
      ],
    "SecurityControlsConfiguration": {
```

```
    "DisabledSecurityControlIdentifiers": [
      "CloudTrail.2"
    ],
    "SecurityControlCustomParameters": [
      {
        "SecurityControlId": "ACM.1",
        "Parameters": {
          "daysToExpiration": {
            "ValueType": "CUSTOM",
            "Value": {
              "Integer": 15
            }
          }
        }
      }
    ]
  }
}
```

AWS CLI

Per personalizzare i parametri di controllo in più account e regioni

Per creare una nuova politica di configurazione con parametri personalizzati

1. Esegui il [create-configuration-policy](#) comando dall'account amministratore delegato nella regione di residenza.
2. Per l'`SecurityControlCustomParameters` soggetto, fornisci l'identificatore di ogni controllo che desiderate personalizzare.
3. Per l'`Parameters` soggetto, fornisci il nome di ogni parametro che desiderate personalizzare. Per ogni parametro che personalizzi, fornisci `CUSTOM` `ValueType`. Per `Value`, fornisci il tipo di dati del parametro e il valore personalizzato. Il `Value` campo non può essere vuoto quando lo `ValueType` è `CUSTOM`. Se la richiesta omette un parametro supportato dal controllo, tale parametro mantiene il valore corrente. È possibile trovare parametri, tipi di dati e valori validi supportati per un controllo eseguendo il [get-security-control-definition](#) comando.

Per aggiungere o modificare parametri in una politica di configurazione esistente

1. Per aggiungere o aggiornare parametri di input personalizzati in una politica di configurazione esistente, esegui il [update-configuration-policy](#) comando dall'account amministratore delegato nella regione di origine.
2. Per il `identifier` campo, fornisci l'Amazon Resource Name (ARN) o l'ID della policy che desideri aggiornare.
3. Per l'`SecurityControlCustomParameters` soggetto, fornisci l'identificatore di ogni controllo che desideri personalizzare.
4. Per l'`Parameters` soggetto, fornite il nome di ogni parametro che desiderate personalizzare. Per ogni parametro che personalizzi, fornisci `CUSTOMValueType`. Per `Value`, fornisci il tipo di dati del parametro e il valore personalizzato. Se la richiesta omette un parametro supportato dal controllo, tale parametro mantiene il valore corrente. È possibile trovare parametri, tipi di dati e valori validi supportati per un controllo eseguendo il [get-security-control-definition](#) comando.

Comando di esempio per creare una nuova politica di configurazione:

```
$ aws securityhub create-configuration-policy \
--region us-east-1 \
--name "SampleConfigurationPolicy" \
--description "Configuration policy for production accounts" \
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,
"EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1::standards/aws-foundational-security-best-practices/v/1.0.0","arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0"], "SecurityControlsConfiguration":
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":
{"daysToExpiration": {"ValueType": "CUSTOM", "Value": "Integer": 15}}]}}}'
```

Personalizzazione dei parametri di controllo in un unico account e regione

Se non utilizzi la configurazione centrale o disponi di un account autogestito, puoi personalizzare i parametri di controllo per il tuo account in una regione alla volta

Scegli il tuo metodo preferito e segui i passaggi per personalizzare i parametri di controllo. Le modifiche si applicano solo al tuo account nella regione corrente. Per personalizzare i parametri di

controllo in altre regioni, ripeti i passaggi seguenti in ogni account e regione aggiuntivi in cui desideri personalizzare i parametri. Lo stesso controllo può utilizzare valori di parametri diversi in regioni diverse.

Security Hub console

Per personalizzare i parametri di controllo in un account e in una regione

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, scegli Controlli. Nella tabella, scegli un controllo che supporti i parametri personalizzati per cui desideri modificare i parametri. La colonna Parametri personalizzati indica quali controlli supportano i parametri personalizzati.
3. Nella pagina dei dettagli del controllo, scegli la scheda Parametri, quindi scegli Modifica.
4. Specificate i valori dei parametri che desiderate.
5. Facoltativamente, nella sezione Motivo della modifica, selezionare un motivo per la personalizzazione dei parametri.
6. Selezionare Salva.

Security Hub API

Per personalizzare i parametri di controllo in un account e in un'unica regione

1. Invoca l'[UpdateSecurityControl](#) API.
2. Per `SecurityControlId`, fornisci l'ID del controllo che desideri personalizzare.
3. Per l'`Parameters` oggetto, fornisci il nome di ogni parametro che desiderate personalizzare. Per ogni parametro che personalizzi, fornisci `CUSTOMValueType`. Per `Value`, fornisci il tipo di dati del parametro e il valore personalizzato. Se la richiesta omette un parametro supportato dal controllo, tale parametro mantiene il valore corrente. Puoi trovare parametri, tipi di dati e valori validi supportati per un controllo richiamando l'API. [GetSecurityControlDefinition](#)
4. Facoltativamente `LastUpdateReason`, fornisci un motivo per personalizzare i parametri di controllo.

Esempio di richiesta API:

```
{
  "SecurityControlId": "ACM.1",
```

```
"Parameters": {
  "daysToExpiration": {
    "ValueType": "CUSTOM",
    "Value": {
      "Integer": 15
    }
  }
},
"LastUpdateReason": "Internal compliance requirement"
}
```

AWS CLI

Per personalizzare i parametri di controllo in un account e in un'unica regione

1. Esegui il comando [update-security-control](#).
2. Per `security-control-id`, fornisci l'ID del controllo che desideri personalizzare.
3. Per l'`parameters` oggetto, fornisci il nome di ogni parametro che desiderate personalizzare. Per ogni parametro che personalizzi, fornisci `CUSTOMValueType`. Per `Value`, fornisci il tipo di dati del parametro e il valore personalizzato. Se la richiesta omette un parametro supportato dal controllo, tale parametro mantiene il valore corrente. È possibile trovare parametri, tipi di dati e valori validi supportati per un controllo eseguendo il [get-security-control-definition](#) comando.
4. Facoltativamente `last-update-reason`, fornisci un motivo per personalizzare i parametri di controllo.

Comando di esempio:

```
$ aws securityhub update-security-control \
--region us-east-1 \
--security-control-id ACM.1 \
--parameters '{"daysToExpiration": {"ValueType": "CUSTOM", "Value": {"Integer": 15}}}' \
--last-update-reason "Internal compliance requirement"
```

Verifica dello stato dei parametri di controllo

È importante convalidare e controllare lo stato delle modifiche ai parametri di controllo. Questo aiuta a garantire che un controllo funzioni come previsto e fornisca il valore di sicurezza previsto. Per verificare che l'aggiornamento di un parametro sia andato a buon fine, puoi esaminare i dettagli del controllo sulla console Security Hub. Sulla console, scegli il controllo per visualizzarne i dettagli. La scheda Parametri mostra lo stato della modifica del parametro.

A livello di programmazione, se la richiesta di aggiornamento di un parametro è valida, il valore del `UpdateStatus` campo è `UPDATING` in risposta all'[BatchGetSecurityControls](#) operazione. Ciò significa che l'aggiornamento era valido, ma i risultati potrebbero non includere ancora i valori dei parametri aggiornati. Quando il valore di `UpdateState` viene modificato in `READY`, i risultati iniziano a includere i valori dei parametri aggiornati.

L'`UpdateSecurityControl` operazione restituisce una `InvalidInputException` risposta per i valori dei parametri non validi. La risposta fornisce ulteriori dettagli sul motivo dell'errore. Ad esempio, è possibile che abbiate specificato un valore che non rientra nell'intervallo valido per un parametro. Oppure, hai specificato un valore che non utilizza il tipo di dati corretto. Invia nuovamente la richiesta con un input valido. Se l'aggiornamento di un parametro non riesce, Security Hub mantiene il valore corrente del parametro.

Se si verifica un errore interno quando si tenta di aggiornare il valore di un parametro, Security Hub riprova automaticamente se è stato AWS Config abilitato. Per ulteriori informazioni, consulta [Configurazione AWS Config](#).

Revisione dei parametri di controllo

Puoi rivedere i valori correnti dei singoli parametri di controllo nel tuo account. Se si utilizza la configurazione centrale, l'amministratore delegato del Security Hub può anche esaminare i valori dei parametri specificati in una politica di configurazione.

Scegliete il metodo preferito e seguite i passaggi per rivedere i valori correnti dei parametri di controllo.

Security Hub console

Per rivedere i valori dei parametri correnti

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, scegli Controlli. Scegli un controllo.

3. Scegli la scheda Parametri. Questa scheda mostra i valori correnti dei parametri per il controllo.

Security Hub API

Per rivedere i valori dei parametri correnti

Richiama l'[BatchGetSecurityControls](#) API e fornisci uno o più ARN o ID di controllo di sicurezza. L'Parametersoggetto nella risposta mostra i valori correnti dei parametri per i controlli specificati.

Esempio di richiesta API:

```
{
  "SecurityControlIds": ["APIGateway.1", "CloudWatch.15", "IAM.7"]
}
```

AWS CLI

Per rivedere i valori correnti dei parametri

Esegui il [batch-get-security-controls](#) comando e fornisci uno o più ARN o ID di controllo di sicurezza. L'Parametersoggetto nella risposta mostra i valori correnti dei parametri per i controlli specificati.

Comando di esempio:

```
$ aws securityhub batch-get-security-controls \
--region us-east-1 \
--security-control-ids '["APIGateway.1", "CloudWatch.15", "IAM.7"]'
```

Scegliete il metodo preferito per visualizzare i valori correnti dei parametri in una politica di configurazione centrale.

Security Hub console

Per esaminare i valori dei parametri correnti in una politica di configurazione

1. Apri la AWS Security Hub console all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).

Accedi utilizzando le credenziali dell'account amministratore delegato di Security Hub nella regione di residenza.

2. Nel riquadro di navigazione, scegli Impostazioni e configurazione.
3. Nella scheda Politiche, seleziona la politica di configurazione, quindi scegli Visualizza dettagli. Vengono quindi visualizzati i dettagli della politica, inclusi i valori dei parametri correnti.

Security Hub API

Per esaminare i valori dei parametri correnti in una politica di configurazione

1. Richiama l'[GetConfigurationPolicy](#) API dall'account amministratore delegato nella regione di residenza.
2. Fornisci l'ARN o l'ID della politica di configurazione di cui desideri visualizzare i dettagli. La risposta include i valori dei parametri correnti.

```
{
  "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
```

AWS CLI

Per esaminare i valori dei parametri correnti in una politica di configurazione

1. Esegui il [get-configuration-policy](#) comando dall'account amministratore delegato nella regione di residenza.
2. Fornisci l'ARN o l'ID della politica di configurazione di cui desideri visualizzare i dettagli. La risposta include i valori dei parametri correnti.

```
$ aws securityhub get-configuration-policy \
--region us-east-1 \
--identifier "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
```


I risultati del controllo mostrano anche i valori dei parametri correnti. In [AWS Sintassi del Security Finding Format \(ASFF\)](#), questi valori vengono visualizzati nel Parameters campo dell'Complianceoggetto. Per esaminare i risultati sulla console Security Hub, scegli Findings nel riquadro di navigazione. Per esaminare i risultati a livello di codice, usa l'[GetFindings](#)operazione.

Note

Dopo il rilascio della funzionalità dei parametri di controllo personalizzati, Security Hub aggiornerà i risultati di controllo esistenti per includere il campo Parameters ASFF. Questa operazione potrebbe richiedere fino a 24 ore.

Ripristino dei valori dei parametri di controllo predefiniti

Un parametro di controllo può avere un valore predefinito definito da Security Hub. Potremmo aggiornare il valore predefinito di un parametro per riflettere le migliori pratiche di sicurezza in evoluzione. Se non hai specificato un valore personalizzato per un parametro di controllo, il controllo tiene automaticamente traccia di tali aggiornamenti e utilizza il nuovo valore predefinito.

È possibile tornare a utilizzare i valori dei parametri predefiniti per un controllo. Il modo in cui eseguire questa operazione dipende dall'utilizzo o meno della configurazione centrale.

Note

Non tutti i parametri di controllo hanno un valore Security Hub predefinito. In questi casi, quando Value Type è impostato su DEFAULT, non esiste un valore predefinito specifico utilizzato da Security Hub. Piuttosto, Security Hub ignora il parametro in assenza di un valore personalizzato.

Ripristino dei valori dei parametri predefiniti su più account e regioni

Se si utilizza la configurazione centrale, è possibile ripristinare i parametri di controllo per gli account e le unità organizzative gestiti centralmente su più account e regioni.

Scegli il tuo metodo preferito e segui i passaggi per ripristinare i valori dei parametri predefiniti su più account e regioni utilizzando la configurazione centrale.

Security Hub console

Per ripristinare i valori dei parametri predefiniti in più account e regioni


1. Apri la AWS Security Hub console all'indirizzo <https://console.aws.amazon.com/securityhub/>.
Accedi utilizzando le credenziali dell'account amministratore delegato di Security Hub nella regione di residenza.
2. Nel riquadro di navigazione, scegli Impostazioni e configurazione.
3. Scegliere la scheda Policy.
4. Seleziona una politica, quindi scegli Modifica.
5. In Criteri personalizzati, la sezione Controlli mostra un elenco di controlli per i quali sono stati specificati parametri personalizzati.
6. Trova il controllo che ha uno o più valori di parametro da ripristinare. Quindi, scegli Rimuovi per ripristinare i valori predefiniti.
7. Nella sezione Account, verifica gli account o le unità organizzative a cui desideri applicare la politica.
8. Seleziona Successivo.
9. Rivedi le modifiche e verifica che siano corrette. Al termine, scegli Salva politica e applica. Nella tua regione d'origine e in tutte le regioni collegate, questa azione sostituisce le impostazioni di configurazione esistenti degli account e delle unità organizzative associati a questa politica di configurazione. Gli account e le unità organizzative possono essere associati a una politica di configurazione tramite applicazione diretta o eredità da un genitore.

Security Hub API

Per ripristinare i valori dei parametri predefiniti in più account e regioni

1. Richiama l'[UpdateConfigurationPolicy](#) API dall'account amministratore delegato nella regione di origine.
2. Per il `Identifier` campo, fornisci l'Amazon Resource Name (ARN) o l'ID della policy che desideri aggiornare.
3. Per l'`SecurityControlCustomParameters` oggetto, fornisci l'identificatore di ogni controllo per il quale desideri ripristinare uno o più parametri.
4. Nell'`Parameters` oggetto, per ogni parametro che desideri ripristinare, inserisci DEFAULT il campo. `ValueType` Quando `ValueType` è impostato su DEFAULT, non è necessario fornire

un valore per il Value campo. Se nella richiesta è incluso un valore, Security Hub lo ignora. Se la richiesta omette un parametro supportato dal controllo, tale parametro mantiene il valore corrente.

 Warning

Se si omette un oggetto di controllo dal SecurityControlCustomParameters campo, Security Hub ripristina tutti i parametri personalizzati per il controllo ai valori predefiniti. Un elenco completamente vuoto riporta SecurityControlCustomParameters i parametri personalizzati per tutti i controlli ai valori predefiniti.

Esempio di richiesta API:

```
{
  "Identifier": "arn:aws:securityhub:us-east-1:123456789012:configuration-policy/
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "Name": "TestConfigurationPolicy",
  "Description": "Updated configuration policy",
  "UpdatedReason": "Revert ACM.1 parameter to default value",
  "ConfigurationPolicy": {
    "SecurityHub": {
      "ServiceEnabled": true,
      "EnabledStandardIdentifiers": [
        "arn:aws:securityhub:us-east-1::standards/aws-foundational-
security-best-practices/v/1.0.0",
        "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0"
      ],
      "SecurityControlsConfiguration": {
        "DisabledSecurityControlIdentifiers": [
          "CloudTrail.2"
        ],
        "SecurityControlCustomParameters": [
          {
            "SecurityControlId": "ACM.1",
            "Parameters": {
              "daysToExpiration": {
                "ValueType": "DEFAULT"
              }
            }
          }
        ]
      }
    }
  }
}
```



```
--description "Updated configuration policy" \  
--updated-reason "Revert ACM.1 parameter to default value"  
--configuration-policy '{"SecurityHub": {"ServiceEnabled": true,  
  "EnabledStandardIdentifiers": ["arn:aws:securityhub:us-east-1:standards/aws-  
foundational-security-best-practices/v/1.0.0","arn:aws:securityhub:::ruleset/  
cis-aws-foundations-benchmark/v/1.2.0"],"SecurityControlsConfiguration":  
{"DisabledSecurityControlIdentifiers": ["CloudTrail.2"],  
"SecurityControlCustomParameters": [{"SecurityControlId": "ACM.1", "Parameters":  
{"daysToExpiration": {"ValueType": "DEFAULT"}}]}}}'
```

Ripristino dei valori dei parametri predefiniti in un singolo account e regione

Se non utilizzi la configurazione centrale o disponi di un account autogestito, puoi tornare a utilizzare i valori dei parametri predefiniti per il tuo account in una regione alla volta.

Scegli il tuo metodo preferito e segui i passaggi per ripristinare i valori dei parametri predefiniti per il tuo account in una singola regione. Per ripristinare i valori dei parametri predefiniti in altre regioni, ripeti questi passaggi in ogni regione aggiuntiva.

Note

Se disabiliti Security Hub, i parametri di controllo personalizzati vengono ripristinati. Se abiliti nuovamente Security Hub in futuro, tutti i controlli utilizzeranno i valori dei parametri predefiniti per iniziare.

Security Hub console

Per ripristinare i valori dei parametri predefiniti in un account e in una regione

1. Apri la AWS Security Hub console all'indirizzo <https://console.aws.amazon.com/securityhub/>.
2. Nel riquadro di navigazione, scegli Controlli. Scegliete il controllo per il quale desiderate ripristinare i valori dei parametri predefiniti.
3. Nella Parameters scheda, scegli Personalizzato accanto a un parametro di controllo. Quindi, scegli Rimuovi personalizzazione. Questo parametro ora utilizza il valore predefinito di Security Hub e tiene traccia degli aggiornamenti futuri al valore predefinito.
4. Ripetere il passaggio precedente per ogni valore di parametro che si desidera ripristinare.

Security Hub API

Per ripristinare i valori dei parametri predefiniti in un account e in una regione

1. Invoca l'API. [UpdateSecurityControl](#)
2. Per `SecurityControlId`, fornisci l'ARN o l'ID del controllo di cui desideri ripristinare i parametri.
3. Nell'`Parameters` oggetto, per ogni parametro che desideri ripristinare, inserisci `DEFAULT` il campo. `ValueType` Quando `ValueType` è impostato su `DEFAULT`, non è necessario fornire un valore per il `Value` campo. Se nella richiesta è incluso un valore, Security Hub lo ignora.
4. Facoltativamente `LastUpdateReason`, fornisci un motivo per ripristinare i valori dei parametri predefiniti.

Esempio di richiesta API:

```
{
  "SecurityControlId": "ACM.1",
  "Parameters": {
    "daysToExpiration": {
      "ValueType": "DEFAULT"
    },
  },
  "LastUpdateReason": "New internal requirement"
}
```

AWS CLI

Per ripristinare i valori dei parametri predefiniti in un account e in una regione

1. Esegui il comando [update-security-control](#).
2. Per `security-control-id`, fornisci l'ARN o l'ID del controllo di cui desideri ripristinare i parametri.
3. Nell'`parameters` oggetto, per ogni parametro che desideri ripristinare, inserisci `DEFAULT` il campo. `ValueType` Quando `ValueType` è impostato su `DEFAULT`, non è necessario fornire un valore per il `Value` campo. Se nella richiesta è incluso un valore, Security Hub lo ignora.
4. Facoltativamente `last-update-reason`, fornisci un motivo per ripristinare i valori dei parametri predefiniti.

Comando di esempio:

```
$ aws securityhub update-security-control \  
--region us-east-1 \  
--security-control-id ACM.1 \  
--parameters '{"daysToExpiration": {"ValueType": "DEFAULT"}}' \  
--last-update-reason "New internal requirement"
```

Controlli che supportano parametri personalizzati

Per un elenco dei controlli di sicurezza che supportano i parametri personalizzati, puoi fare riferimento alla pagina Controlli sulla console Security Hub o al [Riferimento ai controlli del Security Hub](#). Per recuperare questo elenco a livello di codice, è possibile utilizzare l'operazione [ListSecurityControlDefinitions](#). Nella risposta, l'CustomizablePropertiesoggetto indica quali controlli supportano parametri personalizzabili.

Controlli del Security Hub che potresti voler disabilitare

Ti consigliamo di disabilitare alcuni AWS Security Hub controlli per ridurre i rumori di ricerca e limitare i costi.

Controlli che riguardano le risorse globali

Alcuni Servizi AWS supportano risorse globali, il che significa che puoi accedere alla risorsa da qualsiasi Regione AWS. Per risparmiare sui costi di AWS Config, puoi disabilitare la registrazione delle risorse globali in tutte le regioni tranne una. Dopo aver eseguito questa operazione, tuttavia, Security Hub continua a eseguire i controlli di sicurezza in tutte le regioni in cui è abilitato un controllo e ti addebita in base al numero di controlli per account per regione. Di conseguenza, per ridurre i rumori di ricerca e risparmiare sui costi di Security Hub, è necessario disabilitare anche i controlli che coinvolgono risorse globali in tutte le regioni ad eccezione della regione che registra le risorse globali.

Se un controllo coinvolge risorse globali ma è disponibile in una sola regione, disabilitarlo in quella regione impedisce di ottenere risultati sulla risorsa sottostante. In questo caso, consigliamo di mantenere il controllo abilitato. Quando si utilizza l'aggregazione tra regioni, la regione in cui è disponibile il controllo deve essere la regione di aggregazione o una delle regioni collegate. I seguenti controlli coinvolgono risorse globali ma sono disponibili solo in una singola regione:

- Tutti i CloudFront controlli: disponibili solo negli Stati Uniti orientali (Virginia settentrionale)

- GlobalAccelerator.1 — Disponibile solo negli Stati Uniti occidentali (Oregon)
- Route53.2 — Disponibile solo negli Stati Uniti orientali (Virginia settentrionale)
- WAF.1, WAF.6, WAF.7 e WAF.8 — Disponibile solo negli Stati Uniti orientali (Virginia settentrionale)

Note

Se si utilizza la configurazione centrale, Security Hub disattiva automaticamente i controlli che coinvolgono risorse globali in tutte le regioni tranne la regione di origine. Gli altri controlli che scegli di abilitare tramite una politica di configurazione sono abilitati in tutte le regioni in cui sono disponibili. Per limitare i risultati di questi controlli a una sola regione, puoi aggiornare le impostazioni del AWS Config registratore e disattivare la registrazione globale delle risorse in tutte le regioni tranne la regione d'origine. Quando utilizzi la configurazione centrale, non hai la copertura necessaria per un controllo che non è disponibile nella regione d'origine e in nessuna delle regioni collegate. Per ulteriori informazioni sulla configurazione centrale, consulta [Come funziona la configurazione centrale](#).

Se si disabilita la registrazione di risorse globali in una o più regioni, il controllo [Config.1] AWS Config deve essere abilitato genera una ricerca non riuscita in tali regioni. Questo perché Config.1 richiede la registrazione delle risorse globali per poter passare. [È possibile sopprimere i risultati di questo controllo manualmente o tramite una regola di automazione.](#)

Per i controlli con un tipo di pianificazione periodica, è necessario disabilitarli in Security Hub per impedire la fatturazione. L'impostazione del AWS Config parametro `includeGlobalResourceTypes` su `false` non influisce sui controlli periodici del Security Hub.

Di seguito è riportato un elenco di controlli del Security Hub che coinvolgono risorse globali:

- [\[Account.1\] Le informazioni di contatto di sicurezza devono essere fornite per un Account AWS](#)
- [\[Account.2\] Account AWS deve far parte di un'organizzazione AWS Organizations](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)

- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)
- [\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)
- [\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)
- [\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)
- [\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)
- [\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)
- [\[IAM.7\] Le politiche relative alle password per gli utenti IAM dovrebbero avere configurazioni solide](#)
- [\[IAM.8\] Le credenziali utente IAM non utilizzate devono essere rimosse](#)
- [\[IAM.9\] L'MFA deve essere abilitata per l'utente root](#)
- [\[IAM.10\] Le politiche relative alle password per gli utenti IAM dovrebbero avere durate elevate AWS Config](#)
- [\[IAM.11\] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola](#)
- [\[IAM.12\] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola](#)
- [\[IAM.13\] Assicurati che la politica delle password IAM richieda almeno un simbolo](#)
- [\[IAM.14\] Assicurati che la politica delle password IAM richieda almeno un numero](#)
- [\[IAM.15\] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14](#)
- [\[IAM.16\] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password](#)

- [\[IAM.17\] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno](#)
- [\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)
- [\[IAM.19\] L'MFA deve essere abilitata per tutti gli utenti IAM](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)
- [\[IAM.22\] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse](#)
- [\[IAM.22\] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse](#)
- [\[IAM.22\] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse](#)
- [\[IAM.22\] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[KMS.1\] Le politiche gestite dai clienti di IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS](#)
- [\[KMS.2\] I principali IAM non devono disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.10\] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

Controlli che si occupano della CloudTrail registrazione

Questo controllo si occupa dell'utilizzo di AWS Key Management Service (AWS KMS) per crittografare i log delle AWS CloudTrail tracce. Se registri questi percorsi in un account di registrazione centralizzato, devi solo abilitare questo controllo nell'account e nella regione in cui avviene la registrazione centralizzata.

Note

Se si utilizza la [configurazione centrale](#), lo stato di attivazione di un controllo è allineato tra la regione di origine e le regioni collegate. Non è possibile disabilitare un controllo in alcune regioni e abilitarlo in altre. In questo caso, sopprimi i risultati dei seguenti controlli per ridurre i disturbi rilevati.

- [\[CloudTrail.2\] CloudTrail dovrebbe avere la crittografia a riposo abilitata](#)

Controlli che gestiscono gli allarmi CloudWatch

Se preferisci utilizzare Amazon GuardDuty per il rilevamento delle anomalie anziché gli CloudWatch allarmi Amazon, puoi disabilitare questi controlli, che si concentrano sugli CloudWatch allarmi.

- [\[CloudWatch.1\] Dovrebbero esistere un filtro logmetrico e un allarme per l'utilizzo da parte dell'utente «root»](#)
- [\[CloudWatch.2\] Assicurati che esistano un filtro metrico di log e un allarme per le chiamate API non autorizzate](#)
- [\[CloudWatch.3\] Assicurarsi che esistano un filtro metrico di registro e un allarme per l'accesso alla Console di gestione senza MFA](#)
- [\[CloudWatch.4\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy IAM](#)
- [\[CloudWatch.5\] Assicurati che esistano un filtro metrico di registro e un allarme per le CloudTrail AWS Config variazioni di durata](#)
- [\[CloudWatch.6\] Assicurati che esistano un filtro metrico di registro e un allarme per gli AWS Management Console errori di autenticazione](#)
- [\[CloudWatch.7\] Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o l'eliminazione programmata delle chiavi gestite dal cliente](#)
- [\[CloudWatch.8\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alle policy dei bucket S3](#)
- [\[CloudWatch.9\] Assicurati che esistano un filtro metrico di log e un allarme per le AWS Config modifiche alla configurazione](#)
- [\[CloudWatch.10\] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche ai gruppi di sicurezza](#)

- [\[CloudWatch.11\] Assicurati che esistano un filtro metrico di registro e un allarme per le modifiche alle liste di controllo degli accessi alla rete \(NACL\)](#)
- [\[CloudWatch.12\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche ai gateway di rete](#)
- [\[CloudWatch.13\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla tabella delle rotte](#)
- [\[CloudWatch.14\] Assicurati che esistano un filtro metrico di log e un allarme per le modifiche al VPC](#)

Visualizzazione dei dettagli di un controllo

Per ogni AWS Security Hub controllo, è possibile visualizzare una pagina di dettagli utili.

La parte superiore della pagina dei dettagli del controllo offre una panoramica del controllo, tra cui:

- Stato di abilitazione: la parte superiore della pagina indica se il controllo è abilitato per almeno uno standard in almeno un account membro. Se è stata impostata una regione di aggregazione, il controllo è abilitato se è abilitato per almeno uno standard in almeno una regione. Se il controllo è disabilitato, puoi abilitarlo da questa pagina. Se il controllo è abilitato, è possibile disabilitarlo da questa pagina. Per ulteriori informazioni, consulta [the section called “Abilitazione e disabilitazione dei controlli in tutti gli standard”](#).
- Stato del controllo: questo stato riassume le prestazioni di un controllo in base allo stato di conformità dei risultati del controllo. Security Hub genera in genere lo stato di controllo iniziale entro 30 minuti dalla prima visita alla pagina di riepilogo o alla pagina degli standard di sicurezza sulla console di Security Hub. Gli stati sono disponibili solo per i controlli abilitati quando si visitano tali pagine. Utilizza l'operazione [UpdateStandardsControl](#) API per abilitare o disabilitare un controllo. Inoltre, la registrazione AWS Config delle risorse deve essere configurata per visualizzare lo stato del controllo. Dopo la prima generazione degli stati di controllo, Security Hub aggiorna lo stato del controllo ogni 24 ore in base ai risultati delle 24 ore precedenti. Nella pagina dei dettagli standard e nella pagina dei dettagli del controllo, Security Hub visualizza un timestamp per indicare quando lo stato è stato aggiornato l'ultima volta.

Gli account amministratore visualizzano uno stato di controllo aggregato tra l'account amministratore e gli account dei membri. Se hai impostato una regione di aggregazione, lo stato di controllo include i risultati in tutte le regioni collegate. Per ulteriori informazioni sullo stato del controllo, vedere [the section called “Stato di conformità e stato di controllo”](#).

Note

Possono essere necessarie fino a 24 ore dall'attivazione di un controllo per la generazione degli stati di controllo per la prima volta nelle regioni della Cina e. AWS GovCloud (US) Region

La scheda Standard e requisiti elenca gli standard per i quali è possibile abilitare un controllo e i requisiti relativi al controllo da diversi quadri di conformità.

La parte inferiore della pagina dei dettagli contiene informazioni sui risultati attivi del controllo. I risultati del controllo vengono generati dai controlli di sicurezza relativi al controllo. L'elenco dei risultati di controllo non include i risultati archiviati.

L'elenco dei risultati utilizza schede che visualizzano diversi sottoinsiemi dell'elenco. Nella maggior parte delle schede, l'elenco dei risultati mostra i risultati con uno stato del flusso di lavoro pari a NEW, NOTIFIED o. RESOLVED I SUPPRESSED risultati vengono visualizzati in una scheda separata.

Per ogni risultato, l'elenco fornisce l'accesso ai dettagli della ricerca, come lo stato di conformità e le risorse correlate. È inoltre possibile impostare lo stato del flusso di lavoro di ogni risultato e inviare i risultati ad azioni personalizzate. Per ulteriori informazioni, consulta [the section called “Visualizzazione e adozione di misure in base ai risultati del controllo”](#).

Visualizzazione dei dettagli di un controllo

Scegli il metodo di accesso preferito e segui questi passaggi per visualizzare i dettagli di un controllo. I dettagli si applicano all'account corrente e alla regione e includono quanto segue:

- Titolo e descrizione del controllo
- Link alle istruzioni di riparazione in caso di esito negativo del controllo
- Severità del controllo
- Stato di attivazione del controllo
- (Sulla console) Un elenco di risultati recenti relativi al controllo. Quando si utilizza l'API Security Hub o AWS CLI, si utilizza [GetFindings](#) per recuperare i risultati del controllo.

Security Hub console

1. Apri la AWS Security Hub console all'indirizzo <https://console.aws.amazon.com/securityhub/>.

2. Scegli Controlli nel riquadro di navigazione.
3. Seleziona un controllo.

Security Hub API

1. Esegui [ListSecurityControlDefinitions](#) e fornisci uno o più ARN standard per ottenere un elenco di ID di controllo per quello standard. Per ottenere ARN standard, esegui [DescribeStandards](#). Se non fornisci un ARN standard, questa API restituisce tutti gli ID di controllo del Security Hub. Questa API restituisce ID di controllo di sicurezza indipendenti dagli standard, non gli ID di controllo basati su standard esistenti prima di queste versioni di funzionalità.

Richiesta di esempio:

```
{
  "StandardsArn": "arn:aws:securityhub:::standards/aws-foundational-security-
  best-practices/v/1.0.0"
}
```

2. Esegui [BatchGetSecurityControls](#) per ottenere dettagli su uno o più controlli nella versione corrente Account AWS e Regione AWS.

Richiesta di esempio:

```
{
  "SecurityControlIds": ["Config.1", "IAM.1"]
}
```

AWS CLI

1. Esegui il [list-security-control-definitions](#) comando e fornisci uno o più ARN standard per ottenere un elenco di ID di controllo. Per ottenere ARN standard, esegui il `describe-standards` comando. Se non si fornisce un ARN standard, questo comando restituisce tutti gli ID di controllo del Security Hub. Questo comando restituisce gli ID di controllo di sicurezza indipendenti dagli standard, non gli ID di controllo basati sugli standard che esistevano prima di queste versioni di funzionalità.

```
aws securityhub --region us-east-1 list-security-control-definitions --  
standards-arn "arn:aws:securityhub:us-east-1::standards/aws-foundational-  
security-best-practices/v/1.0.0"
```

2. Esegui il [batch-get-security-controls](#) comando per ottenere dettagli su uno o più controlli nella versione corrente e. Account AWS Regione AWS

```
aws securityhub --region us-east-1 batch-get-security-controls --security-  
control-ids '["Config.1", "IAM.1"]'
```

Filtraggio e ordinamento dell'elenco dei controlli

Nella pagina Controlli, puoi visualizzare un elenco dei tuoi controlli. Puoi filtrare e ordinare l'elenco per concentrarti su un sottoinsieme specifico di controlli.

- Tutti abilitati (controlli abilitati in almeno uno standard abilitato)
- Fallito (controlli con uno Failed stato)
- Sconosciuto (controlli con uno Unknown stato)
- Passato (controlli con Passed stato)
- Disabilitato (controlli disabilitati in tutti gli standard)
- Nessun dato (controlli senza risultati)
- Tutti (contano tutti i controlli, abilitati e disabilitati, indipendentemente dallo stato del controllo o dai risultati)

Per ulteriori informazioni sullo stato del controllo, vedere [Stato di conformità e stato di controllo](#).

Se utilizzi l'integrazione con AWS Organizations e hai effettuato l'accesso all'account AWS Security Hub amministratore, la scheda Tutti abilitati include i controlli abilitati in almeno un account membro. Se hai impostato una regione di aggregazione, la scheda Tutti abilitati include i controlli abilitati in almeno una regione collegata.

La scheda Failed è visualizzata per impostazione predefinita. In ogni scheda, per impostazione predefinita, i controlli sono ordinati per gravità, da Critico a Basso. È inoltre possibile ordinare i controlli in base all'ID del controllo, allo stato di conformità, alla gravità o al numero di controlli non riusciti. La barra di ricerca consente di cercare controlli specifici.

Tip

Se disponi di flussi di lavoro automatizzati basati sui risultati del controllo, ti consigliamo di utilizzare i [campi SecurityControlId o SecurityControlArn ASFF](#) come filtri, anziché Title o Description. Questi ultimi campi possono cambiare occasionalmente, mentre l'ID di controllo e l'ARN sono identificatori statici.

Scegliendo l'opzione accanto al controllo viene visualizzato un pannello laterale che mostra gli standard in cui il controllo è attualmente abilitato. Puoi anche vedere gli standard in cui il controllo è attualmente disabilitato. Da questo pannello è possibile disabilitare un controllo disattivandolo in tutti gli standard. Per ulteriori informazioni sull'attivazione e la disabilitazione dei controlli tra gli standard, vedere [Abilitazione e disabilitazione dei controlli in tutti gli standard](#). Per gli account amministratore, le informazioni presentate nel pannello laterale si riferiscono a tutti gli account dei membri.

Nell'API Security Hub, [ListSecurityControlDefinitions](#) esegui per recuperare un elenco di ID di controllo. Una volta ottenuti gli ID di controllo che ti interessano, corri [BatchGetSecurityControls](#) a recuperare i dati relativi a quel sottoinsieme di controlli per l'attuale Account AWS e Regione AWS.

Visualizzazione e adozione di misure in base ai risultati del controllo

La pagina dei dettagli del controllo mostra un elenco di risultati attivi per un controllo. L'elenco non include i risultati archiviati.

La pagina dei dettagli del controllo supporta l'aggregazione dei risultati. Se è stata impostata una regione di aggregazione, lo stato del controllo e l'elenco dei controlli di sicurezza nella pagina dei dettagli del controllo includono i controlli provenienti da tutti i collegamenti. Regioni AWS

L'elenco fornisce strumenti per filtrare e ordinare i risultati, in modo che tu possa concentrarti prima sui risultati più urgenti. Una scoperta può includere collegamenti ai dettagli delle risorse nella relativa console di servizio. Per i controlli basati su AWS Config regole, è possibile visualizzare i dettagli sulla regola e sulla sequenza temporale di configurazione.

Puoi anche utilizzare l' AWS Security Hub API per recuperare un elenco di risultati. Per ulteriori informazioni, consulta [the section called “Esame dei dettagli del ritrovamento”](#).

Argomenti

- [Visualizzazione dei dettagli relativi a una risorsa di ricerca e ricerca di controlli](#)

- [Esempi di risultati del controllo](#)
- [Filtraggio, ordinamento e download dei risultati di controllo](#)
- [Intervenire in base ai risultati del controllo](#)

Visualizzazione dei dettagli relativi a una risorsa di ricerca e ricerca di controlli

AWS Security Hub fornisce i seguenti dettagli per ogni risultato di controllo per aiutarvi a esaminarlo:

- Una cronologia delle modifiche apportate dagli utenti al risultato
- Un `.json` file per la scoperta
- Informazioni sulla risorsa relativa al ritrovamento
- La regola di configurazione relativa al risultato
- Note che gli utenti hanno aggiunto al risultato

La sezione seguente spiega come accedere a questi dettagli.

Cronologia delle ricerche

La cronologia delle ricerche è una funzionalità del Security Hub che consente di tenere traccia delle modifiche apportate a un risultato negli ultimi 90 giorni.

La cronologia dei risultati è disponibile per i risultati di controllo e altri risultati del Security Hub. Per ulteriori informazioni, consulta [Revisione della cronologia dei risultati](#).

Visualizzazione del file.json completo per un risultato

È possibile visualizzare e scaricare la versione completa `.json` di un risultato.

Per visualizzare il `.json`, nella colonna Finding `.json`, scegli l'icona.

Nel pannello Finding JSON, per scaricare il file, scegliete **.json Scarica**.

Visualizzazione delle informazioni su una risorsa di ricerca

La colonna Risorsa contiene il tipo di risorsa e l'identificatore della risorsa.

Per visualizzare le informazioni sulla risorsa, scegliete l'identificatore della risorsa. Infatti Account AWS, se l'account è un account di membro dell'organizzazione, le informazioni includono sia l'ID dell'account che il nome dell'account. Per gli account che sono stati invitati manualmente, le informazioni includono solo l'ID dell'account.

Se si dispone dell'autorizzazione per visualizzare la risorsa nel servizio originale, l'identificatore della risorsa visualizza un collegamento al servizio. Ad esempio, per un AWS utente, i dettagli della risorsa forniscono un collegamento per visualizzare i dettagli dell'utente in IAM.

Se la risorsa si trova in un account diverso, Security Hub visualizza un messaggio per avvisarti.

Visualizzazione della cronologia di configurazione per una risorsa di ricerca

Una via di indagine è la tempistica di configurazione della risorsa in AWS Config

Se sei autorizzato a visualizzare la sequenza temporale di configurazione per la risorsa di ricerca, l'elenco dei risultati fornisce un collegamento alla sequenza temporale.

Security Hub visualizza un messaggio per avvisarti se la risorsa si trova in un account diverso.

Per accedere alla sequenza temporale di configurazione in AWS Config

1. Nella colonna Indagate, scegliete l'icona.
2. Nel menu, scegliete Cronologia della configurazione. Se non hai accesso alla timeline di configurazione, il link non viene visualizzato.

Visualizzazione della AWS Config regola per una risorsa di ricerca

Se il controllo è basato su una AWS Config regola, potresti anche voler visualizzare i dettagli della AWS Config regola. Le informazioni sulla AWS Config regola possono aiutarti a comprendere meglio il motivo per cui un controllo ha avuto esito positivo o negativo.

Se si dispone dell'autorizzazione per visualizzare la AWS Config regola per il controllo, l'elenco dei risultati fornisce un collegamento alla AWS Config regola in AWS Config.

Security Hub visualizza un messaggio per avvisarti se la risorsa si trova in un account diverso.

Per accedere alla AWS Config regola

1. Nella colonna Indaga, scegli l'icona.
2. Nel menu, scegli Config rule. Se non hai accesso alla AWS Config regola, la regola Config non è collegata.

Visualizzazione delle note relative ai risultati

Se a un risultato è associata una nota, nella colonna Aggiornato viene visualizzata l'icona di una nota.

Per visualizzare la nota associata a un risultato

Nella colonna Aggiornato, scegliete l'icona della nota.

Esempi di risultati del controllo

Il formato dei risultati di controllo varia a seconda che tu abbia attivato o meno i risultati di controllo consolidati. Quando attivi questa funzionalità, Security Hub genera un singolo risultato per un controllo di controllo anche quando il controllo si applica a più standard abilitati. Per ulteriori informazioni, consulta [Risultati di controllo consolidati](#).

La sezione seguente mostra esempi di risultati di controllo. Questi includono i risultati di ogni standard di Security Hub quando i risultati del controllo consolidato sono disattivati nel tuo account e un esempio di risultato di controllo tra gli standard quando è attivato.

Note

I risultati faranno riferimento a diversi campi e valori nelle regioni e nella AWS GovCloud (US) regione della Cina. Per ulteriori informazioni, consulta [Impatto del consolidamento sui campi e sui valori ASFF](#).

I risultati del controllo consolidato sono disattivati

- [Esempi di risultati relativi allo standard AWS Foundational Security Best Practices \(FSBP\)](#)
- [Esempio di ricerca per Center for Internet Security \(CIS\) Foundations Benchmark v1.2.0 AWS](#)
- [Esempio di ricerca per Center for Internet Security \(CIS\) Foundations Benchmark v1.4.0 AWS](#)
- [Esempio di ricerca per Center for Internet Security \(CIS\) Foundations Benchmark v3.0.0 AWS](#)
- [Esempio di risultato per il National Institute of Standards and Technology \(NIST\) SP 800-53 Rev. 5](#)
- [Esempio di risultato relativo allo standard PCI DSS \(Payment Card Industry Data Security Standard\)](#)
- [Esempio di risultato per AWS Resource Tagging Standard](#)
- [Esempi di risultati per Service-Managed Standard: AWS Control Tower](#)

I risultati del controllo consolidato sono attivati

- [Ricerca di campioni in tutti gli standard](#)

Esempi di risultati per FSBP

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
Foundational-Security-Best-Practices"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.076Z",
  "LastObservedAt": "2021-09-28T16:10:06.956Z",
  "CreatedAt": "2020-08-06T02:18:23.076Z",
  "UpdatedAt": "2021-09-28T16:10:00.093Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use
the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master
key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security
Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub::standards/aws-foundational-security-best-
practices/v/1.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/aws-foundational-security-best-practices/v/1.0.0",
    "ControlId": "CloudTrail.2",

```

```

    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
    "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
    "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-
foundational-security-best-practices/v/1.0.0/CloudTrail.2",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/aws-foundational-
security-best-practices/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-
EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "standards/aws-foundation-best-practices/v/1.0.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    }
  },
  "Types": [

```

```

    "Software and Configuration Checks/Industry and Regulatory Standards/AWS-
    Foundational-Security-Best-Practices"
  ]
}
}

```

Risultati di esempio per CIS Foundations Benchmark v3.0.0 AWS

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
  benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
    Foundations Benchmark"
  ],
  "FirstObservedAt": "2024-04-18T07:46:18.193Z",
  "LastObservedAt": "2024-04-23T07:47:01.137Z",
  "CreatedAt": "2024-04-18T07:46:18.193Z",
  "UpdatedAt": "2024-04-23T07:46:46.165Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "2.2.1 EBS default encryption should be enabled",
  "Description": "Elastic Compute Cloud (EC2) supports encryption at rest when using
  the Elastic Block Store (EBS) service. While disabled by default, forcing encryption
  at EBS volume creation is supported.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security
      Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation"
    }
  }
}

```

```
  },
  "ProductFields": {
    "StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/v/3.0.0",
    "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0",
    "ControlId": "2.2.1",
    "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/EC2.7/remediation",
    "RelatedAWSResources:0/name": "securityhub-ec2-ebs-encryption-by-default-2843ed9e",
    "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
    "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-foundations-benchmark/v/3.0.0/2.2.1",
    "aws/securityhub/ProductName": "Security Hub",
    "aws/securityhub/CompanyName": "AWS",
    "aws/securityhub/annotation": "EBS Encryption by default is not enabled.",
    "Resources:0/Id": "arn:aws:iam::123456789012:root",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/3.0.0/2.2.1/finding/38a89798-6819-4fae-861f-9cca8034602c"
  },
  "Resources": [
    {
      "Type": "AwsAccount",
      "Id": "AWS:::Account:123456789012",
      "Partition": "aws",
      "Region": "us-east-1"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "RelatedRequirements": [
      "CIS AWS Foundations Benchmark v3.0.0/2.2.1"
    ],
    "SecurityControlId": "EC2.7",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/cis-aws-foundations-benchmark/v/3.0.0"
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  }
}
```

```

},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
},
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
]
},
"ProcessedAt": "2024-04-23T07:47:07.088Z"
}

```

Risultati di esempio per CIS Foundations Benchmark v1.4.0 AWS

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "cis-aws-foundations-benchmark/v/1.4.0/3.7",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
  ],
  "FirstObservedAt": "2022-10-21T22:14:48.913Z",
  "LastObservedAt": "2022-12-22T22:24:56.980Z",
  "CreatedAt": "2022-10-21T22:14:48.913Z",
  "UpdatedAt": "2022-12-22T22:24:52.409Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "3.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
}

```



```

"Description": "AWS CloudTrail is a web service that records AWS API calls for an
account and makes those logs available to users and resources in accordance with IAM
policies. AWS Key Management Service (KMS) is a managed service that helps create
and control the encryption keys used to encrypt account data, and uses Hardware
Security Modules (HSMs) to protect the security of encryption keys. CloudTrail logs
can be configured to leverage server side encryption (SSE) and AWS KMS customer
created master keys (CMK) to further protect CloudTrail logs. It is recommended that
CloudTrail be configured to use SSE-KMS.",
"Remediation": {
  "Recommendation": {
    "Text": "For directions on how to correct this issue, consult the AWS Security
Hub controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/cis-aws-foundations-benchmark/
v/1.4.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-1:123456789012:subscription/cis-aws-foundations-benchmark/v/1.4.0",
  "ControlId": "3.7",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-
enabled-855f82d1",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/cis-aws-
foundations-benchmark/v/1.4.0/3.7",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.4.0/3.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [
  {
    "Type": "AwsCloudTrailTrail",
    "Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
    "Partition": "aws",
    "Region": "us-east-1"
  }
]

```

```

],
"Compliance": {
  "Status": "FAILED",
  "RelatedRequirements": [
    "CIS AWS Foundations Benchmark v1.4.0/3.7"
  ],
  "SecurityControlId": "CloudTrail.2",
  "AssociatedStandards": [{
    "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"
  }]
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
  ]
}
}

```

Risultati di esempio per CIS Foundations Benchmark v1.2.0 AWS

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-foundations-
benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "arn:aws:securityhub::ruleset/cis-aws-foundations-benchmark/v/1.2.0/
rule/2.7",
  "AwsAccountId": "123456789012",
  "Types": [

```

```

"Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
],
"FirstObservedAt": "2020-08-29T04:10:06.337Z",
"LastObservedAt": "2021-09-28T16:10:05.350Z",
"CreatedAt": "2020-08-29T04:10:06.337Z",
"UpdatedAt": "2021-09-28T16:10:00.087Z",
"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "2.7 Ensure CloudTrail logs are encrypted at rest using KMS CMKs",
"Description": "AWS Key Management Service (KMS) is a managed service that helps
create and control the encryption keys used to encrypt account data, and uses Hardware
Security Modules (HSMs) to protect the security of encryption keys. CloudTrail
logs can be configured to leverage server side encryption (SSE) and KMS customer
created master keys (CMK) to further protect CloudTrail logs. It is recommended that
CloudTrail be configured to use SSE-KMS.",
"Remediation": {
  "Recommendation": {
    "Text": "For directions on how to correct this issue, consult the AWS Security
Hub controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsGuideArn": "arn:aws:securityhub:::ruleset/cis-aws-foundations-benchmark/
v/1.2.0",
  "StandardsGuideSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/cis-aws-foundations-benchmark/v/1.2.0",
  "RuleId": "2.7",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
  "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
  "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/cis-aws-
foundations-benchmark/v/1.2.0/2.7",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",

```

```

    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/cis-aws-
foundations-benchmark/v/1.2.0/2.7/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
  },
  "Resources": [
    {
      "Type": "AwsCloudTrailTrail",
      "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
      "Partition": "aws",
      "Region": "us-east-2"
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "CloudTrail.2",
    "AssociatedStandards": [{
      "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"
    }]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM",
      "Original": "MEDIUM"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards/CIS AWS
Foundations Benchmark"
    ]
  }
}

```

Esempio di risultato per NIST SP 800-53 Rev. 5

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/
CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",

```

```

"ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
"ProductName": "Security Hub",
"CompanyName": "AWS",
"Region": "us-east-1",
"GeneratorId": "nist-800-53/v/5.0.0/CloudTrail.2",
"AwsAccountId": "123456789012",
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards"
],
"FirstObservedAt": "2023-02-17T14:22:46.726Z",
"LastObservedAt": "2023-02-17T14:22:50.846Z",
"CreatedAt": "2023-02-17T14:22:46.726Z",
"UpdatedAt": "2023-02-17T14:22:46.726Z",
"Severity": {
  "Product": 40,
  "Label": "MEDIUM",
  "Normalized": 40,
  "Original": "MEDIUM"
},
"Title": "CloudTrail.2 CloudTrail should have encryption at-rest enabled",
"Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
"Remediation": {
  "Recommendation": {
    "Text": "For directions on how to fix this issue, consult the AWS Security Hub NIST 800-53 R5 documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/nist-800-53/v/5.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0",
  "ControlId": "CloudTrail.2",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.9/remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-fe95bf3f",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/aws-foundational-security-best-practices/v/1.0.0/CloudTrail.2",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",

```

```
"Resources:0/Id": "arn:aws:cloudtrail:us-west-2:123456789012:trail/AWS MacieTrail-DO-NOT-EDIT",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/nist-800-53/v/5.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [
  {
    "Type": "AwsCloudTrailTrail",

    "Id": "arn:aws:cloudtrail:us-east-1:123456789012:trail/AWS MacieTrail-DO-NOT-EDIT",

    "Partition": "aws",

    "Region": "us-east-1"
  }
],
"Compliance": {
  "Status": "FAILED",
  "RelatedRequirements": [
    "NIST.800-53.r5 AU-9",
    "NIST.800-53.r5 CA-9(1)",
    "NIST.800-53.r5 CM-3(6)",
    "NIST.800-53.r5 SC-13",
    "NIST.800-53.r5 SC-28",
    "NIST.800-53.r5 SC-28(1)",
    "NIST.800-53.r5 SC-7(10)",
    "NIST.800-53.r5 SI-7(6)"
  ],
  "SecurityControlId": "CloudTrail.2",
  "AssociatedStandards": [
    {
      "StandardsId": "standards/nist-800-53/v/5.0.0"
    }
  ]
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
```

```

    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ]
},
"ProcessedAt": "2023-02-17T14:22:53.572Z"
}

```

Esempio di ricerca per PCI DSS

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "pci-dss/v/3.2.1/PCI.CloudTrail.1",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ],
  "FirstObservedAt": "2020-08-06T02:18:23.089Z",
  "LastObservedAt": "2021-09-28T16:10:06.942Z",
  "CreatedAt": "2020-08-06T02:18:23.089Z",
  "UpdatedAt": "2021-09-28T16:10:00.090Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "PCI.CloudTrail.1 CloudTrail logs should be encrypted at rest using AWS KMS CMKs",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption by checking if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {

```

```

    "Text": "For directions on how to correct this issue, consult the AWS Security
Hub controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
  }
},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/pci-dss/v/3.2.1",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-
east-2:123456789012:subscription/pci-dss/v/3.2.1",
  "ControlId": "PCI.CloudTrail.1",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/
remediation",
  "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
  "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-2:123456789012:control/pci-dss/
v/3.2.1/PCI.CloudTrail.1",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:subscription/pci-dss/v/3.2.1/
PCI.CloudTrail.1/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [
  {
    "Type": "AwsCloudTrailTrail",
    "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
    "Partition": "aws",
    "Region": "us-east-2"
  }
],
"Compliance": {
  "Status": "FAILED",
  "RelatedRequirements": [
    "PCI DSS 3.4"
  ],
  "SecurityControlId": "CloudTrail.2",
  "AssociatedStandards": [{
    "StandardsId": "standards/pci-dss/v/3.2.1"
  }]
},

```



```

"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {
    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards/PCI-DSS"
  ]
}
}

```

Esempio di ricerca per AWS Resource Tagging Standard

```


{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:eu-central-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "eu-central-1",
  "GeneratorId": "security-control/EC2.44",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2024-02-19T21:00:32.206Z",
  "LastObservedAt": "2024-04-29T13:01:57.861Z",
  "CreatedAt": "2024-02-19T21:00:32.206Z",
  "UpdatedAt": "2024-04-29T13:01:41.242Z",
  "Severity": {
    "Label": "LOW",
    "Normalized": 1,
    "Original": "LOW"
  },
  "Title": "EC2 subnets should be tagged",
  "Description": "This control checks whether an Amazon EC2 subnet has tags with the specific keys defined in the parameter requiredTagKeys. The control fails if the

```

```
subnet doesn't have any tag keys or if it doesn't have all the keys specified in
the parameter requiredTagKeys. If the parameter requiredTagKeys isn't provided, the
control only checks for the existence of a tag key and fails if the subnet isn't
tagged with any key. System tags, which are automatically applied and begin with aws:,
are ignored.",
"Remediation": {
  "Recommendation": {
    "Text": "For information on how to correct this issue, consult the AWS Security
Hub controls documentation.",
    "Url": "https://docs.aws.amazon.com/console/securityhub/EC2.44/remediation"
  }
},
"ProductFields": {
  "RelatedAWSResources:0/name": "securityhub-tagged-ec2-subnet-6ceafede",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",
  "aws/securityhub/annotation": "No tags are present.",
  "Resources:0/Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
  "aws/securityhub/FindingId": "arn:aws:securityhub:eu-central-1::product/aws/
securityhub/arn:aws:securityhub:eu-central-1:123456789012:security-control/EC2.44/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [
{
  "Type": "AwsEc2Subnet",
  "Id": "arn:aws:ec2:eu-central-1:123456789012:subnet/subnet-1234567890abcdef0",
  "Partition": "aws",
  "Region": "eu-central-1",
  "Details": {
    "AwsEc2Subnet": {
      "AssignIpv6AddressOnCreation": false,
      "AvailabilityZone": "eu-central-1b",
      "AvailabilityZoneId": "euc1-az3",
      "AvailableIpAddressCount": 4091,
      "CidrBlock": "10.24.34.0/23",
      "DefaultForAz": true,
      "MapPublicIpOnLaunch": true,
      "OwnerId": "123456789012",
      "State": "available",
      "SubnetArn": "arn:aws:ec2:eu-central-1:123456789012:subnet/
subnet-1234567890abcdef0",
      "SubnetId": "subnet-1234567890abcdef0",
```

```
        "VpcId": "vpc-021345abcdef6789"
      }
    }
  ],
  "Compliance": {
    "Status": "FAILED",
    "SecurityControlId": "EC2.44",
    "AssociatedStandards": [
      {
        "StandardsId": "standards/aws-resource-tagging-standard/v/1.0.0"
      }
    ],
    "SecurityControlParameters": [
      {
        "Name": "requiredTagKeys",
        "Value": [
          "peepoo"
        ]
      }
    ]
  },
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "LOW",
      "Original": "LOW"
    },
    "Types": [
      "Software and Configuration Checks/Industry and Regulatory Standards"
    ]
  },
  "ProcessedAt": "2024-04-29T13:02:03.259Z"
}
```

Esempi di risultati per Service-Managed Standard: AWS Control Tower

 Note

Questo standard è disponibile solo se sei un AWS Control Tower utente che lo ha creato in. AWS Control Tower Per ulteriori informazioni, consulta [Standard di gestione dei servizi: AWS Control Tower](#).

```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-11-17T01:25:30.296Z",
  "LastObservedAt": "2022-11-17T01:25:45.805Z",
  "CreatedAt": "2022-11-17T01:25:30.296Z",
  "UpdatedAt": "2022-11-17T01:25:30.296Z",
  "Severity": {
    "Product": 40,
    "Label": "MEDIUM",
    "Normalized": 40,
    "Original": "MEDIUM"
  },
  "Title": "CT.CloudTrail.2 CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For information on how to correct this issue, consult the AWS Security Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  }
}
```

```

},
"ProductFields": {
  "StandardsArn": "arn:aws:securityhub::standards/service-managed-aws-control-tower/v/1.0.0",
  "StandardsSubscriptionArn": "arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0",
  "ControlId": "CT.CloudTrail.2",
  "RecommendationUrl": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation",
  "RelatedAWSResources:0/name": "securityhub-cloud-trail-encryption-enabled-fe95bf3f",
  "RelatedAWSResources:0/type": "AWS::Config::ConfigRule",
  "StandardsControlArn": "arn:aws:securityhub:us-east-1:123456789012:control/service-managed-aws-control-tower/v/1.0.0/CloudTrail.2",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWSMacieTrail-DO-NOT-EDIT",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/securityhub/arn:aws:securityhub:us-east-1:123456789012:subscription/service-managed-aws-control-tower/v/1.0.0/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
},
"Resources": [
  {
    "Type": "AwsAccount",
    "Id": "AWS:::Account:123456789012",
    "Partition": "aws",
    "Region": "us-east-1"
  }
],
"Compliance": {
  "Status": "FAILED",
  "SecurityControlId": "CloudTrail.2",
  "AssociatedStandards": [{
    "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"
  }]
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
  "Severity": {

```

```

    "Label": "MEDIUM",
    "Original": "MEDIUM"
  },
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ]
}
}

```

Ricerca di esempi tra gli standard (quando i risultati del controllo consolidato sono attivati)

```

{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111",
  "ProductArn": "arn:aws:securityhub:us-east-2::product/aws/securityhub",
  "ProductName": "Security Hub",
  "CompanyName": "AWS",
  "Region": "us-east-2",
  "GeneratorId": "security-control/CloudTrail.2",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Industry and Regulatory Standards"
  ],
  "FirstObservedAt": "2022-10-06T02:18:23.076Z",
  "LastObservedAt": "2022-10-28T16:10:06.956Z",
  "CreatedAt": "2022-10-06T02:18:23.076Z",
  "UpdatedAt": "2022-10-28T16:10:00.093Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": "40",
    "Original": "MEDIUM"
  },
  "Title": "CloudTrail should have encryption at-rest enabled",
  "Description": "This AWS control checks whether AWS CloudTrail is configured to use the server side encryption (SSE) AWS Key Management Service (AWS KMS) customer master key (CMK) encryption. The check will pass if the KmsKeyId is defined.",
  "Remediation": {
    "Recommendation": {
      "Text": "For directions on how to correct this issue, consult the AWS Security Hub controls documentation.",
      "Url": "https://docs.aws.amazon.com/console/securityhub/CloudTrail.2/remediation"
    }
  }
}

```

```
},
"ProductFields": {
  "Related AWS Resources:0/name": "securityhub-cloud-trail-encryption-enabled-
fe95bf3f",
  "Related AWS Resources:0/type": "AWS::Config::ConfigRule",
  "aws/securityhub/ProductName": "Security Hub",
  "aws/securityhub/CompanyName": "AWS",
  "Resources:0/Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-
DO-NOT-EDIT",
  "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-2::product/aws/
securityhub/arn:aws:securityhub:us-east-2:123456789012:security-control/CloudTrail.2/
finding/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111"
}
"Resources": [
  {
    "Type": "AwsCloudTrailTrail",
    "Id": "arn:aws:cloudtrail:us-east-2:123456789012:trail/AWS MacieTrail-DO-NOT-
EDIT",
    "Partition": "aws",
    "Region": "us-east-2"
  }
],
"Compliance": {
  "Status": "FAILED",
  "RelatedRequirements": [
    "PCI DSS v3.2.1/3.4",
    "CIS AWS Foundations Benchmark v1.2.0/2.7",
    "CIS AWS Foundations Benchmark v1.4.0/3.7"
  ],
  "SecurityControlId": "CloudTrail.2",
  "AssociatedStandards": [
    { "StandardsId": "standards/aws-foundational-security-best-practices/v/1.0.0"},
    { "StandardsId": "standards/pci-dss/v/3.2.1"},
    { "StandardsId": "ruleset/cis-aws-foundations-benchmark/v/1.2.0"},
    { "StandardsId": "standards/cis-aws-foundations-benchmark/v/1.4.0"},
    { "StandardsId": "standards/service-managed-aws-control-tower/v/1.0.0"},
  ]
},
"WorkflowState": "NEW",
"Workflow": {
  "Status": "NEW"
},
"RecordState": "ACTIVE",
"FindingProviderFields": {
```

```
"Severity": {
  "Label": "MEDIUM",
  "Original": "MEDIUM"
},
"Types": [
  "Software and Configuration Checks/Industry and Regulatory Standards"
]
}
}
```

Filtraggio, ordinamento e download dei risultati di controllo

È possibile filtrare l'elenco dei risultati del controllo in base allo stato di conformità utilizzando le schede di filtro. Puoi anche filtrare l'elenco in base ad altri valori dei campi di ricerca e scaricare i risultati dall'elenco.

Filtraggio e ordinamento dell'elenco dei controlli

La scheda Tutti i controlli elenca tutti i risultati attivi con uno stato del flusso di lavoro pari a NEWNOTIFIED, o. RESOLVED Per impostazione predefinita, l'elenco è ordinato in modo che i risultati non riusciti siano in cima all'elenco. Questo ordinamento consente di dare priorità ai risultati che devono essere risolti.

Gli elenchi nelle schede Failed, Unknown e Passed vengono filtrati in base al valore di Compliance.Status Gli elenchi includono inoltre solo i risultati attivi con uno stato del flusso di lavoro pari a NEWNOTIFIED, o. RESOLVED

La scheda Eliminati contiene un elenco di risultati attivi con uno stato del flusso di lavoro pari a SUPPRESSED

Oltre ai filtri integrati in ogni scheda, puoi filtrare gli elenchi utilizzando i valori dei seguenti campi:

- ID account
- Stato del flusso di lavoro
- Compliance status (Stato di conformità)
- ID risorsa
- Tipo di risorsa

È possibile ordinare ogni elenco utilizzando una qualsiasi delle colonne.

Scaricamento dell'elenco dei risultati dei controlli

Se si accede a Standard di sicurezza e si sceglie uno standard, viene visualizzato un elenco di controlli per lo standard. Scegliendo un controllo dall'elenco si accede alla pagina dei dettagli del controllo con un elenco di risultati relativi al controllo. Da qui, è possibile scaricare i risultati del controllo in un file.csv.

Se filtri l'elenco dei risultati, il download include solo i controlli che corrispondono al filtro.

Se si selezionano risultati specifici dall'elenco, il download include solo i risultati selezionati.

Per scaricare i risultati, scegli Scarica. La pagina corrente dei risultati viene scaricata.

Intervenire in base ai risultati del controllo

Per riflettere lo stato attuale della tua indagine, imposti lo stato del flusso di lavoro. Per ulteriori informazioni, consulta [the section called "Impostazione dello stato dei risultati del flusso di lavoro"](#).

Nel AWS Security Hub, puoi anche inviare risultati selezionati a un'azione personalizzata in Amazon EventBridge. Per ulteriori informazioni, consulta [the section called "Invio dei risultati a un'operazione personalizzata"](#).

Utilizzo del pannello di controllo Riepilogo

Sulla console AWS Security Hub, la dashboard nella pagina Riepilogo può aiutarti a identificare le aree di problema di sicurezza nel tuo AWS ambiente, senza la necessità di strumenti di analisi aggiuntivi o query complesse. È possibile personalizzare il layout della dashboard, aggiungere o rimuovere widget e filtrare i dati per concentrarsi sulle aree di particolare interesse. Puoi anche salvare i criteri di filtro come set di filtri per recuperare rapidamente tipi di dati specifici in futuro.

Se personalizzi la dashboard o filtri i dati, Security Hub salva automaticamente le impostazioni per un uso successivo. Inoltre, le impostazioni vengono salvate indipendentemente per ogni utente del tuo account Security Hub. Ciò significa che utenti diversi possono avere layout, widget e set di filtri diversi per la dashboard.

Ogni volta che apri la dashboard di riepilogo, Security Hub aggiorna automaticamente la maggior parte dei dati del dashboard. Tuttavia, alcuni dati vengono aggiornati meno frequentemente. Ad esempio, i punteggi di sicurezza e gli stati di controllo vengono aggiornati ogni 24 ore.

Se hai configurato una regione di aggregazione interregionale per Security Hub, i dati del dashboard includono i risultati della regione di aggregazione e di tutte le regioni collegate. Se sei l'amministratore delegato del Security Hub di un'organizzazione, i dati includono i risultati relativi al tuo account amministratore e agli account dei membri. Facoltativamente, puoi filtrare i dati per account. Se hai un account membro o un account autonomo, i dati includono i risultati solo per il tuo account.

Widget disponibili per la dashboard di riepilogo

La dashboard di riepilogo include widget che riflettono il moderno panorama delle minacce alla sicurezza del cloud, guidati dalle operazioni e dalle esperienze di sicurezza dei AWS clienti. Alcuni widget vengono visualizzati per impostazione predefinita, mentre altri no. Puoi personalizzare la visualizzazione della dashboard aggiungendo o rimuovendo i widget.

Per aggiungerli, scegli **Aggiungi widget** in alto a destra nella pagina di riepilogo. Nella barra di ricerca, inserisci il titolo del widget. Trascina e rilascia il widget sulla dashboard.

I widget sono mostrati per impostazione predefinita

Per impostazione predefinita, la dashboard Riepilogo include i seguenti widget:

Standard di sicurezza

Visualizza il punteggio di sicurezza riepilogativo più recente e il punteggio di sicurezza per ogni standard di Security Hub. I punteggi di sicurezza, che vanno dallo 0 al 100 per cento, rappresentano la percentuale di controlli superati rispetto a tutti i controlli abilitati. Per ulteriori informazioni su questi punteggi, vedere. [Come vengono calcolati i punteggi di sicurezza](#) Questo widget ti aiuta a comprendere la tua posizione generale in materia di sicurezza.

Risorse con il maggior numero di risultati

Fornisce una panoramica delle risorse, degli account e delle applicazioni con il maggior numero di risultati. L'elenco è ordinato in ordine decrescente in base al numero di risultati. Nel widget, ogni scheda mostra i primi sei elementi di quella categoria, raggruppati per gravità e tipo di risorsa. Se scegli un numero nella colonna Risultati totali, Security Hub apre una pagina che mostra i risultati per l'asset. Questo widget ti aiuta a identificare rapidamente quali delle tue risorse principali presentano potenziali minacce alla sicurezza.

Risultati per regione

Mostra il numero totale di risultati, raggruppati per gravità, Regione AWS in ognuno dei quali Security Hub è abilitato. Questo widget ti aiuta a identificare i problemi di sicurezza che potenzialmente interessano regioni particolari. Se apri la dashboard nella tua regione di aggregazione, questo widget ti aiuta a monitorare potenziali problemi di sicurezza in ogni regione collegata.

I tipi di minacce più comuni

Fornisce un'analisi dettagliata dei 10 tipi di minacce più comuni nell'AWSambiente in uso. Ciò include minacce come l'aumento dei privilegi, l'uso di credenziali esposte o la comunicazione con indirizzi IP dannosi.

Per visualizzare questi dati, [Amazon GuardDuty](#) deve essere abilitato. In caso affermativo, scegli un tipo di minaccia in questo widget per aprire la GuardDuty console ed esaminare i risultati relativi a questa minaccia. Questo widget consente di valutare le potenziali minacce nel contesto di altri problemi di sicurezza.

Vulnerabilità del software con exploit

Fornisce un riepilogo delle vulnerabilità software presenti nell'AWSambiente in uso e che presentano exploit noti. Puoi anche esaminare un'analisi dettagliata delle vulnerabilità per cui sono disponibili e non sono disponibili correzioni.

Per visualizzare questi dati, è necessario [abilitare Amazon Inspector](#). In tal caso, scegli una statistica in questo widget per aprire la console Amazon Inspector e visualizzare ulteriori dettagli sulla vulnerabilità. Questo widget ti aiuta a valutare le vulnerabilità del software nel contesto di altri problemi di sicurezza.

Nuove scoperte nel tempo

Mostra l'andamento del numero di nuovi risultati giornalieri negli ultimi 90 giorni. Puoi suddividere i dati per gravità o per fornitore per un contesto aggiuntivo. Questo widget ti aiuta a capire se il volume di ricerca è aumentato o diminuito in momenti specifici negli ultimi 90 giorni.

Risorse con il maggior numero di risultati

Fornisce un riepilogo delle risorse che hanno generato il maggior numero di risultati, suddivise per i seguenti tipi di risorse: bucket Amazon Simple Storage Service (Amazon S3), istanze Amazon Elastic Compute Cloud (Amazon EC2) e funzioni. AWS Lambda

Nel widget, ogni scheda si concentra su uno dei tipi di risorse precedenti, elencando le 10 istanze di risorse che hanno generato il maggior numero di risultati. Per esaminare i risultati di una risorsa specifica, scegli l'istanza della risorsa. Questo widget ti aiuta a valutare i risultati di sicurezza associati a AWS risorse comuni.

Widget nascosti per impostazione predefinita

I seguenti widget sono disponibili anche per la dashboard Riepilogo, ma sono nascosti per impostazione predefinita:

AMI con il maggior numero di risultati

Fornisce un elenco delle 10 Amazon Machine Images (AMI) che hanno generato il maggior numero di risultati. Questi dati sono disponibili solo se Amazon EC2 è abilitato per il tuo account. Ti aiuta a identificare quali AMI rappresentano potenziali rischi per la sicurezza.

Principali IAM con il maggior numero di risultati

Fornisce un elenco dei 10 utenti AWS Identity and Access Management (IAM) che hanno generato il maggior numero di risultati. Questo widget consente di eseguire attività amministrative e di fatturazione. Mostra quali utenti contribuiscono maggiormente all'utilizzo del Security Hub.

Account con il maggior numero di risultati (per gravità)

Mostra un grafico dei 10 account che hanno generato il maggior numero di risultati, raggruppati per gravità. Questo widget ti aiuta a determinare su quali account concentrare le attività di analisi e correzione.

Account con il maggior numero di risultati (per tipo di risorsa)

Mostra un grafico dei 10 account che hanno generato il maggior numero di risultati, raggruppati per tipo di risorsa. Questo widget consente di determinare a quali account e tipi di risorse dare priorità per l'analisi e la correzione.

Approfondimenti

Elenca cinque [approfondimenti gestiti da Security Hub](#) e il numero di risultati che hanno generato. Insights identifica un'area di sicurezza specifica che richiede attenzione.

I risultati più recenti delle AWS integrazioni

Mostra il numero di risultati ricevuti in Security Hub da [integrated Servizi AWS](#). Mostra anche quando hai ricevuto più di recente i risultati di ciascun servizio integrato. Questo widget fornisce dati consolidati sui risultati provenienti da più Servizi AWS fonti. Per approfondire, scegli un servizio integrato. Security Hub apre quindi la console per quel servizio.

Filtraggio della dashboard di riepilogo

Per curare i dati nella dashboard di riepilogo e includere solo i dati di sicurezza più pertinenti per te, puoi filtrare la dashboard. Ad esempio, se fai parte di un team applicativo, potresti creare una visualizzazione dedicata per un'applicazione critica nel tuo ambiente di produzione. Se fai parte di un team di sicurezza, potresti creare una visualizzazione dedicata che ti aiuti a concentrarti sui risultati ad alta gravità. Per filtrare i dati nella dashboard di riepilogo, inserisci i criteri di filtro nella casella del filtro sopra la dashboard. Se applichi criteri di filtro, i criteri si applicano a tutti i dati sulla dashboard ad eccezione dei dati nei widget degli standard di Insights e Security.

È possibile filtrare i dati utilizzando i seguenti campi:

- Account name (Nome account)
- ID account
- Amazon Resource Name (ARN) dell'applicazione
- Nome applicazione

- Nome del prodotto (per un prodotto Servizio AWS o un prodotto di terze parti che invia i risultati a Security Hub)
- Record state (Stato del record)
- Region
- Tag risorsa
- Gravità
- Stato del flusso di lavoro

Per impostazione predefinita, i dati del dashboard vengono filtrati in base ai seguenti criteri: `Workflow status` è `NOTIFIED` o `NEW` ed `Record state` è `ACTIVE`. Questi criteri vengono visualizzati sopra la dashboard, sotto la casella del filtro. Per rimuovere questi criteri, scegli X nel token di filtro relativo ai criteri che desideri rimuovere.

Se applichi criteri di filtro che desideri utilizzare nuovamente, puoi salvarli come set di filtri. Un set di filtri è un insieme di criteri di filtro che crei e salvi per riapplicare quando esaminate i dati nella dashboard di riepilogo.

Note

I seguenti campi non possono essere salvati come parte di un set di filtri: ARN dell'applicazione, nome dell'applicazione e tag di risorsa.

Creazione e salvataggio di set di filtri

Segui questi passaggi per creare e salvare un set di filtri.

Per creare e salvare un set di filtri

1. Aprire la console AWS Security Hub all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, scegli Riepilogo.
3. Nella casella del filtro sopra la dashboard di riepilogo, inserisci i criteri di filtro per il set di filtri.
4. Nel menu Cancella filtri, scegli Salva nuovo set di filtri.
5. Nella finestra di dialogo Salva set di filtri, inserite un nome per il set di filtri.
6. (Facoltativo) Per utilizzare il filtro impostato di default ogni volta che aprite la pagina di riepilogo, selezionate l'opzione per impostarlo come visualizzazione predefinita.

7. Selezionare Salva.

Per passare da un set di filtri che hai creato a uno salvato, utilizza il menu Scegli un set di filtri sopra la dashboard di riepilogo. Quando si seleziona un set di filtri, Security Hub applica i criteri del set di filtri ai dati sulla dashboard.

Aggiornamento o eliminazione dei set di filtri

Segui questi passaggi per aggiornare o eliminare un set di filtri esistente. Se si elimina un set di filtri attualmente impostato come visualizzazione predefinita della dashboard di riepilogo, la visualizzazione predefinita viene ripristinata sulla visualizzazione predefinita di Security Hub.

Per aggiornare o eliminare un set di filtri

1. Aprire la console AWS Security Hub all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, scegli Riepilogo.
3. Nel menu Scegli un set di filtri sopra la pagina di riepilogo, scegli il set di filtri.
4. Nel menu Cancella filtri, effettuate una delle seguenti operazioni:
 - Per aggiornare il set di filtri, scegliete Aggiorna il set di filtri corrente. Quindi, inserisci le modifiche nella finestra di dialogo che appare.
 - Per eliminare il set di filtri, scegliete Elimina il set di filtri corrente. Quindi, scegliete Elimina nella finestra di dialogo che appare.

Personalizzazione della dashboard di riepilogo

È possibile personalizzare la dashboard di riepilogo in diversi modi. Puoi aggiungere e rimuovere widget dalla dashboard. Puoi anche riorganizzare e ridimensionare i widget sulla dashboard.

Se personalizzi la dashboard, Security Hub applica immediatamente le modifiche e salva le nuove impostazioni della dashboard. Le modifiche si applicano alla visualizzazione della dashboard in tutti Regioni AWS i browser.

Per personalizzare la dashboard di riepilogo

1. Aprire la console AWS Security Hub all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, scegli Riepilogo.

3. Effettuare una delle seguenti operazioni:

- Per aggiungere un widget, scegli **Aggiungi widget** nell'angolo in alto a destra della pagina. Nella barra di ricerca, inserisci il titolo del widget da aggiungere. Quindi, trascina il widget nella posizione desiderata.
- Per rimuovere un widget, scegli i tre punti nell'angolo in alto a destra del widget.
- Per spostare un widget, scegli la maniglia nell'angolo superiore sinistro del widget, quindi trascina il widget nella posizione desiderata.
- Per modificare le dimensioni di un widget, scegli la maniglia di ridimensionamento nell'angolo inferiore destro del widget. Trascina il bordo del widget fino a raggiungere la dimensione desiderata.

Per ripristinare successivamente le impostazioni originali, scegli **Ripristina il layout predefinito** nella parte superiore della pagina.

Creazione di risorse Security Hub con AWS CloudFormation

AWS Security Hub si integra con AWS CloudFormation, un servizio che consente di modellare e configurare le AWS risorse in modo da dedicare meno tempo alla creazione e alla gestione delle risorse e dell'infrastruttura. Crei un modello che descrive tutte le AWS risorse che desideri (come le regole di automazione) e fornisce e AWS CloudFormation configura tali risorse per te.

Quando lo usi AWS CloudFormation, puoi riutilizzare il modello per configurare le risorse del Security Hub in modo coerente e ripetuto. Descrivi le tue risorse una sola volta, quindi fornisci le stesse risorse più e più volte in più Account AWS regioni.

Security Hub e AWS CloudFormation modelli

Per fornire e configurare le risorse per Security Hub e i servizi correlati, è necessario comprendere come funzionano [AWS CloudFormation i modelli](#). I modelli sono file di testo in formato JSON o YAML. Questi modelli descrivono le risorse che desideri inserire negli stack. AWS CloudFormation

Se non conosci JSON o YAML, puoi usare AWS CloudFormation Designer per iniziare a usare i modelli. AWS CloudFormation [Per ulteriori informazioni, consulta Cos'è Designer? AWS CloudFormation](#) nella Guida AWS CloudFormation per l'utente.

È possibile creare AWS CloudFormation modelli per i seguenti tipi di risorse del Security Hub:

- Abilitazione del Security Hub
- Designazione dell'amministratore delegato del Security Hub per un'organizzazione
- Abilitazione di uno standard di sicurezza
- Creazione di una visione personalizzata
- Creazione di una regola di automazione
- Abbonamento a un'integrazione di prodotti di terze parti

Per ulteriori informazioni, inclusi esempi di modelli JSON e YAML per le risorse, consulta il [riferimento ai tipi di risorse nella AWS Security Hub Guida](#) per l'utente. AWS CloudFormation

Scopri di più su AWS CloudFormation

Per ulteriori informazioni AWS CloudFormation, consulta le seguenti risorse:

- [AWS CloudFormation](#)
- [AWS CloudFormation Guida per l'utente](#)
- [AWS CloudFormation Documentazione di riferimento delle API](#)
- [AWS CloudFormation Guida per l'utente dell'interfaccia a riga di comando](#)

Iscrizione agli annunci di Security Hub con Amazon Simple Notification Service

Questa sezione fornisce informazioni sulla sottoscrizione agli annunci di AWS Security Hub con Amazon Simple Notification Service (Amazon SNS) per ricevere notifiche su Security Hub.

Dopo l'iscrizione, riceverai notifiche sui seguenti eventi (nota il corrispondente `AnnouncementType` per ogni evento):

- `GENERAL`— Notifiche generali sul servizio Security Hub.
- `UPCOMING_STANDARDS_CONTROLS`— I controlli o gli standard specifici del Security Hub verranno rilasciati a breve. Questo tipo di annuncio consente di preparare i flussi di lavoro di risposta e correzione prima del rilascio.
- `NEW_REGIONS`— Il supporto per Security Hub è disponibile in una nuova versione Regione AWS.
- `NEW_STANDARDS_CONTROLS`— Sono stati aggiunti nuovi controlli o standard del Security Hub.
- `UPDATED_STANDARDS_CONTROLS`— I controlli o gli standard esistenti del Security Hub sono stati aggiornati.
- `RETIRED_STANDARDS_CONTROLS`— I controlli o gli standard esistenti del Security Hub sono stati ritirati.
- `UPDATED_ASFF`— La sintassi, i campi o i valori del AWS Security Finding Format (ASFF) sono stati aggiornati.
- `NEW_INTEGRATION`— Sono disponibili nuove integrazioni con altri AWS servizi o prodotti di terze parti.
- `NEW_FEATURE`— Sono disponibili nuove funzionalità del Security Hub.
- `UPDATED_FEATURE`— Le funzionalità esistenti di Security Hub sono state aggiornate.

Le notifiche sono disponibili in tutti i formati supportati da Amazon SNS. Puoi iscriverti agli annunci di Security Hub in tutte le versioni in [Regioni AWS cui Security Hub è disponibile](#).

Un utente deve disporre `Subscribe` delle autorizzazioni per iscriversi a un argomento di Amazon SNS. Puoi raggiungere questo obiettivo con le policy di Amazon SNS, le policy IAM o entrambe. Per ulteriori informazioni, consulta le [politiche di IAM e Amazon SNS insieme nella Amazon Simple Notification Service Developer Guide](#).

Note

Security Hub invia annunci Amazon SNS sugli aggiornamenti del servizio Security Hub a tutti gli abbonati. Account AWS Per ricevere notifiche sui risultati del Security Hub, vedere [Gestione e revisione dei dettagli e della cronologia dei risultati](#).

Puoi abbonarti a una coda Amazon Simple Queue Service (Amazon SQS) per un argomento Amazon SNS, ma devi utilizzare un argomento Amazon SNS Amazon Resource Name (ARN) che si trova nella stessa regione. Per ulteriori informazioni, consulta l'argomento [Tutorial: Subscribing a Amazon SQS queue to an Amazon SNS nella Amazon Simple Queue Service Developer Guide](#).

Puoi anche utilizzare una AWS Lambda funzione per richiamare eventi quando ricevi notifiche. Per ulteriori informazioni, incluso un codice di funzione di esempio, consulta [Tutorial: Using AWS Lambda with Amazon Simple Notification Service](#) nella AWS Lambda Developer Guide.

Gli ARN dell'argomento Amazon SNS per ogni regione sono i seguenti.

Regione AWS	ARN di un argomento Amazon SNS
Stati Uniti orientali (Ohio)	<code>arn:aws:sns:us-east-2:291342846459:SecurityHubAnnouncements</code>
Stati Uniti orientali (Virginia settentrionale)	<code>arn:aws:sns:us-east-1:088139225913:SecurityHubAnnouncements</code>
Stati Uniti occidentali (California settentrionale)	<code>arn:aws:sns:us-west-1:137690824926:SecurityHubAnnouncements</code>
Stati Uniti occidentali (Oregon)	<code>arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements</code>

Regione AWS	ARN di un argomento Amazon SNS
Africa (Città del Capo)	<code>arn:aws:sns:af-south-1:463142546776:SecurityHubAnnouncements</code>
Asia Pacifico (Hong Kong)	<code>arn:aws:sns:ap-east-1:464812404305:SecurityHubAnnouncements</code>
Asia Pacific (Hyderabad)	<code>arn:aws:sns:ap-south-2:849907286123:SecurityHubAnnouncements</code>
Asia Pacifico (Giacarta)	<code>arn:aws:sns:ap-southeast-3:627843640627:SecurityHubAnnouncements</code>
Asia Pacifico (Mumbai)	<code>arn:aws:sns:ap-south-1:707356269775:SecurityHubAnnouncements</code>
Asia Pacific (Osaka)	<code>arn:aws:sns:ap-northeast-3:633550238216:SecurityHubAnnouncements</code>
Asia Pacific (Seul)	<code>arn:aws:sns:ap-northeast-2:374299265323:SecurityHubAnnouncements</code>
Asia Pacifico (Singapore)	<code>arn:aws:sns:ap-southeast-1:512267288502:SecurityHubAnnouncements</code>
Asia Pacifico (Sydney)	<code>arn:aws:sns:ap-southeast-2:475730049140:SecurityHubAnnouncements</code>

Regione AWS	ARN di un argomento Amazon SNS
Asia Pacifico (Tokyo)	<code>arn:aws:sns:ap-northeast-1:592469075483:SecurityHubAnnouncements</code>
Canada (Centrale)	<code>arn:aws:sns:ca-central-1:137749997395:SecurityHubAnnouncements</code>
Cina (Pechino)	<code>arn:aws-cn:sns:cn-north-1:672341567257:SecurityHubAnnouncements</code>
China (Ningxia)	<code>arn:aws-cn:sns:cn-northwest-1:672534482217:SecurityHubAnnouncements</code>
Europa (Francoforte)	<code>arn:aws:sns:eu-central-1:871975303681:SecurityHubAnnouncements</code>
Europa (Irlanda)	<code>arn:aws:sns:eu-west-1:705756202095:SecurityHubAnnouncements</code>
Europa (Londra)	<code>arn:aws:sns:eu-west-2:883600840440:SecurityHubAnnouncements</code>
Europa (Milano)	<code>arn:aws:sns:eu-south-1:151363035580:SecurityHubAnnouncements</code>
Europa (Parigi)	<code>arn:aws:sns:eu-west-3:313420042571:SecurityHubAnnouncements</code>

Regione AWS	ARN di un argomento Amazon SNS
Europa (Spagna)	<code>arn:aws:sns:eu-south-2:777487947751:SecurityHubAnnouncements</code>
Europa (Stoccolma)	<code>arn:aws:sns:eu-north-1:191971010772:SecurityHubAnnouncements</code>
Europa (Zurigo)	<code>arn:aws:sns:eu-central-2:704347005078:SecurityHubAnnouncements</code>
Israele (Tel Aviv)	<code>arn:aws:sns:il-central-1:726652212146:SecurityHubAnnouncements</code>
Medio Oriente (Bahrein)	<code>arn:aws:sns:me-south-1:585146626860:SecurityHubAnnouncements</code>
Medio Oriente (Emirati Arabi Uniti)	<code>arn:aws:sns:me-central-1:431548502100:SecurityHubAnnouncements</code>
Sud America (San Paolo)	<code>arn:aws:sns:sa-east-1:359811883282:SecurityHubAnnouncements</code>
AWS GovCloud (Stati Uniti orientali)	<code>arn:aws-us-gov:sns:us-gov-east-1:239368469855:SecurityHubAnnouncements</code>
AWS GovCloud (Stati Uniti occidentali)	<code>arn:aws-us-gov:sns:us-gov-west-1:239334163374:SecurityHubAnnouncements</code>

I messaggi sono in genere gli stessi in tutte le regioni all'interno di una [partizione](#), quindi puoi iscriverti a una regione in ogni partizione per ricevere annunci che riguardano tutte le aree di quella partizione. Gli annunci associati agli account dei membri non vengono replicati nell'account amministratore. Di conseguenza, ogni account, incluso l'account amministratore, avrà solo una copia di ogni annuncio. Puoi decidere quale account utilizzare per iscriverti agli annunci di Security Hub.

[Per informazioni sul costo dell'abbonamento agli annunci di Security Hub, consulta i prezzi di Amazon SNS.](#)

Iscrizione agli annunci del Security Hub (console)

1. Apri la console Amazon SNS all'indirizzo <https://console.aws.amazon.com/sns/v3/home>.
2. Nell'elenco delle regioni, scegli la regione in cui desideri iscriverti agli annunci del Security Hub. Questo esempio utilizza la regione us-west-2.
3. Nel riquadro di navigazione scegliere Subscriptions (Sottoscrizioni), quindi selezionare Create subscription (Crea sottoscrizione).
4. Inserisci l'argomento ARN nella casella Argomento ARN. Ad esempio, `arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements`.
5. Per Protocol, scegli come desideri ricevere gli annunci del Security Hub. Se scegli Email, for Endpoint, inserisci l'indirizzo email che desideri utilizzare per ricevere annunci.
6. Scegli Crea sottoscrizione.
7. Confermare la sottoscrizione. Ad esempio, se hai scelto il protocollo e-mail, Amazon SNS invierà un messaggio di conferma dell'iscrizione all'indirizzo e-mail che hai fornito.

Iscrizione agli annunci del Security Hub () AWS CLI

1. Esegui il comando seguente:

```
aws sns --region us-west-2 subscribe --topic-arn arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements --protocol email --notification-endpoint your_email@your_domain.com
```

2. Confermare la sottoscrizione. Ad esempio, se hai scelto il protocollo e-mail, Amazon SNS invierà un messaggio di conferma dell'iscrizione all'indirizzo e-mail che hai fornito.

Formato dei messaggi Amazon SNS

Gli esempi seguenti mostrano gli annunci di Security Hub di Amazon SNS sull'introduzione di nuovi controlli di sicurezza. Il contenuto dei messaggi varia in base al tipo di annuncio, ma il formato è lo stesso per tutti i tipi di annuncio. Facoltativamente, può essere incluso un Link campo che fornisce dettagli sull'annuncio.

Esempio: annuncio del Security Hub per nuovi controlli (protocollo e-mail)

```
{
  "AnnouncementType": "NEW_STANDARDS_CONTROLS",
  "Title": "[New Controls] 36 new Security Hub controls added to the AWS Foundational Security Best Practices standard",
  "Description": "We have added 36 new controls to the AWS Foundational Security Best Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation (CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud (Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR) (ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5, ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12, ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3, NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7), Amazon Redshift (Redshift.9), Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service (SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS Foundational Security Best Practices standard in an account and configured Security Hub to automatically enable new controls, these controls are enabled by default. Availability of controls can vary by Region. "
}
```

Esempio: annuncio del Security Hub per nuovi controlli (protocollo Email-JSON)

```
{
  "Type" : "Notification",
  "MessageId" : "d124c9cf-326a-5931-9263-92a92e7af49f",
  "TopicArn" : "arn:aws:sns:us-west-2:393883065485:SecurityHubAnnouncements",
  "Message" : "{\"AnnouncementType\": \"NEW_STANDARDS_CONTROLS\", \"Title\": \"[New Controls] 36 new Security Hub controls added to the AWS Foundational Security Best Practices standard\", \"Description\": \"We have added 36 new controls to the AWS Foundational Security Best Practices standard. These include controls for Amazon Auto Scaling (AutoScaling.3, AutoScaling.4, AutoScaling.6), AWS CloudFormation
```

```
(CloudFormation.1), Amazon CloudFront (CloudFront.10), Amazon Elastic Compute Cloud
(Amazon EC2) (EC2.23, EC2.24, EC2.27), Amazon Elastic Container Registry (Amazon ECR)
(ECR.1, ECR.2), Amazon Elastic Container Service (Amazon ECS) (ECS.3, ECS.4, ECS.5,
ECS.8, ECS.10, ECS.12), Amazon Elastic File System (Amazon EFS) (EFS.3, EFS.4), Amazon
Elastic Kubernetes Service (Amazon EKS) (EKS.2), Elastic Load Balancing (ELB.12,
ELB.13, ELB.14), Amazon Kinesis (Kinesis.1), AWS Network Firewall (NetworkFirewall.3,
NetworkFirewall.4, NetworkFirewall.5), Amazon OpenSearch Service (OpenSearch.7),
Amazon Redshift (Redshift.9),
Amazon Simple Storage Service (Amazon S3) (S3.13), Amazon Simple Notification Service
(SNS.2), AWS WAF (WAF.2, WAF.3, WAF.4, WAF.6, WAF.7, WAF.8). If you enabled the AWS
Foundational Security Best Practices standard in an account and configured SSecurity
Hub to automatically enable new controls, these controls are enabled by default.
Availability of controls can vary by Region. \"}",
  "Timestamp" : "2022-08-04T19:11:12.652Z",
  "SignatureVersion" : "1",
  "Signature" :
  "HTHgNFRYMetCvisulgLm4CVySvK9qCXFPHQDxY19tuCFQuIrd7Y04m4YFR28XKMgzqrF20YP
+EilipUm2S0TpEEt0TekU5bn74+YmNZfwr4aPFx0vUuQCV0shmHl37hjkilJhCg/t53QQiLFP7MH
+MTXIUPR37k5SuFCXvjpRQ8ynV532AH3Wpv0HmojDLMg+eg51V1fUs0G8yiJVCBEJhJ1yS
+gkwJdhRk2UQab9RcAmE6COK3hRwcjDwqTXz5nR6Ywv1ZqZfLl17gYKslt+jsyd/k+7k0qGm0JRDr7qhE7H
+7vaGRL0ptsQnbW8VmeYnDbahE08FV+Mp1rpV+7Qg==",
  "SigningCertURL" : "https://sns.us-west-2.amazonaws.com/
SimpleNotificationService-56e67fcb41f6fec09b0196692625d385.pem",
  "UnsubscribeURL" : "https://sns.us-west-2.amazonaws.com/?
Action=Unsubscribe&SubscriptionArn=arn:aws:sns:us-
west-2:393883065485:SecurityHubAnnouncements:9d0230d7-d582-451d-9f15-0c32818bf61f"
}
```

Sicurezza in AWS Security Hub

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, è possibile trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle organizzazioni più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra te e AWS. Il [modello di responsabilità condivisa](#) descrive questo come sicurezza del cloud e sicurezza nel cloud:

- La sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce i servizi AWS nel cloud AWS. AWS fornisce inoltre servizi che puoi utilizzare in sicurezza. I revisori di terze parti testano e verificano regolarmente l'efficacia della sicurezza come parte dei [programmi di conformità AWS](#). Per ulteriori informazioni sui programmi di conformità che si applicano a AWS Security Hub, consulta [Servizi coperti dal programma di conformità AWS](#).
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione aiuta a capire come applicare il modello di responsabilità condivisa quando si utilizza Security Hub. I seguenti argomenti mostrano come configurare Security Hub per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le risorse del Security Hub.

Argomenti

- [Protezione dei dati in AWS Security Hub](#)
- [AWS Identity and Access Management per AWS Security Hub](#)
- [Convalida della conformità per AWS Security Hub](#)
- [Resilienza nel AWS Security Hub](#)
- [Sicurezza dell'infrastruttura nell'AWS Security Hub](#)
- [AWS Security Hub ed endpoint VPC dell'interfaccia \(AWS PrivateLink\)](#)

Protezione dei dati in AWS Security Hub

Il [modello di responsabilità condivisa](#) di AWS si applica alla protezione dei dati in AWS Security Hub. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale

che esegue tutto l'Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. Inoltre, sei responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS che utilizzi. Per ulteriori informazioni sulla privacy dei dati, vedi le [Domande frequenti sulla privacy dei dati](#). Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al [Modello di responsabilità condivisa AWS e GDPR](#) nel Blog sulla sicurezza AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWS e di configurare singoli utenti con AWS IAM Identity Center o AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza predefiniti in Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se necessiti di moduli crittografici convalidati FIPS 140-2 quando accedi ad AWS attraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il [Federal Information Processing Standard \(FIPS\) 140-2](#).

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Security Hub o altro Servizi AWS utilizzando la console, l'API o AWS gli SDK. AWS CLI I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Security Hub è un'offerta di servizi multi-tenant. Per garantire la protezione dei dati, Security Hub crittografa i dati inattivi e i dati in transito tra i servizi componenti.

AWS Identity and Access Management per AWS Security Hub

AWS Identity and Access Management (IAM) è un software Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle AWS risorse. Gli amministratori

IAM controllano chi può essere autenticato (effettuato l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse del Security Hub. IAM è uno Servizio AWS strumento che puoi utilizzare senza costi aggiuntivi.

Argomenti

- [Destinatari](#)
- [Autenticazione con identità](#)
- [Gestione dell'accesso con policy](#)
- [Come AWS Security Hub funziona con IAM](#)
- [Esempi di policy basate sull'identità per Security Hub](#)
- [Ruoli collegati ai servizi per Security Hub](#)
- [AWS politiche gestite per AWS Security Hub](#)
- [Risoluzione dei problemi di identità e accesso in AWS Security Hub](#)

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Security Hub.

Utente del servizio: se utilizzi il servizio Security Hub per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Security Hub per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità in Security Hub, vedi [Risoluzione dei problemi di identità e accesso in AWS Security Hub](#).

Amministratore del servizio: se sei responsabile delle risorse di Security Hub presso la tua azienda, probabilmente hai pieno accesso a Security Hub. È tuo compito determinare a quali funzionalità e risorse del Security Hub devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per saperne di più su come la tua azienda può utilizzare IAM con Security Hub, consulta [Come AWS Security Hub funziona con IAM](#).

Amministratore IAM: se sei un amministratore IAM, potresti voler conoscere i dettagli su come scrivere policy per gestire l'accesso a Security Hub. Per visualizzare esempi di policy basate

sull'identità di Security Hub che puoi utilizzare in IAM, consulta. [Esempi di policy basate sull'identità per Security Hub](#)

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi [Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente](#).

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta [Signing AWS API request](#) nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta [Autenticazione a più fattori](#) nella Guida per l'utente di AWS IAM Identity Center e [Utilizzo dell'autenticazione a più fattori \(MFA\) in AWS](#) nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conservare le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente

root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione [Attività che richiedono le credenziali dell'utente root](#) nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta [Cos'è Centro identità IAM?](#) nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un [utente IAM](#) è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina [Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine](#) nella Guida per l'utente di IAM.

Un [gruppo IAM](#) è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli

utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta [Quando creare un utente IAM \(invece di un ruolo\)](#) nella Guida per l'utente di IAM.

Ruoli IAM

Un [ruolo IAM](#) è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console [cambiando ruolo](#). Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta [Utilizzo di ruoli IAM](#) nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- **Accesso utente federato:** per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta [Creazione di un ruolo per un provider di identità di terza parte](#) nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta [Set di autorizzazioni](#) nella Guida per l'utente di AWS IAM Identity Center .
- **Autorizzazioni utente IAM temporanee:** un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- **Accesso multi-account:** è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.
- **Accesso a più servizi:** alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.

- **Sessioni di accesso diretto (FAS):** quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina [Forward access sessions](#).
- **Ruolo di servizio:** un ruolo di servizio è un [ruolo IAM](#) che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione [Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS](#) nella Guida per l'utente di IAM.
- **Ruolo collegato al servizio:** un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.
- **Applicazioni in esecuzione su Amazon EC2:** puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Cloud è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWS a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta [Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2](#) nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta [Quando creare un ruolo IAM \(invece di un utente\)](#) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La

maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta [Panoramica delle policy JSON](#) nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'azione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruoli IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta [Scelta fra policy gestite e policy inline](#) nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta [Panoramica delle liste di controllo degli accessi \(ACL\)](#) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- **Limiti delle autorizzazioni:** un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta [Limiti delle autorizzazioni per le entità IAM](#) nella Guida per l'utente di IAM.
- **Politiche di controllo dei servizi (SCP):** le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in AWS Organizations. AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle [Policy di controllo dei servizi](#) nella Guida per l'utente di AWS Organizations .
- **Policy di sessione:** le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire

da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta [Policy di sessione](#) nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta [Logica di valutazione delle policy](#) nella IAM User Guide.

Come AWS Security Hub funziona con IAM

Prima di utilizzare AWS Identity and Access Management per gestire l'accesso a Security Hub, scopri quali funzionalità IAM sono disponibili per l'uso con Security Hub.

Funzionalità IAM che puoi usare con Amazon Macie

Funzionalità IAM	Supporto per Macie
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	No
Chiavi di condizione delle policy	Sì
Liste di controllo accessi di rete (ACL)	No
Controllo degli accessi basato sugli attributi (ABAC): tag nelle politiche	Sì
Credenziali temporanee	Sì
Inoltro delle sessioni di accesso (FAS)	Sì
● Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per una panoramica di alto livello su come Security Hub e altri Servizi AWS funzionano con la maggior parte delle funzionalità IAM, consulta [Servizi AWS That work with IAM nella IAM User Guide](#).

Politiche basate sull'identità per Security Hub

Supporta le policy basate su identità	Si
---------------------------------------	----

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta [Creazione di policy IAM](#) nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta [Guida di riferimento agli elementi delle policy JSON IAM](#) nella Guida per l'utente di IAM.

Security Hub supporta politiche basate sull'identità. Per ulteriori informazioni, consulta [Esempi di policy basate sull'identità per Security Hub](#).

Politiche basate su risorse per Security Hub

Supporta le policy basate su risorse	No
--------------------------------------	----

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario [specificare un principale](#) in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account

a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste ulteriori policy basate su identità. Per ulteriori informazioni, consulta [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.

Security Hub non supporta policy basate sulle risorse. Non è possibile collegare una policy IAM direttamente a una risorsa Security Hub.

Azioni politiche per Security Hub

Supporta le operazioni di policy	Sì
----------------------------------	----

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Le azioni politiche in Security Hub utilizzano il seguente prefisso prima dell'azione:

```
securityhub:
```

Ad esempio, per concedere a un utente l'autorizzazione ad abilitare Security Hub, che è un'azione che corrisponde al `EnableSecurityHub` funzionamento dell'API Security Hub, includi `securityhub:EnableSecurityHub` azione nella sua politica. Le istruzioni della policy devono includere un elemento `Action` o `NotAction`. Security Hub definisce il proprio set di azioni che descrivono le attività che è possibile eseguire con questo servizio.

```
"Action": "securityhub:EnableSecurityHub"
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola. Per esempio:

```
"Action": [  
  "securityhub:EnableSecurityHub",  
  "securityhub:BatchEnableStandards"
```

È inoltre possibile specificare più azioni utilizzando i caratteri jolly (*). Ad esempio, per specificare tutte le azioni che iniziano con la parola Get, includi la seguente azione:

```
"Action": "securityhub:Get*"
```

Tuttavia, è consigliabile definire policy in grado di seguire il principio del privilegio minimo. In altre parole, è necessario creare policy che includano solo le autorizzazioni necessarie per eseguire un'attività specifica.

L'utente deve avere accesso all'DescribeStandardsControloperazione per poter accedere a BatchGetSecurityControlsBatchGetStandardsControlAssociations, eListStandardsControlAssociations.

L'utente deve avere accesso all'UpdateStandardsControloperazione per poter accedere aBatchUpdateStandardsControlAssociations, eUpdateSecurityControl.

Per un elenco delle azioni del Security Hub, vedere [Azioni definite da AWS Security Hub](#) nel Service Authorization Reference. Per esempi di policy che specificano le azioni del Security Hub, vedere [Esempi di policy basate sull'identità per Security Hub](#).

Risorse

Supporta le risorse di policy

No

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON Resource della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento Resource o un elemento NotResource. Come best practice, specifica una risorsa utilizzando il suo [nome della risorsa Amazon \(ARN\)](#). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Security Hub definisce i seguenti tipi di risorse:

- Hub
- Product
- Finding aggregator, noto anche come aggregatore interregionale
- Regola di automazione
- Politica di configurazione

È possibile specificare questi tipi di risorse nelle politiche utilizzando gli ARN.

Per un elenco dei tipi di risorse Security Hub e la sintassi ARN per ciascuno di essi, vedere [Tipi di risorse definiti da AWS Security Hub](#) nel Service Authorization Reference. Per sapere quali azioni è possibile specificare per ogni tipo di risorsa, vedere [Azioni definite da AWS Security Hub](#) nel Service Authorization Reference. Per esempi di politiche che specificano le risorse, vedere [Esempi di policy basate sull'identità per Security Hub](#).

Chiavi relative alle condizioni delle policy per Security Hub

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì
---	----

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni condizionali che utilizzano [operatori di condizione](#), ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione AND logica. Se si specificano

più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. OR Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta [Elementi delle policy IAM: variabili e tag](#) nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di [contesto delle condizioni AWS globali nella Guida](#) per l'utente IAM.

Per un elenco delle chiavi di condizione di Security Hub, consulta [Chiavi di condizione AWS Security Hub](#) nel Service Authorization Reference. Per sapere con quali azioni e risorse è possibile utilizzare una chiave di condizione, consulta [Azioni definite da AWS Security Hub](#). Per esempi di politiche che utilizzano chiavi condizionali, consulta [Esempi di policy basate sull'identità per Security Hub](#).

Liste di controllo degli accessi (ACL) in Security Hub

Supporta le ACL

No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Security Hub non supporta gli ACL, il che significa che non è possibile collegare un ACL a una risorsa Security Hub.

Controllo degli accessi basato sugli attributi (ABAC) con Security Hub

Supporta ABAC (tag nelle policy)

Sì

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è

il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'[elemento condizione](#) di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta [Che cos'è ABAC?](#) nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta [Utilizzo del controllo degli accessi basato su attributi \(ABAC\)](#) nella Guida per l'utente di IAM.

È possibile allegare tag alle risorse del Security Hub. È inoltre possibile controllare l'accesso alle risorse fornendo informazioni sui tag nell'[Conditionelemento](#) di una policy.

Per informazioni sull'etichettatura delle risorse del Security Hub, vedere [Taggare le risorse del AWS Security Hub](#). Per un esempio di policy basata sull'identità che controlla l'accesso a una risorsa in base ai tag, vedi [Esempi di policy basate sull'identità per Security Hub](#)

Utilizzo di credenziali temporanee con Security Hub

Supporta le credenziali temporanee	Sì
------------------------------------	----

Alcune Servizi AWS non funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla [Servizi AWS compatibilità con IAM nella IAM User Guide](#).

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta [Cambio di un ruolo \(console\)](#) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API `or. AWS CLI` o `AWS CLI`. È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS consiglia di generare dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta [Credenziali di sicurezza provvisorie in IAM](#).

È possibile utilizzare credenziali temporanee per effettuare l'accesso con la federazione, assumere un ruolo IAM o un ruolo multi-account. È possibile ottenere credenziali di sicurezza temporanee chiamando operazioni AWS STS API come `o. AssumeRoleGetFederationToken`.

Security Hub supporta l'uso di credenziali temporanee.

Sessioni di accesso diretto per Security Hub

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì
--	----

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama un Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina [Forward access sessions](#).

Ad esempio, Security Hub invia le richieste FAS a valle Servizi AWS quando si integra Security Hub con AWS Organizations e quando si designa l'account amministratore delegato di Security Hub per un'organizzazione in Organizations.

Per altre attività, Security Hub utilizza un ruolo collegato al servizio per eseguire azioni per conto dell'utente. Per i dettagli su questo ruolo, consulta [Ruoli collegati ai servizi per Security Hub](#).

Ruoli di servizio per Security Hub

Security Hub non assume né utilizza ruoli di servizio. Per eseguire azioni per conto dell'utente, Security Hub utilizza un ruolo collegato al servizio. Per i dettagli su questo ruolo, consulta [Ruoli collegati ai servizi per Security Hub](#).

⚠ Warning

La modifica delle autorizzazioni per un ruolo di servizio può creare problemi operativi con l'utilizzo di Security Hub. Modifica i ruoli di servizio solo quando Security Hub fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Security Hub

Supporta i ruoli collegati ai servizi

Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un servizio AWS. Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Security Hub utilizza un ruolo collegato al servizio per eseguire azioni per conto dell'utente. Per i dettagli su questo ruolo, consulta [Ruoli collegati ai servizi per Security Hub](#)

Esempi di policy basate sull'identità per Security Hub

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse del Security Hub. Inoltre, non sono in grado di eseguire attività utilizzando l'API AWS Management Console, AWS CLI, o AWS. Un amministratore deve creare le policy IAM che concedono a utenti e ruoli l'autorizzazione per eseguire operazioni API specifiche sulle risorse specificate di cui hanno bisogno. L'amministratore deve quindi collegare queste policy a utenti o gruppi che richiedono tali autorizzazioni.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta [Creazione di policy nella scheda JSON](#) nella Guida per l'utente IAM.

Argomenti

- [Best practice delle policy](#)
- [Utilizzo della console Security Hub](#)
- [Esempio: consentire agli utenti di visualizzare le loro autorizzazioni](#)
- [Esempio: consentire agli utenti di creare e gestire una politica di configurazione](#)

- [Esempio: consenti agli utenti di visualizzare i risultati](#)
- [Esempio: consentire agli utenti di creare e gestire regole di automazione](#)

Best practice delle policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare le risorse del Security Hub nel tuo account. Queste operazioni possono comportare costi aggiuntivi per l'Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Nozioni di base sulle policy gestite da AWS e passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWS che concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWS specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta [Policy gestite da AWS](#) o [Policy gestite da AWS per le funzioni dei processi](#) nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta [Policy e autorizzazioni in IAM](#) nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione [Elementi delle policy JSON di IAM: condizione](#) nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta [Convalida delle policy per IAM Access Analyzer](#) nella Guida per l'utente di IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA

quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta [Configurazione dell'accesso alle API protetto con MFA](#) nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta [Best practice di sicurezza in IAM](#) nella Guida per l'utente di IAM.

Utilizzo della console Security Hub

Per accedere alla console AWS Security Hub è necessario disporre di un insieme di autorizzazioni minimo. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse del Security Hub presenti nel tuo Account AWS. Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario concedere le autorizzazioni minime della console agli utenti che effettuano chiamate solo alla AWS CLI o all'API AWS. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che tali utenti e ruoli possano utilizzare la console Security Hub, allega anche la seguente politica AWS gestita all'entità. Per ulteriori informazioni, consulta la sezione [Aggiunta di autorizzazioni a un utente](#) nella Guida per l'utente di IAM:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```

```
]
}
```

Esempio: consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono allegate alla relativa identità utente. La policy include le autorizzazioni per completare questa azione sulla console o a livello di programmazione utilizzando la AWS CLI o l'API AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ViewOwnUserInfo",
      "Effect": "Allow",
      "Action": [
        "iam:GetUserPolicy",
        "iam:ListGroupForUser",
        "iam:ListAttachedUserPolicies",
        "iam:ListUserPolicies",
        "iam:GetUser"
      ],
      "Resource": ["arn:aws:iam::*:user/${aws:username}"]
    },
    {
      "Sid": "NavigateInConsole",
      "Effect": "Allow",
      "Action": [
        "iam:GetGroupPolicy",
        "iam:GetPolicyVersion",
        "iam:GetPolicy",
        "iam:ListAttachedGroupPolicies",
        "iam:ListGroupPolicies",
        "iam:ListPolicyVersions",
        "iam:ListPolicies",
        "iam:ListUsers"
      ],
      "Resource": "*"
    }
  ]
}
```

Esempio: consentire agli utenti di creare e gestire una politica di configurazione

Questo esempio mostra come è possibile creare una policy IAM che consenta a un utente di creare, visualizzare, aggiornare ed eliminare le politiche di configurazione. Questa policy di esempio consente inoltre all'utente di avviare, interrompere e visualizzare le associazioni di policy. Affinché questa policy IAM funzioni, l'utente deve essere l'amministratore delegato del Security Hub di un'organizzazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAndUpdateConfigurationPolicy",
      "Effect": "Allow",
      "Action": [
        "securityhub:CreateConfigurationPolicy",
        "securityhub:UpdateConfigurationPolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ViewConfigurationPolicy",
      "Effect": "Allow",
      "Action": [
        "securityhub:GetConfigurationPolicy",
        "securityhub:ListConfigurationPolicies"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DeleteConfigurationPolicy",
      "Effect": "Allow",
      "Action": [
        "securityhub:DeleteConfigurationPolicy"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ViewConfigurationPolicyAssociation",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchGetConfigurationPolicyAssociations",
        "securityhub:GetConfigurationPolicyAssociation",

```



```

        "securityhub:ListConfigurationPolicyAssociations"
    ],
    "Resource": "*"
  },
  {
    "Sid": "UpdateConfigurationPolicyAssociation",
    "Effect": "Allow",
    "Action": [
      "securityhub:StartConfigurationPolicyAssociation",
      "securityhub:StartConfigurationPolicyDisassociation"
    ],
    "Resource": "*"
  }
]
}

```

Esempio: consenti agli utenti di visualizzare i risultati

Questo esempio mostra come è possibile creare una policy IAM che consenta a un utente di visualizzare i risultati del Security Hub.

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReviewFindings",
      "Effect": "Allow",
      "Action": [
        "securityhub:GetFindings"
      ],
      "Resource": "*"
    }
  ]
}

```

Esempio: consentire agli utenti di creare e gestire regole di automazione

Questo esempio mostra come è possibile creare una policy IAM che consenta a un utente di creare, visualizzare, aggiornare ed eliminare le regole di automazione del Security Hub. Affinché questa policy IAM funzioni, l'utente deve essere un amministratore del Security Hub. Per limitare le autorizzazioni, ad esempio per consentire a un utente di visualizzare solo le regole di automazione, puoi rimuovere le autorizzazioni di creazione, aggiornamento ed eliminazione.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CreateAndUpdateAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:CreateAutomationRule",
        "securityhub:BatchUpdateAutomationRules"
      ],
      "Resource": "*"
    },
    {
      "Sid": "ViewAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchGetAutomationRules",
        "securityhub:ListAutomationRules"
      ],
      "Resource": "*"
    },
    {
      "Sid": "DeleteAutomationRules",
      "Effect": "Allow",
      "Action": [
        "securityhub:BatchDeleteAutomationRules"
      ],
      "Resource": "*"
    }
  ]
}
```

Ruoli collegati ai servizi per Security Hub

AWS Security Hub utilizza un ruolo collegato al [servizio AWS Identity and Access Management \(IAM\) denominato](#) `AWSServiceRoleForSecurityHub`. Questo ruolo collegato ai servizi è un ruolo IAM collegato direttamente a Security Hub. È predefinito da Security Hub e include tutte le autorizzazioni richieste da Security Hub per chiamare altri Servizi AWS e monitorare AWS le risorse per tuo conto. Security Hub utilizza questo ruolo collegato al servizio in tutti i Regioni AWS casi in cui Security Hub è disponibile.

Un ruolo collegato al servizio semplifica la configurazione di Security Hub perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Security Hub definisce le autorizzazioni del suo ruolo collegato al servizio e, a meno che le autorizzazioni non siano definite diversamente, solo Security Hub può assumere il ruolo. Le autorizzazioni definite includono la politica di fiducia e la politica delle autorizzazioni e non è possibile collegare tale politica di autorizzazione a nessun'altra entità IAM.

Per visualizzare i dettagli del ruolo collegato al servizio, nella pagina Impostazioni della console Security Hub, scegli Generale, quindi Visualizza le autorizzazioni del servizio.

È possibile eliminare il ruolo collegato al servizio Security Hub solo dopo aver prima disabilitato Security Hub in tutte le regioni in cui è abilitato. In questo modo proteggi le tue risorse Security Hub perché non puoi rimuovere inavvertitamente le autorizzazioni per accedervi.

Per informazioni su altri servizi che supportano i ruoli collegati ai servizi, consulta i [AWSservizi che funzionano con IAM](#) nella Guida per l'utente di IAM e individua i servizi con Sì nella colonna Service-Linked Role. Scegli Sì in corrispondenza di un link per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Argomenti

- [Autorizzazioni di ruolo collegate ai servizi per Security Hub](#)
- [Creazione di un ruolo collegato ai servizi per Security Hub](#)
- [Modifica di un ruolo collegato al servizio per Security Hub](#)
- [Eliminazione di un ruolo collegato al servizio per Security Hub](#)

Autorizzazioni di ruolo collegate ai servizi per Security Hub

Security Hub utilizza il ruolo collegato al servizio denominato `AWSServiceRoleForSecurityHub`. È un ruolo collegato al servizio necessario per accedere AWS Security Hub alle tue risorse. Il ruolo collegato al servizio consente a Security Hub di ricevere risultati da altri Servizi AWS e configurare l'AWS Configinfrastruttura necessaria per eseguire i controlli di sicurezza.

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi `AWSServiceRoleForSecurityHub` considera attendibili i seguenti servizi:

- `securityhub.amazonaws.com`

Il ruolo collegato ai servizi `AWSServiceRoleForSecurityHub` utilizza la policy gestita [AWSSecurityHubServiceRolePolicy](#).

È necessario concedere le autorizzazioni per consentire a un'identità IAM (come un ruolo, un gruppo o un utente) di creare, modificare o eliminare un ruolo collegato al servizio.

`AWSServiceRoleForSecurityHub` Affinché il ruolo collegato al servizio venga creato correttamente, l'identità IAM utilizzata per accedere a Security Hub deve disporre delle autorizzazioni richieste. Per concedere le autorizzazioni richieste, allega la seguente policy al ruolo, al gruppo o all'utente.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    }
  ]
}
```

Creazione di un ruolo collegato ai servizi per Security Hub

Il ruolo `AWSServiceRoleForSecurityHub` collegato al servizio viene creato automaticamente quando abiliti Security Hub per la prima volta o abiliti Security Hub in un'area supportata in cui in precedenza non era abilitato. Puoi anche creare il ruolo collegato ai servizi `AWSServiceRoleForSecurityHub` manualmente, utilizzando la console IAM, la CLI IAM o l'API IAM.

⚠ Important

Il ruolo collegato al servizio creato per l'account amministratore di Security Hub non si applica agli account membri del Security Hub.

Per ulteriori informazioni sulla creazione manuale del ruolo, consulta [Creazione di un ruolo collegato ai servizi](#) nella Guida per l'utente IAM.

Modifica di un ruolo collegato al servizio per Security Hub

Security Hub non consente di modificare il ruolo `AWSServiceRoleForSecurityHub` collegato al servizio. Dopo aver creato un ruolo collegato al servizio, non puoi modificarne il nome, perché potrebbero farvi riferimento diverse entità. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta [Modifica di un ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Security Hub

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo, non hai un'entità non utilizzata che non viene monitorata o gestita attivamente.

⚠ Important

Per eliminare il ruolo `AWSServiceRoleForSecurityHub` collegato al servizio, devi prima disabilitare Security Hub in tutte le regioni in cui è abilitato. Se Security Hub non è disabilitato quando si tenta di eliminare il ruolo collegato al servizio, l'eliminazione non riesce. Per ulteriori informazioni, consulta [Disabilitazione del Security Hub](#).

Quando si disabilita Security Hub, il ruolo `AWSServiceRoleForSecurityHub` collegato al servizio non viene eliminato automaticamente. Se abiliti nuovamente Security Hub, inizia a utilizzare il ruolo esistente `AWSServiceRoleForSecurityHub` collegato al servizio.

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Usa la console IAM, la CLI IAM oppure l'API IAM per eliminare il ruolo collegato ai servizi `AWSServiceRoleForSecurityHub`. Per ulteriori informazioni, consultare [Eliminazione del ruolo collegato ai servizi](#) nella Guida per l'utente di IAM.

AWS politiche gestite per AWS Security Hub

Una politica AWS gestita è una politica autonoma creata e amministrata da AWS. AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo [policy gestite dal cliente](#) specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare [Policy gestite da AWS](#) nella Guida per l'utente di IAM.

AWS politica gestita: AWSSecurityHubFullAccess

È possibile allegare la policy `AWSSecurityHubFullAccess` alle identità IAM.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo principale a tutte le azioni del Security Hub. Questa politica deve essere associata a un principale prima che quest'ultimo abiliti manualmente Security Hub per il proprio account. Ad esempio, i responsabili con queste autorizzazioni possono sia visualizzare che aggiornare lo stato dei risultati. Possono configurare approfondimenti personalizzati e abilitare le integrazioni. Possono abilitare e disabilitare standard e controlli. I responsabili di un account amministratore possono anche gestire gli account dei membri.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `securityhub`— Consente ai responsabili l'accesso completo a tutte le azioni del Security Hub.
- `guardduty`— Consente ai responsabili di ottenere informazioni sullo stato dell'account in Amazon GuardDuty.
- `iam`— Consente ai dirigenti di creare un ruolo collegato al servizio.

- **inspector**— Consente ai responsabili di ottenere informazioni sullo stato dell'account in Amazon Inspector.
- **pricing**— Consente ai committenti di ottenere un listino prezzi e prodotti. Servizi AWS

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SecurityHubAllowAll",
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubServiceLinkedRole",
      "Effect": "Allow",
      "Action": "iam:CreateServiceLinkedRole",
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "iam:AWSServiceName": "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid": "OtherServicePermission",
      "Effect": "Allow",
      "Action": [
        "guardduty:GetDetector",
        "guardduty:ListDetectors",
        "inspector2:BatchGetAccountStatus",
        "pricing:GetProducts"
      ],
      "Resource": "*"
    }
  ]
}
```

Politica gestita da Security Hub: AWSSecurityHubReadOnlyAccess

È possibile allegare la policy `AWSSecurityHubReadOnlyAccess` alle identità IAM.

Questa politica concede autorizzazioni di sola lettura che consentono agli utenti di visualizzare le informazioni in Security Hub. I responsabili a cui è allegata questa politica non possono effettuare aggiornamenti in Security Hub. Ad esempio, i responsabili con queste autorizzazioni possono visualizzare l'elenco dei risultati associati al proprio account, ma non possono modificare lo stato di un risultato. Possono visualizzare i risultati degli approfondimenti, ma non possono creare o configurare approfondimenti personalizzati. Non possono configurare controlli o integrazioni di prodotti.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- **securityhub**— Consente agli utenti di eseguire azioni che restituiscono un elenco di elementi o dettagli su un elemento. Ciò include le operazioni API che iniziano con `GetList`, `Describe`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AWSSecurityHubReadOnlyAccess",
      "Effect": "Allow",
      "Action": [
        "securityhub:Get*",
        "securityhub:List*",
        "securityhub:BatchGet*",
        "securityhub:Describe*"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS politica gestita: `AWSSecurityHubOrganizationsAccess`

È possibile allegare la policy `AWSSecurityHubOrganizationsAccess` alle identità IAM.

Questa politica concede le autorizzazioni amministrative necessarie per supportare l'integrazione del Security Hub con Organizations. AWS Organizations

Queste autorizzazioni consentono all'account di gestione dell'organizzazione di designare l'account amministratore delegato per Security Hub. Consentono inoltre all'account amministratore delegato di Security Hub di abilitare gli account dell'organizzazione come account membro.

Questa politica fornisce solo le autorizzazioni per Organizations. L'account di gestione dell'organizzazione e l'account amministratore delegato di Security Hub richiedono anche le autorizzazioni per le azioni associate in Security Hub. Queste autorizzazioni possono essere concesse utilizzando la politica gestita `AWSecurityHubFullAccess`.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `organizations:ListAccounts`— Consente ai responsabili di recuperare l'elenco degli account che fanno parte di un'organizzazione.
- `organizations:DescribeOrganization`— Consente ai dirigenti di recuperare informazioni sull'organizzazione.
- `organizations:ListRoots`— Consente ai dirigenti di elencare la radice di un'organizzazione.
- `organizations:ListDelegatedAdministrators`— Consente ai dirigenti di elencare l'amministratore delegato di un'organizzazione.
- `organizations:ListAWSServiceAccessForOrganization`— Consente ai dirigenti di elencare le informazioni utilizzate da un' Servizi AWS organizzazione.
- `organizations:ListOrganizationalUnitsForParent`— Consente ai responsabili di elencare le unità organizzative (OU) secondarie di un'unità organizzativa principale.
- `organizations:ListAccountsForParent`— Consente ai responsabili di elencare gli account secondari di un'unità organizzativa principale.
- `organizations:DescribeAccount`— Consente ai responsabili di recuperare informazioni su un account dell'organizzazione.
- `organizations:DescribeOrganizationalUnit`— Consente ai responsabili di recuperare informazioni su un'unità organizzativa all'interno dell'organizzazione.
- `organizations:DescribeOrganization`— Consente ai responsabili di recuperare informazioni sulla configurazione dell'organizzazione.
- `organizations:EnableAWSServiceAccess`— Consente ai responsabili di abilitare l'integrazione del Security Hub con Organizations.
- `organizations:RegisterDelegatedAdministrator`— Consente ai responsabili di designare l'account amministratore delegato per Security Hub.

- `organizations:DeregisterDelegatedAdministrator`— Consente ai responsabili di rimuovere l'account amministratore delegato per Security Hub.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "OrganizationPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:ListAccounts",
        "organizations:DescribeOrganization",
        "organizations:ListRoots",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:ListOrganizationalUnitsForParent",
        "organizations:ListAccountsForParent",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrganizationPermissionsEnable",
      "Effect": "Allow",
      "Action": "organizations:EnableAWSServiceAccess",
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": "securityhub.amazonaws.com"
        }
      }
    },
    {
      "Sid": "OrganizationPermissionsDelegatedAdmin",
      "Effect": "Allow",
      "Action": [
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "arn:aws:organizations::*:account/o-*/**",
      "Condition": {
```

```
        "StringEquals": {
            "organizations:ServicePrincipal": "securityhub.amazonaws.com"
        }
    }
}
```

AWS politica gestita: AWSSecurityHubServiceRolePolicy

Non è possibile collegare `AWSSecurityHubServiceRolePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente a Security Hub di eseguire azioni per conto dell'utente. Per ulteriori informazioni, consulta [the section called “Ruoli collegati ai servizi”](#).

Questa politica concede autorizzazioni amministrative che consentono al ruolo collegato al servizio di eseguire i controlli di sicurezza per i controlli del Security Hub.

Dettagli dell'autorizzazione

Questa policy include le autorizzazioni per eseguire le seguenti operazioni:

- `cloudtrail`— Recupera informazioni sui sentieri. CloudTrail
- `cloudwatch`— Recupera gli allarmi correnti CloudWatch .
- `logs`— Recupera i filtri metrici per i log. CloudWatch
- `sns`— Recupera l'elenco delle sottoscrizioni a un argomento SNS.
- `config`— Recupera informazioni sui registratori di configurazione, sulle risorse e sulle regole. AWS Config Consente inoltre al ruolo collegato al servizio di creare ed eliminare AWS Config regole e di eseguire valutazioni in base alle regole.
- `iam`— Ottieni e genera report sulle credenziali per gli account.
- `organizations`— Recupera le informazioni sull'account e sull'unità organizzativa (OU) di un'organizzazione.
- `securityhub`— Recupera informazioni su come sono configurati il servizio, gli standard e i controlli del Security Hub.
- `tag`— Recupera informazioni sui tag delle risorse.

```
{
  "Version": "2012-10-17",
  "Statement": [
```

```
{
  "Sid": "SecurityHubServiceRolePermissions",
  "Effect": "Allow",
  "Action": [
    "cloudtrail:DescribeTrails",
    "cloudtrail:GetTrailStatus",
    "cloudtrail:GetEventSelectors",
    "cloudwatch:DescribeAlarms",
    "cloudwatch:DescribeAlarmsForMetric",
    "logs:DescribeMetricFilters",
    "sns:ListSubscriptionsByTopic",
    "config:DescribeConfigurationRecorders",
    "config:DescribeConfigurationRecorderStatus",
    "config:DescribeConfigRules",
    "config:DescribeConfigRuleEvaluationStatus",
    "config:BatchGetResourceConfig",
    "config:SelectResourceConfig",
    "iam:GenerateCredentialReport",
    "organizations:ListAccounts",
    "config:PutEvaluations",
    "tag:GetResources",
    "iam:GetCredentialReport",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListChildren",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "securityhub:BatchDisableStandards",
    "securityhub:BatchEnableStandards",
    "securityhub:BatchUpdateStandardsControlAssociations",
    "securityhub:BatchGetSecurityControls",
    "securityhub:BatchGetStandardsControlAssociations",
    "securityhub:CreateMembers",
    "securityhub>DeleteMembers",
    "securityhub:DescribeHub",
    "securityhub:DescribeOrganizationConfiguration",
    "securityhub:DescribeStandards",
    "securityhub:DescribeStandardsControls",
    "securityhub:DisassociateFromAdministratorAccount",
    "securityhub:DisassociateMembers",
    "securityhub:DisableSecurityHub",
    "securityhub:EnableSecurityHub",
    "securityhub:GetEnabledStandards",
    "securityhub:ListStandardsControlAssociations",
```

```

        "securityhub:ListSecurityControlDefinitions",
        "securityhub:UpdateOrganizationConfiguration",
        "securityhub:UpdateSecurityControl",
        "securityhub:UpdateSecurityHubConfiguration",
        "securityhub:UpdateStandardsControl",
        "tag:GetResources"
    ],
    "Resource": "*"
  },
  {
    "Sid": "SecurityHubServiceRoleConfigPermissions",
    "Effect": "Allow",
    "Action": [
      "config:PutConfigRule",
      "config>DeleteConfigRule",
      "config:GetComplianceDetailsByConfigRule"
    ],
    "Resource": "arn:aws:config:*:*:config-rule/aws-service-rule/*securityhub*"
  },
  {
    "Sid": "SecurityHubServiceRoleOrganizationsPermissions",
    "Effect": "Allow",
    "Action": [
      "organizations:ListDelegatedAdministrators"
    ],
    "Resource": "*",
    "Condition": {
      "StringEquals": {
        "organizations:ServicePrincipal": [
          "securityhub.amazonaws.com"
        ]
      }
    }
  }
]
}

```

Aggiornamenti del Security Hub alle policy AWS gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Security Hub da quando questo servizio ha iniziato a tenere traccia di queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della [cronologia dei documenti](#) di Security Hub.

Modifica	Descrizione	Data
AWSSecurityHubFullAccess — Aggiornamento a una politica esistente	Security Hub ha aggiornato la politica per ottenere dettagli sui prezzi Servizi AWS e sui prodotti.	24 aprile 2024
AWSSecurityHubReadOnlyAccess — Aggiornamento a una politica esistente	Security Hub ha aggiornato questa politica gestita aggiungendo un Sid campo.	22 febbraio 2024
AWSSecurityHubFullAccess — Aggiornamento a una politica esistente	Security Hub ha aggiornato la policy in modo da determinare se Amazon GuardDuty e Amazon Inspector sono abilitati in un account. Questo aiuta i clienti a riunire più informazioni relative alla sicurezza. Servizi AWS	16 novembre 2023
AWSSecurityHubOrganizationsAccess — Aggiornamento a una politica esistente	Security Hub ha aggiornato la politica per concedere autorizzazioni aggiuntive per consentire l'accesso in sola lettura alle funzionalità di amministratore AWS Organizations delegato. Ciò include dettagli come la radice, le unità organizzative (OU), gli account, la struttura organizzativa e l'accesso al servizio.	16 novembre 2023
AWSSecurityHubServiceRolePolicy : aggiornamento a una policy esistente	Security Hub ha aggiunto BatchGetSecurityControls le Disassoci	26 novembre 2023

Modifica	Descrizione	Data
	<p>ateFromAdministrat orAccount autorizzazioni e UpdateSecurityCont rol le autorizzazioni per leggere e aggiornare le proprietà di controllo di sicurezza personalizzabili.</p>	
<p>AWSSecurityHubServiceRolePolicy: aggiornamento a una policy esistente</p>	<p>Security Hub ha aggiunto l'tag: GetRe sources autorizzazione a leggere i tag delle risorse relativi ai risultati.</p>	<p>7 novembre 2023</p>
<p>AWSSecurityHubServiceRolePolicy: aggiornamento a una policy esistente</p>	<p>Security Hub ha aggiunto l'BatchGetStandardsC ontrolAssociations autorizzazione per ottenere informazioni sullo stato di attivazione di un controllo in uno standard.</p>	<p>27 settembre 2023</p>
<p>AWSSecurityHubServiceRolePolicy: aggiornamento a una policy esistente</p>	<p>Security Hub ha aggiunto nuove autorizzazioni per ottenere AWS Organizations dati e leggere e aggiornare le configurazioni del Security Hub, inclusi standard e controlli.</p>	<p>20 settembre 2023</p>

Modifica	Descrizione	Data
AWSSecurityHubServiceRolePolicy : aggiornamento a una policy esistente	Security Hub ha spostato l' <code>config:DescribeConfigRuleEvaluationStatus</code> autorizzazione esistente in una dichiarazione diversa all'interno della policy. L' <code>config:DescribeConfigRuleEvaluationStatus</code> autorizzazione è ora applicata a tutte le risorse.	17 marzo 2023
AWSSecurityHubServiceRolePolicy : aggiornamento a una policy esistente	Security Hub ha spostato l' <code>config:PutEvaluations</code> autorizzazione esistente in una dichiarazione diversa all'interno della policy. L' <code>config:PutEvaluations</code> autorizzazione è ora applicata a tutte le risorse.	14 luglio 2021
AWSSecurityHubServiceRolePolicy : aggiornamento a una policy esistente	Security Hub ha aggiunto una nuova autorizzazione per consentire al ruolo collegato al servizio di fornire risultati di valutazione. AWS Config	29 giugno 2021
AWSSecurityHubServiceRolePolicy — Aggiunto all'elenco delle politiche gestite	Sono state aggiunte informazioni sulla politica gestita <code>AWSSecurityHubServiceRolePolicy</code> , utilizzata dal ruolo collegato al servizio Security Hub.	11 giugno 2021

Modifica	Descrizione	Data
AWSSecurityHubOrganizationsAccess — Nuova politica	Security Hub ha aggiunto una nuova politica che concede le autorizzazioni necessarie per l'integrazione del Security Hub con Organizations.	15 marzo 2021
Security Hub ha iniziato a tracciare le modifiche	Security Hub ha iniziato a tenere traccia delle modifiche per le sue politiche AWS gestite.	15 marzo 2021

Risoluzione dei problemi di identità e accesso in AWS Security Hub

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Security Hub e IAM.

Argomenti

- [Non sono autorizzato a eseguire un'azione in Security Hub](#)
- [Non sono autorizzato a eseguire iam: PassRole](#)
- [Desidero l'accesso programmatico a Security Hub](#)
- [Sono un amministratore e voglio consentire ad altri di accedere a Security Hub](#)
- [Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse del Security Hub](#)

Non sono autorizzato a eseguire un'azione in Security Hub

Se la AWS Management Console indica che non hai l'autorizzazione a eseguire un'operazione, devi contattare l'amministratore per ricevere assistenza. L'amministratore è colui che ti ha fornito le credenziali di accesso.

L'errore di esempio seguente si verifica quando l'utente `mateojackson` tenta di utilizzare la console per visualizzare i dettagli su un `widget` ma non dispone `securityhub:GetWidget` delle autorizzazioni.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
securityhub:GetWidget on resource: my-example-widget
```

In questo caso, Mateo richiede al suo amministratore di aggiornare le policy per poter accedere alla risorsa *my-example-widget* utilizzando l'operazione `securityhub:GetWidget`.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole` operazione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo a Security Hub.

Alcuni Servizi AWS consentono di trasmettere un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato ai servizi. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Security Hub. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Desidero l'accesso programmatico a Security Hub

Gli utenti hanno bisogno di un accesso programmatico se desiderano interagire con AWS esternamente a AWS Management Console. La modalità con cui concedere l'accesso programmatico dipende dal tipo di utente che accede ad AWS.

Per fornire agli utenti l'accesso programmatico, scegli una delle seguenti opzioni.

Quale utente necessita dell'accesso programmatico?	Per	Come
Identità della forza lavoro (Utenti gestiti nel centro identità IAM)	Utilizza credenziali temporane e per firmare richieste programmatiche alla AWS CLI, agli SDK AWS o alle API AWS.	Segui le istruzioni per l'interfaccia che desideri utilizzare. <ul style="list-style-type: none"> • Per la AWS CLI, consulta la pagina Configurazione della AWS CLI per l'uso di AWS IAM Identity Center nella Guida per l'utente dell'AWS Command Line Interface. • Per gli SDK AWS, gli strumenti e le API AWS, consulta la pagina Autenticazione Centro identità IAM nella Guida di riferimento per SDK e strumenti AWS.
IAM	Utilizza credenziali temporane e per firmare richieste programmatiche alla AWS CLI, agli SDK AWS o alle API AWS.	Segui le istruzioni in Utilizzo di credenziali temporanee con le risorse AWS nella Guida per l'utente IAM.
IAM	(Non consigliato) Utilizza credenziali a lungo termine per firmare richieste programmatiche alla AWS CLI, agli SDK AWS o alle API AWS.	Segui le istruzioni per l'interfaccia che desideri utilizzare. <ul style="list-style-type: none"> • Per la AWS CLI, consulta la pagina Autenticazione tramite credenziali utente IAM nella Guida per l'utente dell'AWS Command Line Interface. • Per gli SDK e gli strumenti AWS, consulta la pagina Autenticazione con

Quale utente necessita dell'accesso programmatico?	Per	Come
		<p>credenziali a lungo termine nella Guida di riferimento per SDK e strumenti AWS.</p> <ul style="list-style-type: none"> • Per le API AWS, consulta la pagina Gestione delle chiavi di accesso per utenti IAM nella Guida per l'utente IAM.

Sono un amministratore e voglio consentire ad altri di accedere a Security Hub

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

- Utenti e gruppi in AWS IAM Identity Center:

Crea un set di autorizzazioni. Segui le istruzioni riportate nella pagina [Create a permission set](#) (Creazione di un set di autorizzazioni) nella Guida per l'utente di AWS IAM Identity Center.

- Utenti gestiti in IAM tramite un provider di identità:

Crea un ruolo per la federazione delle identità. Segui le istruzioni riportate nella pagina [Creating a role for a third-party identity provider \(federation\)](#) (Creazione di un ruolo per un provider di identità di terze parti [federazione]) nella Guida per l'utente di IAM.

- Utenti IAM:

- Crea un ruolo che l'utente possa assumere. Per istruzioni, consulta la pagina [Creating a role for an IAM user](#) (Creazione di un ruolo per un utente IAM) nella Guida per l'utente di IAM.
- (Non consigliato) Collega una policy direttamente a un utente o aggiungi un utente a un gruppo di utenti. Segui le istruzioni riportate nella pagina [Aggiunta di autorizzazioni a un utente \(console\)](#) nella Guida per l'utente di IAM.

Voglio consentire a persone esterne a me di accedere Account AWS alle mie risorse del Security Hub

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo.

Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Security Hub supporta queste funzionalità, vedere [Come AWS Security Hub funziona con IAM](#).
- Per informazioni su come garantire l'accesso alle risorse negli Account AWS che possiedi, consulta [Fornire l'accesso a un utente IAM in un altro Account AWS in tuo possesso](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWS di terze parti, consulta [Fornire l'accesso agli Account AWS di proprietà di terze parti](#) nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta [Fornire l'accesso a utenti autenticati esternamente \(Federazione delle identità\)](#) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consultare [Differenza tra i ruoli IAM e le policy basate su risorse](#) nella Guida per l'utente di IAM.

Convalida della conformità per AWS Security Hub

Revisori di terze parti valutano la sicurezza e la conformità di AWS Security Hub come parte di più programmi di conformità di AWS. Questi includono SOC, PCI, FedRAMP, HIPAA e altri.

Per un elenco di servizi AWS che rientrano nell'ambito di programmi di conformità specifici, consulta [Servizi AWS coperti dal programma di compliance](#). Per informazioni generali, consulta [Programmi di conformità di AWS](#).

Puoi scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta l'argomento [Download dei rapporti in AWS Artifact](#).

La tua responsabilità di conformità quando utilizzi Security Hub è determinata dalla sensibilità dei tuoi dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- [Guide Quick Start per la sicurezza e conformità](#): queste guide all'implementazione illustrano considerazioni relative all'architettura e forniscono fasi per l'implementazione di ambienti di base incentrati sulla sicurezza e sulla conformità su AWS.

- [Risorse per la conformità di AWS](#): questa raccolta di workbook e guide potrebbe essere utile al settore e alla posizione.
- [AWS Config](#): questo servizio AWS valuta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti di settore.
- [AWS Security Hub](#): questo servizio AWS fornisce una visione completa dello stato di sicurezza all'interno di AWS che consente di verificare la conformità con gli standard e le best practice di sicurezza del settore.

Resilienza nel AWS Security Hub

L'infrastruttura globale di AWS è basata su Regioni AWS e zone di disponibilità. Le regioni forniscono più zone di disponibilità fisicamente separate e isolate, connesse tramite reti altamente ridondanti, a bassa latenza e throughput elevato. Con le zone di disponibilità, è possibile progettare e gestire applicazioni e database che eseguono il failover automatico tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle Regioni AWS e le zone di disponibilità, consulta [Infrastruttura globale di AWS](#).

Sicurezza dell'infrastruttura nell'AWS Security Hub

Come servizio gestito, AWS Security Hub è protetto dalla sicurezza di rete globale AWS. Per informazioni sui servizi di sicurezza AWS e su come AWS protegge l'infrastruttura, consulta la pagina [Sicurezza del cloud AWS](#). Per progettare l'ambiente AWS utilizzando le best practice per la sicurezza dell'infrastruttura, consulta la pagina [Protezione dell'infrastruttura](#) nel Pilastro della sicurezza di AWS Well-Architected Framework.

Utilizzi chiamate API AWS pubblicate per accedere a Security Hub attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. In alternativa, è possibile utilizzare [AWS Security Token Service](#) (AWS STS) per generare le credenziali di sicurezza temporanee per sottoscrivere le richieste.

AWS Security Hub ed endpoint VPC dell'interfaccia (AWS PrivateLink)

È possibile stabilire una connessione privata tra il VPC e AWS Security Hub creando un endpoint VPC di interfaccia. Gli endpoint di [AWS PrivateLink](#) interfaccia sono basati su una tecnologia che consente di accedere privatamente alle API di Security Hub senza un gateway Internet, un dispositivo NAT, una connessione VPN o AWS una connessione Direct Connect. Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per comunicare con le API di Security Hub. Il traffico tra il tuo VPC e Security Hub non esce dalla rete Amazon.

Ogni endpoint dell'interfaccia è rappresentato da una o più [interfacce di rete elastiche](#) nelle sottoreti.

Per ulteriori informazioni, vedere [Interface VPC endpoints \(AWS PrivateLink\)](#) nella AWS PrivateLink Guida.

Considerazioni sugli endpoint VPC di Security Hub

Prima di configurare un endpoint VPC di interfaccia per Security Hub, assicurati di esaminare [le proprietà e le limitazioni degli endpoint di interfaccia nella Guida](#). AWS PrivateLink

Security Hub supporta l'effettuazione di chiamate a tutte le sue azioni API dal tuo VPC.

Note

Security Hub non supporta gli endpoint VPC nella regione Asia Pacifico (Osaka).

Creazione di un endpoint VPC di interfaccia per Security Hub

Puoi creare un endpoint VPC per il servizio Security Hub utilizzando la console Amazon VPC o il AWS Command Line Interface (). AWS CLI Per ulteriori informazioni, consulta la sezione [Creazione di un endpoint di interfaccia](#) nella Guida per l'utente di AWS PrivateLink.

Crea un endpoint VPC per Security Hub utilizzando il seguente nome di servizio:

- `com.amazonaws.region.securityhub`

Se abiliti il DNS privato per l'endpoint, puoi effettuare richieste API a Security Hub utilizzando il nome DNS predefinito per la regione, ad esempio. `securityhub.us-east-1.amazonaws.com`

Per ulteriori informazioni, vedere [Accedere a un servizio tramite un endpoint di interfaccia](#) nella AWS PrivateLink Guida.

Creazione di una politica degli endpoint VPC per Security Hub

Puoi allegare una policy sugli endpoint VPC che controlla l'accesso a Security Hub. La policy specifica le informazioni riportate di seguito:

- Il principale che può eseguire operazioni.
- Le operazioni che possono essere eseguite.
- Le risorse sui cui si possono eseguire operazioni.

Per ulteriori informazioni, vedere [Controllare l'accesso ai servizi con endpoint VPC](#) nella AWS PrivateLink Guida.

Esempio: policy degli endpoint VPC per le azioni di Security Hub

Di seguito è riportato un esempio di politica degli endpoint per Security Hub. Se collegata a un endpoint, questa policy consente l'accesso alle azioni di Security Hub elencate per tutti i responsabili di tutte le risorse.

```
{
  "Statement": [
    {
      "Principal": "*",
      "Effect": "Allow",
      "Action": [
        "securityhub:getFindings",
        "securityhub:getEnabledStandards",
        "securityhub:getInsights"
      ],
      "Resource": "*"
    }
  ]
}
```



```
]
}
```

Sottoreti condivise

Non puoi creare, descrivere, modificare o eliminare gli endpoint VPC nelle sottoreti condivise con te. Tuttavia, puoi utilizzare gli endpoint VPC in sottoreti condivise con te. Per informazioni sulla condivisione di VPC, consulta [Condividi il tuo VPC con altri account](#) nella Guida per l'utente di Amazon VPC.

Registrazione delle chiamate API AWS Security Hub con AWS CloudTrail

AWS Security Hub è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, ruolo o AWS servizio in Security Hub. CloudTrail acquisisce le chiamate API per Security Hub come eventi. Le chiamate acquisite includono chiamate dalla console Security Hub e chiamate in codice alle operazioni dell'API Security Hub. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Security Hub. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti sulla CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni CloudTrail raccolte, è possibile determinare la richiesta effettuata a Security Hub, l'indirizzo IP da cui è stata effettuata la richiesta, chi ha effettuato la richiesta, quando è stata effettuata e dettagli aggiuntivi.

Per saperne di più CloudTrail, incluso come configurarlo e abilitarlo, consulta la [Guida per l'AWS CloudTrail utente](#).

Informazioni su Security Hub in CloudTrail

CloudTrail è abilitato sul tuo Account AWS quando crei l'account. Quando si verifica un'attività di evento supportata in Security Hub, tale attività viene registrata in un CloudTrail evento insieme ad altri eventi di AWS servizio nella cronologia degli eventi. È possibile visualizzare, cercare e scaricare gli eventi recenti nell'account. Per ulteriori informazioni, vedere [Visualizzazione degli eventi con la cronologia degli CloudTrail eventi](#).

Per una registrazione continua degli eventi nel tuo account, inclusi gli eventi per Security Hub, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3. Per impostazione predefinita, quando crei un trail nella console, il trail si applica a tutte le regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurare altri AWS servizi per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta gli argomenti seguenti:

- [Panoramica della creazione di un percorso](#)
- [CloudTrail servizi e integrazioni supportati](#)
- [Configurazione delle notifiche Amazon SNS per CloudTrail](#)

- [Ricezione di file di CloudTrail registro da più regioni](#) e [ricezione di file di CloudTrail registro da più account](#)

Security Hub supporta la registrazione di tutte le azioni dell'API Security Hub come eventi nei CloudTrail registri. Per visualizzare un elenco delle operazioni del Security Hub, consulta il [riferimento all'API Security Hub](#).

Quando viene registrata l'attività per le seguenti azioni CloudTrail, il valore di `responseElements` è impostato `null` su. Ciò garantisce che le informazioni sensibili non siano incluse nei CloudTrail registri.

- `BatchImportFindings`
- `GetFindings`
- `GetInsights`
- `GetMembers`
- `UpdateFindings`

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente AWS Identity and Access Management (IAM) o `root`.
- Se la richiesta è stata effettuata con le credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro servizio AWS.

Per ulteriori informazioni, consulta [Elemento CloudTrail userIdentity](#).

Esempio: voci del file di registro di Security Hub

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta proveniente da qualsiasi fonte e include informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

L'esempio seguente mostra una voce di CloudTrail registro che illustra l'CreateInsightazione. In questo esempio, viene creata un'informazione dettagliata denominata Test Insight. L'attributo ResourceId viene specificato come l'aggregatore Group by (Raggruppa per) e non viene specificato alcun filtro opzionale per questa informazione dettagliata. Per ulteriori informazioni sulle informazioni dettagliate, consulta [Approfondimenti nel AWS Security Hub](#).

```
{
  "eventVersion": "1.05",
  "userIdentity": {
    "type": "IAMUser",
    "principalId": "AIDAJK6U5DS22IAVUI7BW",
    "arn": "arn:aws:iam::012345678901:user/TestUser",
    "accountId": "012345678901",
    "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
    "userName": "TestUser"
  },
  "eventTime": "2018-11-25T01:02:18Z",
  "eventSource": "securityhub.amazonaws.com",
  "eventName": "CreateInsight",
  "awsRegion": "us-west-2",
  "sourceIPAddress": "205.251.233.179",
  "userAgent": "aws-cli/1.11.76 Python/2.7.10 Darwin/17.7.0 botocore/1.5.39",
  "requestParameters": {
    "Filters": {},
    "ResultField": "ResourceId",
    "Name": "Test Insight"
  },
  "responseElements": {
    "InsightArn": "arn:aws:securityhub:us-west-2:0123456789010:insight/custom/f4c4890b-ac6b-4c26-95f9-e62cc46f3055"
  },
  "requestID": "c0ffffccd-f04d-11e8-93fc-ddcd14710066",
  "eventID": "3dabcebf-35b0-443f-a1a2-26e186ce23bf",
  "readOnly": false,
  "eventType": "AwsApiCall",
  "recipientAccountId": "012345678901"
}
```

Taggare le risorse del AWS Security Hub

Un tag è un'etichetta opzionale che è possibile definire e assegnare alle AWS risorse, inclusi alcuni tipi di risorse del AWS Security Hub. I tag possono aiutarti a identificare, classificare e gestire le risorse in diversi modi, ad esempio per scopo, proprietario, ambiente o altri criteri. Ad esempio, è possibile utilizzare i tag per distinguere le risorse, identificare le risorse che supportano determinati requisiti o flussi di lavoro di conformità o allocare i costi.

È possibile assegnare tag ai seguenti tipi di risorse del Security Hub: regole di automazione, politiche di configurazione e Hub risorsa.

Argomenti

- [Nozioni fondamentali sull'etichettatura](#)
- [Utilizzo di tag nelle policy IAM](#)
- [Aggiungere tag alle risorse del AWS Security Hub](#)
- [Revisione dei tag per le risorse del AWS Security Hub](#)
- [Modifica dei tag per le risorse del AWS Security Hub](#)
- [Rimuovere i tag dalle risorse del AWS Security Hub](#)

Nozioni fondamentali sull'etichettatura


Una risorsa può avere fino a 50 tag. Ogni tag è composto da una chiave di tag obbligatoria e da un valore di tag opzionale, entrambi definibili dall'utente. Una chiave di tag è un'etichetta generale che funge da categoria per un valore di tag più specifico. Un valore di tag funge da descrittore di una chiave di tag.

Ad esempio, se si creano regole di automazione diverse per ambienti diversi (un set di regole di automazione per gli account di test e un altro per gli account di produzione), è possibile assegnare una chiave di Environment tag a tali regole. Il valore del tag associato potrebbe Test riferirsi alle regole associate agli account di test e alle regole associate Prod agli account di produzione e alle unità organizzative.

Quando definisci e assegni i tag alle risorse del AWS Security Hub, tieni presente quanto segue:

- Ogni risorsa può avere un massimo di 50 tag.

- Per ogni risorsa, ogni chiave di tag deve essere unica e può avere un solo valore di tag.
- I valori e le chiavi dei tag rispettano la distinzione tra maiuscole e minuscole. Come best practice, ti consigliamo di definire una strategia per utilizzare i tag in maiuscolo e di implementarla in modo coerente tra le tue risorse.
- Una chiave tag può contenere un massimo di 128 caratteri UTF-8. Il valore di un tag può contenere un massimo di 256 caratteri UTF-8. I caratteri possono essere lettere, numeri, spazi o i seguenti simboli: `_.:/= + - @`
- Il `aws :` prefisso è riservato all'uso di AWS. Non puoi usarlo in nessuna chiave o valore di tag che definisci. Inoltre, non è possibile modificare o rimuovere le chiavi o i valori dei tag che utilizzano questo prefisso. I tag che utilizzano questo prefisso non vengono conteggiati per la quota di 50 tag per ogni risorsa.
- Tutti i tag che assegni sono disponibili solo per te Account AWS e solo nel gruppo Regione AWS in cui li assegni.
- Se si assegnano tag a una risorsa utilizzando Security Hub, i tag vengono applicati solo alla risorsa archiviata direttamente in Security Hub nel paese applicabile Regione AWS. Non vengono applicati alle risorse di supporto associate che Security Hub crea, utilizza o gestisce per te in altri Servizi AWS. Ad esempio, se assegni tag a una regola di automazione che aggiorna i risultati relativi ad Amazon Simple Storage Service (Amazon S3), i tag vengono applicati solo alla regola di automazione in Security Hub per la regione specificata. Non vengono applicati ai tuoi bucket S3. Per assegnare tag anche a una risorsa associata, puoi utilizzare AWS Resource Groups o Servizio AWS quello che memorizza la risorsa, ad esempio Amazon S3 per un bucket S3. L'assegnazione di tag alle risorse associate può aiutarti a identificare le risorse di supporto per le risorse del Security Hub.
- Se si elimina una risorsa, vengono eliminati anche tutti i tag assegnati alla risorsa.

 Important

Non archiviate dati riservati o di altro tipo nei tag. I tag sono accessibili da molti Servizi AWS, tra cui AWS Billing and Cost Management. Non sono destinati a essere utilizzati per dati sensibili.

Per aggiungere e gestire i tag per le risorse di Security Hub, puoi utilizzare la console Security Hub, l'API Security Hub o l'API AWS Resource Groups Tagging. Con Security Hub, puoi aggiungere tag a una risorsa quando la crei. È inoltre possibile aggiungere e gestire tag per singole risorse esistenti.

Con Resource Groups, puoi aggiungere e gestire tag in blocco per più risorse esistenti che coprono più aree Servizi AWS, incluso Security Hub.

Per ulteriori suggerimenti e best practice sull'etichettatura, consulta [Tagging your AWS resources nella Tagging Resources](#) User Guide. AWS

Utilizzo di tag nelle policy IAM

Dopo aver iniziato a taggare le risorse, puoi definire autorizzazioni a livello di risorsa basate su tag nelle policy (IAM). AWS Identity and Access Management Utilizzando i tag in questo modo, puoi implementare un controllo granulare su quali utenti e ruoli all'interno dell'azienda Account AWS sono autorizzati a creare e contrassegnare risorse e quali utenti e ruoli sono autorizzati ad aggiungere, modificare e rimuovere tag più in generale. Per controllare l'accesso in base ai tag, puoi utilizzare le [chiavi di condizione relative ai tag](#) nell'[elemento Condition](#) delle politiche IAM.

Ad esempio, puoi creare una policy IAM che consenta a un utente di avere accesso completo a tutte le risorse del AWS Security Hub, se il Owner tag della risorsa specifica il suo nome utente:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ModifyResourceIfOwner",
      "Effect": "Allow",
      "Action": "securityhub:*",
      "Resource": "*",
      "Condition": {
        "StringEqualsIgnoreCase": {"aws:ResourceTag/Owner": "${aws:username}"}
      }
    }
  ]
}
```

Se vengono definite autorizzazioni a livello di risorsa basate su tag, le autorizzazioni diventano subito effettive. Ciò significa che le risorse sono più sicure non appena vengono create e che è possibile avviare rapidamente l'applicazione di tag alle nuove risorse. È inoltre possibile utilizzare le autorizzazioni a livello di risorsa per controllare quali chiavi e valori di tag possono essere associati a risorse nuove ed esistenti. Per ulteriori informazioni, consulta [Controllo dell'accesso alle risorse AWS mediante i tag delle risorse](#) nella Guida per l'utente di IAM.

Aggiungere tag alle risorse del AWS Security Hub

Per aggiungere tag a una singola risorsa AWS Security Hub, puoi utilizzare la console Security Hub o l'API Security Hub. La console non supporta l'aggiunta di tag alla Hub risorsa.

Per aggiungere tag a più risorse Security Hub contemporaneamente, utilizza le operazioni di tagging dell'API [AWS Resource Groups Tagging](#).

Important

L'aggiunta di tag a una risorsa può influire sull'accesso alla risorsa. Prima di aggiungere un tag a una risorsa, esamina le politiche AWS Identity and Access Management (IAM) che potrebbero utilizzare i tag per controllare l'accesso alle risorse.

Console

Per aggiungere un tag a una risorsa

Quando si crea una regola di automazione o una politica di configurazione, la console Security Hub offre opzioni per aggiungere tag. È possibile fornire la chiave e il valore del tag nella sezione Tag.

Security Hub API & AWS CLI

Per aggiungere un tag a una risorsa

Per creare una risorsa e aggiungervi uno o più tag a livello di codice, utilizzate l'operazione appropriata per il tipo di risorsa che desiderate creare:

- Per creare una politica di configurazione e aggiungervi uno o più tag, richiamate l'[CreateConfigurationPolicy](#) API o, se utilizzate la AWS CLI, eseguite il comando. [create-configuration-policy](#)
- Per creare una regola di automazione e aggiungervi uno o più tag, richiama l'[CreateAutomationRule](#) API o, se utilizzi la AWS CLI, esegui il comando. [create-automation-rule](#)
- Per abilitare Security Hub e aggiungere uno o più tag alla tua Hub risorsa, richiama l'[EnableSecurityHub](#) API o, se stai usando il AWS Command Line Interface (AWS CLI), esegui il [enable-security-hub](#) comando.

Nella richiesta, utilizzate il `tags` parametro per specificare la chiave del tag e il valore del tag opzionale per ogni tag da aggiungere alla risorsa. Il `tags` parametro specifica una matrice di oggetti. Ogni oggetto specifica una chiave di tag e il relativo valore di tag associato.

Per aggiungere uno o più tag a una risorsa esistente, utilizza l'[TagResource](#) operazione dell'API Security Hub o, se utilizzi il AWS CLI, esegui il comando [tag-resource](#). Nella richiesta, specifica l'Amazon Resource Name (ARN) della risorsa a cui desideri aggiungere un tag. Utilizza il `tags` parametro per specificare la chiave del tag (`key`) e il valore del tag opzionale (`value`) per ogni tag da aggiungere. Il `tags` parametro specifica una matrice di oggetti, un oggetto per ogni chiave di tag e il valore del tag associato.

Ad esempio, il AWS CLI comando seguente aggiunge una chiave di `Environment` tag con un valore di `Prod` tag alla politica di configurazione specificata. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di riga rovesciata (`\`) per migliorare la leggibilità.

Esempio di comando CLI:

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags key=Environment,value=Prod
```

Dove:

- `resource-arn` specifica l'ARN della politica di configurazione a cui aggiungere un tag.
- `Environment` è la chiave del tag da aggiungere alla regola.
- `Prod` è il valore del tag per la chiave del tag specificata (`Environment`).

Nell'esempio seguente, il comando aggiunge diversi tag alla politica di configurazione.

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags key=Environment,value=Prod key=CostCenter,value=12345 key=Owner,value=jane-  
doe
```

Per ogni oggetto di una `tags` matrice, sono obbligatori `key` sia gli `value` argomenti che. Tuttavia, il valore dell'`value` argomento può essere una stringa vuota. Se non desiderate associare un

valore di tag a una chiave di tag, non specificate un valore per l'argomento. Ad esempio, il comando seguente aggiunge una chiave di Owner tag senza alcun valore di tag associato:

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags key=Owner,value=
```

Se un'operazione di tagging ha esito positivo, Security Hub restituisce una risposta HTTP 200 vuota. Altrimenti, Security Hub restituisce una risposta HTTP 4xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Revisione dei tag per le risorse del AWS Security Hub

È possibile esaminare i tag (sia chiavi che valori dei tag) per una regola di automazione o una politica di configurazione di Security Hub utilizzando la console Security Hub o l'API Security Hub. La console non supporta la revisione dei tag per la Hub risorsa.

Per esaminare i tag per più risorse Security Hub contemporaneamente, utilizza le operazioni di tagging dell'API [AWS Resource Groups Tagging](#).

Console

Per esaminare i tag di una risorsa

1. Utilizzando le credenziali dell'amministratore del Security Hub, aprire la console AWS Security Hub all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. A seconda del tipo di risorsa a cui vuoi aggiungere un tag, esegui una delle seguenti operazioni:
 - Per esaminare i tag per una regola di automazione, scegli Automazioni nel riquadro di navigazione. Quindi, scegli una regola di automazione.
 - Per esaminare i tag relativi a una politica di configurazione, scegli Configurazione nel riquadro di navigazione. Quindi, nella scheda Politiche, seleziona l'opzione accanto a una politica di configurazione. Si apre un pannello laterale che mostra il numero di tag assegnati alla politica. Puoi espandere l'intestazione Tags per visualizzare le chiavi e i valori dei tag.

La sezione Tag elenca tutti i tag attualmente assegnati alla risorsa.

Security Hub API & AWS CLI

Per rivedere i tag di una risorsa

Per recuperare e rivedere i tag di una risorsa esistente, richiama l'[ListTagsForResource](#) API. Nella tua richiesta, utilizza il `resourceArn` parametro per specificare l'Amazon Resource Name (ARN) della risorsa.

Se si utilizza il AWS CLI, eseguire il [list-tags-for-resource](#) comando e utilizzare il `resource-arn` parametro per specificare l'ARN della risorsa. Per esempio:

```
$ aws securityhub list-tags-for-resource --resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/a1b2c3d4-5678-90ab-cdef-EXAMPLE11111
```

Se l'operazione ha esito positivo, Security Hub restituisce un `tags` array. Ogni oggetto dell'array specifica un tag (sia la chiave del tag che il valore del tag) attualmente assegnato alla risorsa. Per esempio:

```
{
  "tags": [
    {
      "key": "Environment",
      "value": "Prod"
    },
    {
      "key": "CostCenter",
      "value": "12345"
    },
    {
      "key": "Owner",
      "value": ""
    }
  ]
}
```

Dove `Environment` e `CostCenter` `Owner` sono le chiavi dei tag assegnate alla risorsa. `Prod` è il valore del tag associato alla chiave del `Environment` tag. `12345` è il valore del tag associato alla chiave del `CostCenter` tag. La chiave `Owner` tag non ha un valore di tag associato.

Per recuperare un elenco di tutte le risorse del Security Hub che dispongono di tag e di tutti i tag assegnati a ciascuna di tali risorse, utilizza il [GetResources](#) funzionamento dell'API AWS Resource Groups Tagging. Nella richiesta, imposta il valore del `ResourceTypeFilters` parametro su `securityhub`. A tale scopo AWS CLI, eseguite il comando [get-resources](#) e impostate il valore del `resource-type-filters` parametro su `securityhub`. Per esempio:

```
$ aws resourcegroupstaggingapi get-resources --resource-type-filters "securityhub"
```

Se l'operazione ha esito positivo, Resource Groups restituisce un `ResourceTagMappingList` array. L'array contiene un oggetto per ogni risorsa Security Hub con tag. Ogni oggetto specifica l'ARN di una risorsa Security Hub e le chiavi e i valori dei tag assegnati alla risorsa.

Modifica dei tag per le risorse del AWS Security Hub

Per modificare i tag (chiavi o valori dei tag) per una risorsa AWS Security Hub, puoi utilizzare l'API Security Hub. La console Security Hub attualmente non supporta la modifica dei tag.

Per modificare i tag per più risorse Security Hub contemporaneamente, utilizza le operazioni di tagging dell'API [AWS Resource Groups Tagging](#).

Important

La modifica dei tag per una risorsa può influire sull'accesso alla risorsa. Prima di modificare la chiave o il valore di un tag per una risorsa, esamina le politiche AWS Identity and Access Management (IAM) che potrebbero utilizzare il tag per controllare l'accesso alle risorse.

Security Hub API & AWS CLI

Per modificare i tag di una risorsa

Quando modificate un tag per una risorsa a livello di codice, sovrascrivete il tag esistente con nuovi valori. Pertanto, il modo migliore per modificare un tag dipende dal fatto che si desideri modificare una chiave di tag, un valore di tag o entrambi. Per modificare una chiave di tag, [rimuovi il tag corrente](#) e [aggiungi un nuovo tag](#).

Per modificare o rimuovere solo il valore del tag associato a una chiave di tag, sovrascrivi il valore esistente utilizzando il [TagResource](#) funzionamento dell'API Security Hub. Se utilizzi il AWS CLI,

esegui il comando [tag-resource](#). Nella richiesta, specifica l'Amazon Resource Name (ARN) della risorsa di cui desideri modificare o rimuovere il valore del tag.

Per modificare il valore di un tag, utilizza il `tags` parametro per specificare la chiave del tag di cui desideri modificare il valore del tag. È inoltre necessario specificare il nuovo valore del tag per la chiave. Ad esempio, il AWS CLI comando seguente modifica il valore del tag da `Prod` a `Test` per la chiave di `Environment` tag assegnata alla regola di automazione specificata. Questo esempio è formattato per Linux, macOS o Unix e utilizza il carattere di continuazione di riga rovesciata (`\`) per migliorare la leggibilità.

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags key=Environment,value=Test
```

Dove:

- `resource-arn` specifica l'ARN della politica di configurazione.
- `Environment` è la chiave del tag associata al valore del tag da modificare.
- `Test` è il nuovo valore del tag per la chiave di tag specificata (`Environment`).

Per rimuovere un valore di tag da una chiave di tag, non specificate un valore per l'`value` argomento della chiave nel `tags` parametro. Per esempio:

```
$ aws securityhub tag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tags key=owner,value=
```

Se l'operazione ha esito positivo, Security Hub restituisce una risposta HTTP 200 vuota. Altrimenti, Security Hub restituisce una risposta HTTP 4xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Rimuovere i tag dalle risorse del AWS Security Hub

Per rimuovere i tag da una risorsa AWS Security Hub, puoi utilizzare l'API Security Hub. La console Security Hub attualmente non supporta la rimozione dei tag.

Per rimuovere i tag da più risorse Security Hub contemporaneamente, utilizza le operazioni di tagging dell'API [AWS Resource Groups Tagging](#).

Important

La rimozione dei tag da una risorsa può influire sull'accesso alla risorsa. Prima di rimuovere un tag, esamina le politiche AWS Identity and Access Management (IAM) che potrebbero utilizzare il tag per controllare l'accesso alle risorse.

Security Hub API & AWS CLI

Per rimuovere i tag da una risorsa

Per rimuovere uno o più tag da una risorsa a livello di codice, utilizza il [UntagResource](#) funzionamento dell'API Security Hub. Nella tua richiesta, utilizza il `resourceArn` parametro per specificare l'Amazon Resource Name (ARN) della risorsa da cui rimuovere un tag. Usa il `tagKeys` parametro per specificare la chiave del tag da rimuovere. Per rimuovere più tag, aggiungete il `tagKeys` parametro e l'argomento per ogni tag da rimuovere, separati da una e commerciale (&), ad esempio. `tagKeys=key1&tagKeys=key2` Per rimuovere solo un valore di tag specifico (non una chiave di tag) da una risorsa, [modifica il tag anziché rimuovere il tag](#).

Se utilizzi il AWS CLI, esegui il comando [untag-resource](#) per rimuovere uno o più tag da una risorsa. Per il `resource-arn` parametro, specificate l'ARN della risorsa da cui rimuovere un tag. Utilizzate il `tag-keys` parametro per specificare la chiave del tag da rimuovere. Ad esempio, il comando seguente rimuove il `Environment` tag (sia la chiave del tag che il valore del tag) dalla politica di configurazione specificata:

```
$ aws securityhub untag-resource \  
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE1111 \  
--tag-keys Environment
```

Dove `resource-arn` specifica l'ARN della politica di configurazione da cui rimuovere un tag `Environment` ed è la chiave del tag da rimuovere.

Per rimuovere più tag da una risorsa, aggiungi ogni chiave di tag aggiuntiva come argomento per il `tag-keys` parametro. Per esempio:

```
$ aws securityhub untag-resource \  

```

```
--resource-arn arn:aws:securityhub:us-east-1:123456789012:configuration-policy/  
a1b2c3d4-5678-90ab-cdef-EXAMPLE11111 \  
--tag-keys Environment Owner
```

Se l'operazione ha esito positivo, Security Hub restituisce una risposta HTTP 200 vuota. Altrimenti, Security Hub restituisce una risposta HTTP 4 xx o 500 che indica il motivo per cui l'operazione non è riuscita.

Quote Security Hub

Hai Account AWS determinate quote predefinite, precedentemente denominate limiti, per ciascuna di esse. Servizio AWS Queste quote rappresentano il numero massimo di risorse o operazioni di servizio per l'account. Questo argomento contiene collegamenti alle quote che si applicano alle risorse e alle operazioni AWS di Security Hub per il tuo account. Salvo diversa indicazione, ogni quota si applica all'account di ciascuno di essi Regione AWS.

Alcune quote possono essere aumentate, mentre altre no. Per richiedere un aumento di una quota, usa la console [Service Quotas](#). Per informazioni su come richiedere un aumento, consulta [Richiedere un aumento della quota](#) nella Service Quotas User Guide. Se una quota non è disponibile nella console Service Quotas, utilizza il [modulo di aumento del limite di servizio](#) su AWS Support Center Console per richiedere un aumento della quota.

Quote massime

Per un elenco delle quote che si applicano alle risorse del Security Hub, vedere [Endpoint e quote del AWS Security Hub](#) nel. Riferimenti generali di AWS

Quote tariffa

Per un elenco delle quote che si applicano alle operazioni dell'API Security Hub, consulta il [riferimento all'API AWS Security Hub](#).

Se la configurazione è stata effettuata [Aggregazione tra regioni](#), una chiamata ha un BatchUpdateFindings impatto sulle regioni collegate e sulla regione di aggregazione. BatchImportFindings L'GetFindings operazione recupera i risultati dalle regioni collegate e dalla regione di aggregazione. Tuttavia, le UpdateStandardsControl operazioni BatchEnableStandards e sono specifiche della regione.

Limiti regionali del Security Hub

Alcune funzionalità AWS di Security Hub sono disponibili solo in alcuni Regioni AWS. Le seguenti sezioni specificano questi limiti regionali.

Per un elenco delle regioni in cui è disponibile Security Hub, consulta [Endpoint e quote del AWS Security Hub](#) in. Riferimenti generali di AWS

Restrizioni di aggregazione tra regioni

In AWS GovCloud (US), l'[aggregazione tra regioni](#) è disponibile solo per i risultati, la ricerca di aggiornamenti e approfondimenti. AWS GovCloud (US) In particolare, puoi aggregare i risultati, trovare aggiornamenti e approfondimenti solo tra AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali).

Nelle regioni cinesi, l'aggregazione interregionale è disponibile per i risultati, gli aggiornamenti dei risultati e gli approfondimenti solo nelle regioni cinesi. In particolare, puoi aggregare risultati, aggiornamenti e approfondimenti solo tra Cina (Pechino) e Cina (Ningxia).

Non puoi utilizzare una regione disattivata per impostazione predefinita come regione di aggregazione. Per un elenco delle regioni disabilitate per impostazione predefinita, vedi [Abilitazione di una regione](#) in. Riferimenti generali di AWS

Disponibilità di integrazioni per regione

Alcune integrazioni non sono disponibili in tutte le regioni. Se un'integrazione non è disponibile in una regione specifica, non viene elencata nella pagina Integrazioni della console Security Hub quando scegli quella regione.

Integrazioni supportate in Cina (Pechino) e Cina (Ningxia)

[Le regioni Cina \(Pechino\) e Cina \(Ningxia\) supportano solo le seguenti integrazioni con i servizi: AWS](#)

- AWS Firewall Manager
- Amazon GuardDuty
- AWS Identity and Access Management Access Analyzer

- Amazon Inspector
- AWS IoT Device Defender
- AWS Systems Manager Explorer
- AWS Systems Manager OpsCenter
- AWS Systems Manager Gestore di patch

Le regioni Cina (Pechino) e Cina (Ningxia) supportano solo le seguenti integrazioni di [terze parti](#):

- Cloud Custodian
- FireEye Helix
- Helecloud
- IBM QRadar
- PagerDuty
- Palo Alto Networks Cortex XSOAR
- Palo Alto Networks VM-Series
- Prowler
- RSA Archer
- Splunk Enterprise
- Splunk Phantom
- ThreatModeler

Integrazioni supportate in AWS GovCloud (Stati Uniti orientali) e (Stati Uniti occidentali) AWS GovCloud

[Le regioni AWS GovCloud \(Stati Uniti orientali\) e AWS GovCloud \(Stati Uniti occidentali\) supportano solo le seguenti integrazioni con i servizi: AWS](#)

- AWS Config
- Amazon Detective
- AWS Firewall Manager
- Amazon GuardDuty
- AWS Health

- Sistema di analisi degli accessi AWS IAM
- Amazon Inspector
- AWS IoT Device Defender

Le regioni AWS GovCloud (Stati Uniti orientali) e AWS GovCloud (Stati Uniti occidentali) supportano solo le seguenti integrazioni [di terze parti](#):

- Atlassian Jira Service Management
- Atlassian Jira Service Management Cloud
- Atlassian OpsGenie
- Caveonix Cloud
- Cloud Custodian
- Cloud Storage Security Antivirus for Amazon S3
- CrowdStrike Falcon
- FireEye Helix
- Forcepoint CASB
- Forcepoint DLP
- Forcepoint NGFW
- Fugue
- Kion
- MicroFocus ArcSight
- NETSCOUT Cyber Investigator
- PagerDuty
- Palo Alto Networks – Prisma Cloud Compute
- Palo Alto Networks – Prisma Cloud Enterprise
- Palo Alto Networks – VM-Series(disponibile solo negli Stati Uniti occidentali AWS GovCloud)
- Prowler
- Rackspace Technology – Cloud Native Security
- Rapid7 InsightConnect
- RSA Archer
- SecureCloudDb

- ServiceNow ITSM
- Slack
- ThreatModeler
- Vectra AI Cognito Detect

Disponibilità degli standard per regione

Service-Managed Standard: AWS Control Tower è disponibile solo nelle regioni che AWS Control Tower supportano, tra cui. AWS GovCloud (US) Per un elenco delle regioni che lo AWS Control Tower supportano, consulta [How Regioni AWS Work With AWS Control Tower nella Guida](#) per l'AWS Control Tower utente.

Il AWS Resource Tagging Standard non è disponibile in Canada occidentale (Calgary), Cina e. AWS GovCloud (US)

Altri standard di sicurezza sono disponibili in tutte le regioni in cui è disponibile Security Hub.

Disponibilità dei controlli per regione

I controlli del Security Hub potrebbero non essere disponibili in tutte le regioni. Per visualizzare un elenco dei controlli non disponibili in ogni regione, consulta [Limiti regionali sui controlli](#). Un controllo non viene visualizzato nell'elenco dei controlli nella console Security Hub se non è disponibile nella regione a cui hai effettuato l'accesso. L'eccezione è se hai effettuato l'accesso a una regione di aggregazione. In tal caso, puoi visualizzare i controlli disponibili nella regione di aggregazione o in una o più regioni collegate.

Limiti regionali sui controlli

AWS I controlli del Security Hub potrebbero non essere disponibili tutti Regioni AWS. Questa pagina mostra quali controlli non sono disponibili in regioni specifiche. Un controllo non viene visualizzato nell'elenco dei controlli nella console Security Hub se non è disponibile nella regione a cui hai effettuato l'accesso. L'eccezione è se hai effettuato l'accesso a una regione di aggregazione. In tal caso, puoi visualizzare i controlli disponibili nella regione di aggregazione o in una o più regioni collegate.

Indice

- [Stati Uniti orientali \(Virginia settentrionale\)](#)
- [Stati Uniti orientali \(Ohio\)](#)
- [Stati Uniti occidentali \(California settentrionale\)](#)
- [US West \(Oregon\)](#)
- [Africa \(Città del Capo\)](#)
- [Asia Pacifico \(Hong Kong\)](#)
- [Asia Pacifico \(Hyderabad\)](#)
- [Asia Pacifico \(Giacarta\)](#)
- [Asia Pacifico \(Mumbai\)](#)
- [Asia Pacifico \(Melbourne\)](#)
- [Asia Pacifico \(Osaka-Locale\)](#)
- [Asia Pacifico \(Seoul\)](#)
- [Asia Pacifico \(Singapore\)](#)
- [Asia Pacifico \(Sydney\)](#)
- [Asia Pacifico \(Tokyo\)](#)
- [Canada \(Centrale\)](#)
- [Cina \(Pechino\)](#)
- [Cina \(Ningxia\)](#)
- [Europa \(Francoforte\)](#)
- [Europa \(Irlanda\)](#)
- [Europa \(Londra\)](#)
- [Europa \(Milano\)](#)
- [Europa \(Parigi\)](#)
- [Europa \(Spagna\)](#)
- [Europa \(Stoccolma\)](#)
- [Europa \(Zurigo\)](#)
- [Israele \(Tel Aviv\)](#)
- [Medio Oriente \(Bahrein\)](#)
- [Medio Oriente \(Emirati Arabi Uniti\)](#)

- [Sud America \(San Paolo\)](#)
- [AWS GovCloud \(Stati Uniti orientali\)](#)
- [AWS GovCloud \(Stati Uniti occidentali\)](#)

Stati Uniti orientali (Virginia settentrionale)

I seguenti controlli non sono supportati negli Stati Uniti orientali (Virginia settentrionale).

- [\[DataFirehose.1\]](#) I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi
- [\[DMS.10\]](#) Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [\[DMS.11\]](#) Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato
- [\[DMS.12\]](#) Gli endpoint DMS per Redis devono avere TLS abilitato
- [\[DynamoDB.7\]](#) I cluster DynamoDB Accelerator devono essere crittografati in transito
- [\[EFS.6\]](#) I target di montaggio EFS non devono essere associati a una sottorete pubblica
- [\[EKS.3\]](#) I cluster EKS devono utilizzare segreti Kubernetes crittografati
- [\[ElastiCache.4\]](#) ElastiCache per i gruppi di replica Redis deve essere crittografato a riposo
- [\[ElastiCache.5\]](#) ElastiCache per i gruppi di replica Redis devono essere crittografati in transito
- [\[ElastiCache.6\]](#) ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH
- [\[ElastiCache.7\]](#) ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito
- [\[FSX.2\]](#) I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [\[GlobalAccelerator.1\]](#) Gli acceleratori Global Accelerator devono essere etichettati
- [\[MQ.2\]](#) I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [\[MQ.3\]](#) I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie
- I OpenSearch domini [\[Opensearch.11\]](#) devono avere almeno tre nodi primari dedicati
- [\[Redshift.15\]](#) I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate
- [\[SageMaker.4\]](#) Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1
- [\[ServiceCatalog.1\]](#) I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS

- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)

Stati Uniti orientali (Ohio)

I seguenti controlli non sono supportati negli Stati Uniti orientali (Ohio).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)

- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Stati Uniti occidentali (California settentrionale)

I seguenti controlli non sono supportati negli Stati Uniti occidentali (California settentrionale).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)

- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)

- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

US West (Oregon)

I seguenti controlli non sono supportati negli Stati Uniti occidentali (Oregon).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)

- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)

- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Africa (Città del Capo)

I seguenti controlli non sono supportati in Africa (Città del Capo).

- [\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)
- [\[ApiGateway.1\] API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati](#)
- [\[AppSync.2\] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata](#)
- [\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)
- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)

- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.3\] I volumi Amazon EBS collegati devono essere crittografati a riposo](#)
- [\[EC2.4\] Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato](#)
- [\[EC2.8\] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 \(IMDSv2\)](#)
- [\[EC2.12\] Gli EIP Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22](#)
- [\[EC2.14\] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)
- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)

- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[ELB.1\] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS](#)
- [\[ELB.2\] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager](#)
- [\[ELB.4\] L'Application Load Balancer deve essere configurato per eliminare le intestazioni http](#)
- [\[ELB.8\] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita con una durata elevata AWS Config](#)
- [\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF](#)
- [\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)
- [\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)
- [\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)
- [\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)
- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)

- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)
- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)
- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.1\] L'istanza RDS deve essere privata](#)
- [\[RDS.9\] Le istanze DB RDS devono pubblicare i log nei registri CloudWatch](#)
- [\[RDS.10\] L'autenticazione IAM deve essere configurata per le istanze RDS](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[Redshift.3\] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)
- [\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)

- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

Asia Pacifico (Hong Kong)

I seguenti controlli non sono supportati in Asia Pacifico (Hong Kong).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)

- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.10\] L'autenticazione IAM deve essere configurata per le istanze RDS](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)

- [\[SES.1\] Gli elenchi di contatti SES devono essere etichettati](#)
- [\[SES.2\] I set di configurazione SES devono essere etichettati](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Asia Pacific (Hyderabad)

I seguenti controlli non sono supportati in Asia Pacifico (Hyderabad).

- [\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)
- [\[ACM.2\] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit](#)
- [\[Account.2\] Account AWS deve far parte di un'organizzazione AWS Organizations](#)
- [\[ApiGateway.1\] API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati](#)
- [\[ApiGateway.2\] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend](#)
- [\[ApiGateway.3\] Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray](#)
- [\[ApiGateway.4\] L'API Gateway deve essere associato a un ACL Web WAF](#)
- [\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione](#)
- [\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages](#)
- [\[AppSync.2\] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata](#)
- [\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)
- [\[Athena.2\] I cataloghi di dati Athena devono essere etichettati](#)

- [\[Athena.3\] I gruppi di lavoro Athena devono essere etichettati](#)
- [\[AutoScaling.1\] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB](#)
- [\[Autoscaling.5\] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici](#)
- [\[Backup.1\] i punti di AWS Backup ripristino devono essere crittografati a riposo](#)
- [\[Backup.2\] i punti di AWS Backup ripristino devono essere etichettati](#)
- [I AWS Backup vault \[Backup.3\] devono essere etichettati](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[Backup.5\] i piani di AWS Backup backup devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CloudTrail.6\] Assicurati che il bucket S3 utilizzato per archiviare i log non sia accessibile al pubblico CloudTrail](#)
- [\[CloudTrail.7\] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)

- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)
- [\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)
- [\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)
- [\[DMS.2\] I certificati DMS devono essere etichettati](#)
- [\[DMS.3\] Le sottoscrizioni agli eventi DMS devono essere contrassegnate](#)
- [\[DMS.4\] Le istanze di replica DMS devono essere contrassegnate](#)
- [\[DMS.5\] I sottoreti di replica DMS devono essere etichettati](#)
- [\[DMS.6\] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato](#)
- [\[DMS.7\] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata](#)
- [\[DMS.8\] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata](#)
- [\[DMS.9\] Gli endpoint DMS devono utilizzare SSL](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)

- [\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22](#)
- [\[EC2.14\] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389](#)
- [\[EC2.18\] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[EC2.25\] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete](#)
- [\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)
- [\[EC2.34\] Le tabelle delle rotte dei gateway di transito EC2 devono essere etichettate](#)
- [\[EC2.40\] I gateway NAT EC2 devono essere etichettati](#)
- [\[EC2.48\] I log di flusso di Amazon VPC devono essere etichettati](#)
- [\[EC2.51\] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata](#)
- [\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)
- [\[ECR.2\] I repository privati ECR devono avere l'immutabilità dei tag configurata](#)
- [\[ECR.3\] I repository ECR devono avere almeno una politica del ciclo di vita configurata](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)
- [\[ECS.9\] Le definizioni delle attività ECS devono avere una configurazione di registrazione](#)
- [\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)
- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)
- [\[EFS.3\] I punti di accesso EFS devono applicare una directory principale](#)
- [\[EFS.4\] I punti di accesso EFS devono applicare un'identità utente](#)
- [\[EFS.5\] I punti di accesso EFS devono essere etichettati](#)

- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.2\] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[ELB.5\] La registrazione delle applicazioni e dei sistemi Classic Load Balancers deve essere abilitata](#)
- [\[ELB.13\] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità](#)
- [\[ELB.14\] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)
- [\[ElastiCache.6\] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH](#)
- [\[ElastiCache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)
- [\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)
- [\[ES.1\] I domini Elasticsearch devono avere la crittografia a riposo abilitata](#)
- [\[ES.2\] I domini Elasticsearch non devono essere accessibili al pubblico](#)
- [\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)
- [\[ES.4\] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch](#)
- [\[EventBridge.2\] i bus EventBridge degli eventi devono essere etichettati](#)
- [\[EventBridge.3\] i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)

- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[Glue.1\] i AWS Glue lavori devono essere etichettati](#)
- [\[GuardDuty.2\] GuardDuty i filtri devono essere etichettati](#)
- [\[GuardDuty.3\] Gli GuardDuty IPSet devono essere etichettati](#)
- [\[GuardDuty.4\] i GuardDuty rilevatori devono essere etichettati](#)
- [\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)
- [\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)
- [\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)
- [\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)
- [\[IAM.8\] Le credenziali utente IAM non utilizzate devono essere rimosse](#)
- [\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)
- [\[IAM.19\] L'MFA deve essere abilitata per tutti gli utenti IAM](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)
- [\[IAM.22\] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse](#)
- [\[IAM.24\] I ruoli IAM devono essere etichettati](#)
- [\[IAM.25\] Gli utenti IAM devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IAM.27\] Le identità IAM non devono avere la policy allegata AWSCloudShellFullAccess](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)
- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)
- [\[KMS.1\] Le politiche gestite dai clienti di IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS](#)

- [\[KMS.2\] I principali IAM non devono disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS](#)
- [\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)
- [\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)
- [\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[MQ.4\] I broker Amazon MQ devono essere etichettati](#)
- [\[MQ.5\] I broker ActiveMQ devono utilizzare la modalità di distribuzione attiva/standby](#)
- [\[MQ.6\] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster](#)
- [\[MSK.1\] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker](#)
- [\[MSK.2\] Per i cluster MSK dovrebbe essere configurato un monitoraggio avanzato](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)
- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.2\] La registrazione del Network Firewall deve essere abilitata](#)
- [\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)
- [\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)
- [\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)
- [\[NetworkFirewall.6\] Il gruppo di regole Stateless Network Firewall non deve essere vuoto](#)

- [\[NetworkFirewall.9\] I firewall Network Firewall devono avere la protezione da eliminazione abilitata](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)
- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)
- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)
- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [I OpenSearch domini \[Opensearch.9\] devono essere etichettati](#)
- [Nei OpenSearch domini \[Opensearch.10\] deve essere installato l'ultimo aggiornamento software](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.2\] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, in base alla durata PubliclyAccessible AWS Config](#)
- [\[RDS.7\] I cluster RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.9\] Le istanze DB RDS devono pubblicare i log nei registri CloudWatch](#)
- [\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)
- [\[RDS.16\] I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)
- [\[RDS.26\] Le istanze DB RDS devono essere protette da un piano di backup](#)
- [\[RDS.27\] I cluster RDS DB devono essere crittografati quando sono inattivi](#)
- [\[RDS.28\] I cluster RDS DB devono essere etichettati](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[RDS.34\] I cluster Aurora MySQL DB devono pubblicare i log di controllo nei registri CloudWatch](#)
- [\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)

- [\[Redshift.1\] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico](#)
- [\[Redshift.2\] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito](#)
- [\[Redshift.3\] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate](#)
- [\[Redshift.6\] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati](#)
- [\[Redshift.7\] I cluster Redshift devono utilizzare un routing VPC avanzato](#)
- [\[Redshift.10\] I cluster Redshift devono essere crittografati a riposo](#)
- [\[Redshift.12\] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[S3.6\] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS](#)
- [\[S3.17\] I bucket generici S3 devono essere crittografati quando sono inattivi con AWS KMS keys](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)
- [\[SageMaker.2\] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato](#)
- [\[SageMaker.3\] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[SES.1\] Gli elenchi di contatti SES devono essere etichettati](#)
- [\[SES.2\] I set di configurazione SES devono essere etichettati](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SNS.3\] Gli argomenti SNS devono essere etichettati](#)
- [\[SQS.1\] Le code di Amazon SQS devono essere crittografate quando sono inattive](#)
- [\[SQS.2\] Le code SQS devono essere etichettate](#)
- [\[SSM.1\] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager](#)
- [\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)

- [\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)
- [\[StepFunctions.1\] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata](#)
- [I AWS Transfer Family flussi di lavoro \[Transfer.1\] devono essere etichettati](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.2\] Le regole regionali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.4\] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.10\] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

Asia Pacifico (Giacarta)

I seguenti controlli non sono supportati in Asia Pacifico (Giacarta).

- [\[Account.2\] Account AWS deve far parte di un'organizzazione AWS Organizations](#)
- [\[ApiGateway.1\] API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati](#)
- [\[ApiGateway.2\] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend](#)
- [\[ApiGateway.3\] Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray](#)
- [\[ApiGateway.4\] L'API Gateway deve essere associato a un ACL Web WAF](#)
- [\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione](#)
- [\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages](#)
- [\[AppSync.2\] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata](#)

- [\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)
- [\[AutoScaling.3\] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 \(IMDSv2\)](#)
- [\[AutoScaling.6\] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità](#)
- [\[AutoScaling.9\] I gruppi di Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2](#)
- [\[Autoscaling.5\] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici](#)
- [\[Backup.1\] i punti di AWS Backup ripristino devono essere crittografati a riposo](#)
- [\[Backup.2\] i punti di AWS Backup ripristino devono essere etichettati](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[Backup.5\] i piani di AWS Backup backup devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CloudWatch.17\] le azioni di CloudWatch allarme devono essere attivate](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)

- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)
- [\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)
- [\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)
- [\[DMS.2\] I certificati DMS devono essere etichettati](#)
- [\[DMS.3\] Le sottoscrizioni agli eventi DMS devono essere contrassegnate](#)
- [\[DMS.4\] Le istanze di replica DMS devono essere contrassegnate](#)
- [\[DMS.5\] I sottoreti di replica DMS devono essere etichettati](#)
- [\[DMS.6\] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato](#)
- [\[DMS.7\] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata](#)
- [\[DMS.8\] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata](#)
- [\[DMS.9\] Gli endpoint DMS devono utilizzare SSL](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)

- [\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22](#)
- [\[EC2.14\] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389](#)
- [\[EC2.18\] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)
- [\[EC2.51\] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata](#)
- [\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)
- [\[ECR.2\] I repository privati ECR devono avere l'immutabilità dei tag configurata](#)
- [\[ECR.3\] I repository ECR devono avere almeno una politica del ciclo di vita configurata](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.2\] Ai servizi ECS non devono essere assegnati automaticamente indirizzi IP pubblici](#)
- [\[ECS.3\] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host](#)
- [\[ECS.4\] I contenitori ECS devono essere eseguiti come non privilegiati](#)
- [\[ECS.5\] I contenitori ECS devono essere limitati all'accesso in sola lettura ai filesystem root](#)
- [\[ECS.8\] I segreti non devono essere passati come variabili di ambiente del contenitore](#)
- [\[ECS.9\] Le definizioni delle attività ECS devono avere una configurazione di registrazione](#)
- [\[ECS.10\] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate](#)
- [\[ECS.12\] I cluster ECS devono utilizzare Container Insights](#)
- [\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)
- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)

- [\[EFS.3\] I punti di accesso EFS devono applicare una directory principale](#)
- [\[EFS.4\] I punti di accesso EFS devono applicare un'identità utente](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.2\] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[ELB.12\] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[ELB.13\] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità](#)
- [\[ELB.14\] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)
- [\[ElastiCache.6\] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH](#)
- [\[ElastiCache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)
- [\[ES.1\] I domini Elasticsearch devono avere la crittografia a riposo abilitata](#)
- [\[ES.2\] I domini Elasticsearch non devono essere accessibili al pubblico](#)
- [\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[Glue.1\] i AWS Glue lavori devono essere etichettati](#)
- [\[GuardDuty.2\] GuardDuty i filtri devono essere etichettati](#)

- [\[GuardDuty.3\] Gli GuardDuty IPSet devono essere etichettati](#)
- [\[GuardDuty.4\] i GuardDuty rilevatori devono essere etichettati](#)
- [\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)
- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)
- [\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)
- [\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)
- [\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[MSK.1\] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker](#)
- [\[MSK.2\] Per i cluster MSK dovrebbe essere configurato un monitoraggio avanzato](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)
- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità](#)

- [\[NetworkFirewall.3\]](#) Le policy di Network Firewall devono avere almeno un gruppo di regole associato
- [\[NetworkFirewall.4\]](#) L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi
- [\[NetworkFirewall.5\]](#) L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati
- [\[NetworkFirewall.6\]](#) Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [I OpenSearch domini \[Opensearch.1\]](#) devono avere la crittografia a riposo abilitata
- [I OpenSearch domini \[Opensearch.2\]](#) non devono essere accessibili al pubblico
- [I OpenSearch domini \[Opensearch.3\]](#) devono crittografare i dati inviati tra i nodi
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\]](#) nei log dovrebbe essere abilitata CloudWatch
- [I OpenSearch domini \[Opensearch.5\]](#) devono avere la registrazione di controllo abilitata
- [I OpenSearch domini \[Opensearch.6\]](#) devono avere almeno tre nodi di dati
- [I OpenSearch domini \[Opensearch.7\]](#) devono avere un controllo degli accessi granulare abilitato
- [\[Opensearch.8\]](#) Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS
- [I OpenSearch domini \[Opensearch.11\]](#) devono avere almeno tre nodi primari dedicati
- [\[RDS.9\]](#) Le istanze DB RDS devono pubblicare i log nei registri CloudWatch
- [\[RDS.14\]](#) I cluster Amazon Aurora devono avere il backtracking abilitato
- [\[RDS.16\]](#) I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee
- [\[RDS.24\]](#) I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato
- [\[RDS.26\]](#) Le istanze DB RDS devono essere protette da un piano di backup
- [\[RDS.31\]](#) I gruppi di sicurezza RDS DB devono essere etichettati
- [\[Redshift.1\]](#) I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico
- [\[Redshift.2\]](#) Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito
- [\[Redshift.3\]](#) I cluster Amazon Redshift devono avere le istantanee automatiche abilitate
- [\[Redshift.7\]](#) I cluster Redshift devono utilizzare un routing VPC avanzato
- [\[Redshift.9\]](#) I cluster Redshift non devono utilizzare il nome di database predefinito
- [\[Redshift.10\]](#) I cluster Redshift devono essere crittografati a riposo

- [\[Redshift.12\] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[S3.11\] I bucket generici S3 devono avere le notifiche degli eventi abilitate](#)
- [\[S3.13\] I bucket generici S3 devono avere configurazioni del ciclo di vita](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)
- [\[SageMaker.2\] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato](#)
- [\[SageMaker.3\] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SNS.3\] Gli argomenti SNS devono essere etichettati](#)
- [\[SQS.1\] Le code di Amazon SQS devono essere crittografate quando sono inattive](#)
- [\[SQS.2\] Le code SQS devono essere etichettate](#)
- [\[SSM.1\] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager](#)
- [\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)
- [\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.2\] Le regole regionali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.4\] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)

- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.10\] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

Asia Pacifico (Mumbai)

I seguenti controlli non sono supportati in Asia Pacifico (Mumbai).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)

- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Asia Pacifico (Melbourne)

I seguenti controlli non sono supportati in Asia Pacifico (Melbourne).

- [\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)

- [\[ACM.2\] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit](#)
- [\[ApiGateway.4\] L'API Gateway deve essere associato a un ACL Web WAF](#)
- [\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione](#)
- [\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages](#)
- [\[AppSync.2\] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata](#)
- [\[AppSync.4\] Le API AWS AppSync GraphQL devono essere taggate](#)
- [\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)
- [\[Athena.2\] I cataloghi di dati Athena devono essere etichettati](#)
- [\[Athena.3\] I gruppi di lavoro Athena devono essere etichettati](#)
- [\[AutoScaling.1\] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB](#)
- [\[Autoscaling.5\] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici](#)
- [\[Backup.1\] i punti di AWS Backup ripristino devono essere crittografati a riposo](#)
- [\[Backup.2\] i punti di AWS Backup ripristino devono essere etichettati](#)
- [I AWS Backup vault \[Backup.3\] devono essere etichettati](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[Backup.5\] i piani di AWS Backup backup devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)

- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] Le distribuzioni devono essere etichettate CloudFront](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)
- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)
- [\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)
- [\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)
- [\[DMS.2\] I certificati DMS devono essere etichettati](#)
- [\[DMS.3\] Le sottoscrizioni agli eventi DMS devono essere contrassegnate](#)
- [\[DMS.4\] Le istanze di replica DMS devono essere contrassegnate](#)
- [\[DMS.5\] I sottoreti di replica DMS devono essere etichettati](#)
- [\[DMS.6\] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato](#)
- [\[DMS.7\] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata](#)
- [\[DMS.8\] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata](#)
- [\[DMS.9\] Gli endpoint DMS devono utilizzare SSL](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)

- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.1\] Gli snapshot di Amazon EBS non devono essere ripristinabili pubblicamente](#)
- [\[EC2.4\] Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato](#)
- [\[EC2.8\] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 \(IMDSv2\)](#)
- [\[EC2.9\] Le istanze Amazon EC2 non devono avere un indirizzo IPv4 pubblico](#)
- [\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0 o :/0 alla porta 22](#)
- [\[EC2.14\] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0 o :/0 alla porta 3389](#)
- [\[EC2.18\] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[EC2.25\] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete](#)
- [\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)
- [\[EC2.33\] Gli allegati del gateway di transito EC2 devono essere etichettati](#)
- [\[EC2.34\] Le tabelle delle rotte dei gateway di transito EC2 devono essere etichettate](#)
- [\[EC2.40\] I gateway NAT EC2 devono essere etichettati](#)
- [\[EC2.48\] I log di flusso di Amazon VPC devono essere etichettati](#)
- [\[EC2.51\] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata](#)
- [\[EC2.52\] I gateway di transito EC2 devono essere etichettati](#)
- [\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)

- [\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)
- [\[ECS.9\] Le definizioni delle attività ECS devono avere una configurazione di registrazione](#)
- [\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)
- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)
- [\[EFS.3\] I punti di accesso EFS devono applicare una directory principale](#)
- [\[EFS.4\] I punti di accesso EFS devono applicare un'identità utente](#)
- [\[EFS.5\] I punti di accesso EFS devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.2\] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[EKS.6\] I cluster EKS devono essere etichettati](#)
- [\[EKS.7\] Le configurazioni dei provider di identità EKS devono essere contrassegnate](#)
- [\[EKS.8\] I cluster EKS devono avere la registrazione di controllo abilitata](#)
- [\[ELB.13\] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità](#)
- [\[ELB.14\] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)
- [\[ElastiCache.2\] ElastiCache per i cluster di cache Redis dovrebbe avere l'aggiornamento automatico della versione secondaria abilitato](#)
- [\[ElastiCache.3\] ElastiCache per i gruppi di replica Redis dovrebbe avere il failover automatico abilitato](#)
- [\[ElastiCache.4\] ElastiCache per i gruppi di replica Redis deve essere crittografato a riposo](#)
- [\[ElastiCache.5\] ElastiCache per i gruppi di replica Redis devono essere crittografati in transito](#)
- [\[ElastiCache.6\] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH](#)
- [\[ElastiCache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)

- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)
- [\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)
- [\[ES.1\] I domini Elasticsearch devono avere la crittografia a riposo abilitata](#)
- [\[ES.2\] I domini Elasticsearch non devono essere accessibili al pubblico](#)
- [\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)
- [\[ES.4\] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch](#)
- [\[EventBridge.2\] i bus EventBridge degli eventi devono essere etichettati](#)
- [\[EventBridge.3\] i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[Glue.1\] i AWS Glue lavori devono essere etichettati](#)
- [\[GuardDuty.2\] GuardDuty i filtri devono essere etichettati](#)
- [\[GuardDuty.3\] Gli GuardDuty IPSet devono essere etichettati](#)
- [\[GuardDuty.4\] i GuardDuty rilevatori devono essere etichettati](#)
- [\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)
- [\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)
- [\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)
- [\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)
- [\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)
- [\[IAM.7\] Le politiche relative alle password per gli utenti IAM dovrebbero avere configurazioni solide](#)
- [\[IAM.8\] Le credenziali utente IAM non utilizzate devono essere rimosse](#)
- [\[IAM.10\] Le politiche relative alle password per gli utenti IAM dovrebbero avere durate elevate AWS Config](#)

- [\[IAM.11\] Assicurati che la politica delle password IAM richieda almeno una lettera maiuscola](#)
- [\[IAM.12\] Assicurati che la politica delle password IAM richieda almeno una lettera minuscola](#)
- [\[IAM.13\] Assicurati che la politica delle password IAM richieda almeno un simbolo](#)
- [\[IAM.14\] Assicurati che la politica delle password IAM richieda almeno un numero](#)
- [\[IAM.15\] Assicurati che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14](#)
- [\[IAM.16\] Assicurati che la politica delle password di IAM impedisca il riutilizzo delle password](#)
- [\[IAM.17\] Assicurati che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno](#)
- [\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)
- [\[IAM.19\] L'MFA deve essere abilitata per tutti gli utenti IAM](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)
- [\[IAM.22\] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse](#)
- [\[IAM.24\] I ruoli IAM devono essere etichettati](#)
- [\[IAM.25\] Gli utenti IAM devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IAM.27\] Le identità IAM non devono avere la policy allegata AWSCloudShellFullAccess](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)
- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)
- [\[KMS.1\] Le politiche gestite dai clienti di IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS](#)
- [\[KMS.2\] I principali IAM non devono disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS](#)
- [\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)

- [\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)
- [\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[MQ.4\] I broker Amazon MQ devono essere etichettati](#)
- [\[MQ.5\] I broker ActiveMQ devono utilizzare la modalità di distribuzione attiva/standby](#)
- [\[MQ.6\] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster](#)
- [\[MSK.1\] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker](#)
- [\[MSK.2\] Per i cluster MSK dovrebbe essere configurato un monitoraggio avanzato](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)
- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.2\] La registrazione del Network Firewall deve essere abilitata](#)
- [\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)
- [\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)
- [\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)
- [\[NetworkFirewall.6\] Il gruppo di regole Stateless Network Firewall non deve essere vuoto](#)
- [\[NetworkFirewall.9\] I firewall Network Firewall devono avere la protezione da eliminazione abilitata](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)
- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)

- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)
- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [I OpenSearch domini \[Opensearch.9\] devono essere etichettati](#)
- [Nei OpenSearch domini \[Opensearch.10\] deve essere installato l'ultimo aggiornamento software](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.1\] L'istanza RDS deve essere privata](#)
- [\[RDS.3\] Le istanze database RDS devono avere la crittografia dei dati inattivi abilitata](#)
- [\[RDS.7\] I cluster RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)
- [\[RDS.16\] I cluster RDS DB devono essere configurati per copiare i tag nelle istanze](#)
- [\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)
- [\[RDS.26\] Le istanze DB RDS devono essere protette da un piano di backup](#)
- [\[RDS.27\] I cluster RDS DB devono essere crittografati quando sono inattivi](#)
- [\[RDS.28\] I cluster RDS DB devono essere etichettati](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[RDS.34\] I cluster Aurora MySQL DB devono pubblicare i log di controllo nei registri CloudWatch](#)
- [\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Redshift.12\] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)

- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[S3.14\] I bucket generici S3 devono avere il controllo delle versioni abilitato](#)
- [\[S3.15\] I bucket generici S3 devono avere Object Lock abilitato](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)
- [\[SageMaker.2\] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato](#)
- [\[SageMaker.3\] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[SES.1\] Gli elenchi di contatti SES devono essere etichettati](#)
- [\[SES.2\] I set di configurazione SES devono essere etichettati](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SNS.1\] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS](#)
- [\[SNS.3\] Gli argomenti SNS devono essere etichettati](#)
- [\[SQS.1\] Le code di Amazon SQS devono essere crittografate quando sono inattive](#)
- [\[SQS.2\] Le code SQS devono essere etichettate](#)
- [\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)
- [\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)
- [\[SSM.4\] I documenti SSM non devono essere pubblici](#)
- [\[StepFunctions.1\] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata](#)
- [\[StepFunctions.2\] Le attività di Step Functions devono essere etichettate](#)
- [I AWS Transfer Family flussi di lavoro \[Transfer.1\] devono essere etichettati](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)

- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

Asia Pacifico (Osaka-Locale)

I seguenti controlli non sono supportati in Asia Pacifico (Osaka).

- [\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)
- [\[Account.2\] Account AWS deve far parte di un'organizzazione AWS Organizations](#)
- [\[ApiGateway.1\] API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati](#)
- [\[ApiGateway.2\] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend](#)
- [\[ApiGateway.3\] Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray](#)
- [\[ApiGateway.4\] L'API Gateway deve essere associato a un ACL Web WAF](#)
- [\[Autoscaling.5\] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici](#)
- [\[Backup.1\] i punti di AWS Backup ripristino devono essere crittografati a riposo](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)

- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CloudWatch.15\] gli CloudWatch allarmi devono avere azioni specificate configurate](#)
- [\[CloudWatch.16\] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)
- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)
- [\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)
- [\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)
- [\[DMS.7\] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata](#)
- [\[DMS.8\] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)

- [\[DynamoDB.2\] Le tabelle DynamoDB dovrebbero avere il ripristino abilitato point-in-time](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.1\] Gli snapshot di Amazon EBS non devono essere ripristinabili pubblicamente](#)
- [\[EC2.3\] I volumi Amazon EBS collegati devono essere crittografati a riposo](#)
- [\[EC2.4\] Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato](#)
- [\[EC2.7\] La crittografia predefinita di EBS deve essere abilitata](#)
- [\[EC2.8\] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 \(IMDSv2\)](#)
- [\[EC2.9\] Le istanze Amazon EC2 non devono avere un indirizzo IPv4 pubblico](#)
- [\[EC2.10\] Amazon EC2 deve essere configurato per utilizzare endpoint VPC creati per il servizio Amazon EC2](#)
- [\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o :/0 alla porta 22](#)
- [\[EC2.14\] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o :/0 alla porta 3389](#)
- [\[EC2.15\] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici](#)
- [\[EC2.16\] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse](#)
- [\[EC2.17\] Le istanze Amazon EC2 non devono utilizzare più ENI](#)
- [\[EC2.18\] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate](#)
- [\[EC2.20\] Entrambi i tunnel VPN per una connessione VPN da sito a sito devono essere AWS attivi](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)
- [\[EC2.51\] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata](#)
- [\[EC2.52\] I gateway di transito EC2 devono essere etichettati](#)
- [\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)

- [\[ECR.2\] I repository privati ECR devono avere l'immutabilità dei tag configurata](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)
- [\[ECS.2\] Ai servizi ECS non devono essere assegnati automaticamente indirizzi IP pubblici](#)
- [\[ECS.3\] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host](#)
- [\[ECS.4\] I contenitori ECS devono essere eseguiti come non privilegiati](#)
- [\[ECS.8\] I segreti non devono essere passati come variabili di ambiente del contenitore](#)
- [\[ECS.9\] Le definizioni delle attività ECS devono avere una configurazione di registrazione](#)
- [\[ECS.10\] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate](#)
- [\[ECS.12\] I cluster ECS devono utilizzare Container Insights](#)
- [\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)
- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.2\] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[ELB.1\] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS](#)
- [\[ELB.2\] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager](#)
- [\[ELB.3\] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS](#)
- [\[ELB.4\] L'Application Load Balancer deve essere configurato per eliminare le intestazioni http](#)
- [\[ELB.6\] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata](#)
- [\[ELB.8\] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita con una durata elevata AWS Config](#)
- [\[ELB.9\] I Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato](#)
- [\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF](#)

- [\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)
- [\[ElastiCache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)
- [\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)
- [\[ES.1\] I domini Elasticsearch devono avere la crittografia a riposo abilitata](#)
- [\[ES.2\] I domini Elasticsearch non devono essere accessibili al pubblico](#)
- [\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)
- [\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)
- [\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)
- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)
- [\[KMS.1\] Le politiche gestite dai clienti di IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS](#)

- [\[KMS.2\] I principali IAM non devono disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS](#)
- [\[KMS.3\] AWS KMS keys non deve essere eliminato involontariamente](#)
- [\[Lambda.1\] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico](#)
- [\[Lambda.2\] Le funzioni Lambda devono utilizzare runtime supportati](#)
- [\[Lambda.3\] Le funzioni Lambda devono trovarsi in un VPC](#)
- [\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)
- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)
- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)
- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)
- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)

- [\[RDS.1\] L'istantanea RDS deve essere privata](#)
- [\[RDS.4\] Le istantanee dei cluster RDS e le istantanee del database devono essere crittografate quando sono inattive](#)
- [\[RDS.6\] Il monitoraggio avanzato deve essere configurato per le istanze DB RDS](#)
- [\[RDS.7\] I cluster RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.8\] Le istanze DB RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.9\] Le istanze DB RDS devono pubblicare i log nei registri CloudWatch](#)
- [\[RDS.10\] L'autenticazione IAM deve essere configurata per le istanze RDS](#)
- [\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)
- [\[RDS.13\] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)
- [\[RDS.26\] Le istanze DB RDS devono essere protette da un piano di backup](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Redshift.1\] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico](#)
- [\[Redshift.2\] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito](#)
- [\[Redshift.3\] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate](#)
- [\[Redshift.7\] I cluster Redshift devono utilizzare un routing VPC avanzato](#)
- [\[Redshift.10\] I cluster Redshift devono essere crittografati a riposo](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)
- [\[S3.15\] I bucket generici S3 devono avere Object Lock abilitato](#)
- [\[S3.17\] I bucket generici S3 devono essere crittografati quando sono inattivi con AWS KMS keys](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)

- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[SecretsManager.1\] I segreti di Secrets Manager devono avere la rotazione automatica abilitata](#)
- [\[SecretsManager.2\] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente](#)
- [\[SecretsManager.3\] Rimuovi i segreti inutilizzati di Secrets Manager](#)
- [\[SecretsManager.4\] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SNS.1\] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS](#)
- [\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)
- [\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.10\] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

Asia Pacifico (Seoul)

I seguenti controlli non sono supportati in Asia Pacifico (Seoul).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)

- [\[CloudFront.5\]](#) le CloudFront distribuzioni dovrebbero avere la registrazione abilitata
- [\[CloudFront.6\]](#) CloudFront le distribuzioni devono avere WAF abilitato
- [\[CloudFront.7\]](#) le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati
- [\[CloudFront.8\]](#) le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [\[CloudFront.9\]](#) le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate
- [\[CloudFront.10\]](#) CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate
- [\[CloudFront.12\]](#) CloudFront le distribuzioni non devono puntare a origini S3 inesistenti
- [\[CloudFront.13\]](#) CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine
- [\[CloudFront.14\]](#) le distribuzioni devono essere etichettate CloudFront
- [\[CodeArtifact.1\]](#) i CodeArtifact repository devono essere etichettati
- [\[DataFirehose.1\]](#) I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi
- [\[DMS.10\]](#) Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata
- [\[DMS.11\]](#) Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato
- [\[DMS.12\]](#) Gli endpoint DMS per Redis devono avere TLS abilitato
- [\[DynamoDB.3\]](#) I cluster DynamoDB Accelerator (DAX) devono essere crittografati quando sono inattivi
- [\[DynamoDB.7\]](#) I cluster DynamoDB Accelerator devono essere crittografati in transito
- [\[EC2.24\]](#) I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati
- [\[ECR.4\]](#) Gli archivi pubblici ECR devono essere etichettati
- [\[EFS.6\]](#) I target di montaggio EFS non devono essere associati a una sottorete pubblica
- [\[EKS.3\]](#) I cluster EKS devono utilizzare segreti Kubernetes crittografati
- [\[FSX.2\]](#) I file system FSx for Lustre devono essere configurati per copiare i tag nei backup
- [\[GlobalAccelerator.1\]](#) Gli acceleratori Global Accelerator devono essere etichettati
- [\[IAM.26\]](#) I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi
- [\[MQ.2\]](#) I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch
- [\[MQ.3\]](#) I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie
- [I OpenSearch domini \[Opensearch.11\]](#) devono avere almeno tre nodi primari dedicati
- [\[RDS.31\]](#) I gruppi di sicurezza RDS DB devono essere etichettati

- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Asia Pacifico (Singapore)

I seguenti controlli non sono supportati in Asia Pacifico (Singapore).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)

- [\[CloudFront.14\] Le distribuzioni devono essere etichettate CloudFront](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Asia Pacifico (Sydney)

I seguenti controlli non sono supportati in Asia Pacifico (Sydney).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)

- [\[OpenSearch.domini.11\]](#) I domini OpenSearch devono avere almeno tre nodi primari dedicati
- [\[Redshift.3\]](#) I cluster Amazon Redshift devono avere le istantanee automatiche abilitate
- [\[Redshift.15\]](#) I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate
- [\[Route53.1\]](#) I controlli sanitari della Route 53 devono essere etichettati
- [\[Route53.2\]](#) Le zone ospitate pubbliche di Route 53 devono registrare le query DNS
- [\[SageMaker.4\]](#) Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1
- [\[ServiceCatalog.1\]](#) I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS
- [\[Transfer.2\]](#) I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint
- [\[WAF.1\]](#) La registrazione AWS WAF classica Global Web ACL deve essere abilitata
- [\[WAF.6\]](#) Le regole globali AWS WAF classiche devono avere almeno una condizione
- [\[WAF.7\]](#) I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola
- [\[WAF.8\]](#) Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole

Asia Pacifico (Tokyo)

I seguenti controlli non sono supportati in Asia Pacifico (Tokyo).

- [\[CloudFront.1\]](#) CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato
- [\[CloudFront.3\]](#) CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito
- [\[CloudFront.4\]](#) le CloudFront distribuzioni devono avere configurato il failover di origine
- [\[CloudFront.5\]](#) le CloudFront distribuzioni dovrebbero avere la registrazione abilitata
- [\[CloudFront.6\]](#) CloudFront le distribuzioni devono avere WAF abilitato
- [\[CloudFront.7\]](#) le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati
- [\[CloudFront.8\]](#) le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS
- [\[CloudFront.9\]](#) le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate
- [\[CloudFront.10\]](#) CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate

- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)

- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Canada (Centrale)

I seguenti controlli non sono supportati in Canada (Central).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)

- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Cina (Pechino)

I seguenti controlli non sono supportati in Cina (Pechino).

- [\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)
- [\[ACM.2\] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit](#)
- [\[ACM.3\] I certificati ACM devono essere etichettati](#)

- [\[Account.2\] Account AWS deve far parte di un'organizzazione AWS Organizations](#)
- [\[ApiGateway.2\] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend](#)
- [\[ApiGateway.3\] Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray](#)
- [\[ApiGateway.4\] L'API Gateway deve essere associato a un ACL Web WAF](#)
- [\[AppSync.4\] Le API AWS AppSync GraphQL devono essere taggate](#)
- [\[Athena.2\] I cataloghi di dati Athena devono essere etichettati](#)
- [\[Athena.3\] I gruppi di lavoro Athena devono essere etichettati](#)
- [\[AutoScaling.10\] I gruppi di Auto Scaling EC2 devono essere etichettati](#)
- [\[Backup.1\] i punti di AWS Backup ripristino devono essere crittografati a riposo](#)
- [\[Backup.2\] i punti di AWS Backup ripristino devono essere etichettati](#)
- [I AWS Backup vault \[Backup.3\] devono essere etichettati](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[Backup.5\] i piani di AWS Backup backup devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CloudTrail.9\] i percorsi devono essere etichettati CloudTrail](#)
- [\[CloudWatch.15\] gli CloudWatch allarmi devono avere azioni specificate configurate](#)
- [\[CloudWatch.16\] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato](#)

- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.2\] I certificati DMS devono essere etichettati](#)
- [\[DMS.3\] Le sottoscrizioni agli eventi DMS devono essere contrassegnate](#)
- [\[DMS.4\] Le istanze di replica DMS devono essere contrassegnate](#)
- [\[DMS.5\] I sottoreti di replica DMS devono essere etichettati](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)
- [\[DynamoDB.5\] Le tabelle DynamoDB devono essere etichettate](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.15\] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici](#)
- [\[EC2.16\] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse](#)
- [\[EC2.20\] Entrambi i tunnel VPN per una connessione VPN da sito a sito devono essere AWS attivi](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)

- [\[EC2.33\] Gli allegati del gateway di transito EC2 devono essere etichettati](#)
- [\[EC2.34\] Le tabelle delle rotte dei gateway di transito EC2 devono essere etichettate](#)
- [\[EC2.35\] Le interfacce di rete EC2 devono essere etichettate](#)
- [\[EC2.36\] I gateway per i clienti EC2 devono essere etichettati](#)
- [\[EC2.37\] Gli indirizzi IP elastici EC2 devono essere etichettati](#)
- [\[EC2.38\] Le istanze EC2 devono essere etichettate](#)
- [\[EC2.39\] I gateway Internet EC2 devono essere etichettati](#)
- [\[EC2.40\] I gateway NAT EC2 devono essere etichettati](#)
- [\[EC2.41\] Gli ACL di rete EC2 devono essere etichettati](#)
- [\[EC2.42\] Le tabelle di routing EC2 devono essere etichettate](#)
- [\[EC2.43\] I gruppi di sicurezza EC2 devono essere etichettati](#)
- [\[EC2.44\] Le sottoreti EC2 devono essere etichettate](#)
- [\[EC2.45\] I volumi EC2 devono essere etichettati](#)
- [\[EC2.46\] I VPC Amazon devono essere etichettati](#)
- [\[EC2.47\] I servizi endpoint Amazon VPC devono essere etichettati](#)
- [\[EC2.48\] I log di flusso di Amazon VPC devono essere etichettati](#)
- [\[EC2.49\] Le connessioni peering Amazon VPC devono essere etichettate](#)
- [\[EC2.50\] I gateway VPN EC2 devono essere etichettati](#)
- [\[EC2.51\] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata](#)
- [\[EC2.52\] I gateway di transito EC2 devono essere etichettati](#)
- [\[EC2.53\] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da 0.0.0.0/0 alle porte di amministrazione remota del server](#)
- [\[EC2.54\] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server](#)
- [\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)
- [\[ECS.13\] I servizi ECS devono essere etichettati](#)
- [\[ECS.14\] I cluster ECS devono essere etichettati](#)

- [\[ECS.15\] Le definizioni delle attività ECS devono essere contrassegnate](#)
- [\[EFS.5\] I punti di accesso EFS devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[EKS.6\] I cluster EKS devono essere etichettati](#)
- [\[EKS.7\] Le configurazioni dei provider di identità EKS devono essere contrassegnate](#)
- [\[ELB.2\] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager](#)
- [\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF](#)
- [\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)
- [\[EMR.2\] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata](#)
- [\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)
- [\[ES.4\] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch](#)
- [\[ES.9\] I domini Elasticsearch devono essere etichettati](#)
- [\[EventBridge.2\] i bus EventBridge degli eventi devono essere etichettati](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[Glue.1\] i AWS Glue lavori devono essere etichettati](#)
- [\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)
- [\[GuardDuty.2\] GuardDuty i filtri devono essere etichettati](#)
- [\[GuardDuty.3\] Gli GuardDuty IPSet devono essere etichettati](#)
- [\[GuardDuty.4\] i GuardDuty rilevatori devono essere etichettati](#)

- [\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)
- [\[IAM.9\] L'MFA deve essere abilitata per l'utente root](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)
- [\[IAM.23\] Gli analizzatori IAM Access Analyzer devono essere etichettati](#)
- [\[IAM.24\] I ruoli IAM devono essere etichettati](#)
- [\[IAM.25\] Gli utenti IAM devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IAM.27\] Le identità IAM non devono avere la policy allegata AWSCloudShellFullAccess](#)
- [\[IAM.28\] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)
- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[Kinesis.2\] Gli stream Kinesis devono essere etichettati](#)
- [\[Lambda.6\] Le funzioni Lambda devono essere etichettate](#)
- [\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)
- [\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[MQ.4\] I broker Amazon MQ devono essere etichettati](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)

- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.2\] La registrazione del Network Firewall deve essere abilitata](#)
- [\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)
- [\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)
- [\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)
- [\[NetworkFirewall.6\] Il gruppo di regole Stateless Network Firewall non deve essere vuoto](#)
- [\[NetworkFirewall.7\] I firewall Network Firewall devono essere etichettati](#)
- [\[NetworkFirewall.8\] Le politiche firewall di Network Firewall devono essere etichettate](#)
- [\[NetworkFirewall.9\] I firewall Network Firewall devono avere la protezione da eliminazione abilitata](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)
- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)
- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)
- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [I OpenSearch domini \[Opensearch.9\] devono essere etichettati](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [L'autorità di certificazione AWS Private CA principale \[PCA.1\] deve essere disabilitata](#)
- [\[RDS.7\] I cluster RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.10\] L'autenticazione IAM deve essere configurata per le istanze RDS](#)
- [\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)

- [\[RDS.13\] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)
- [\[RDS.16\] I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)
- [\[RDS.25\] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato](#)
- [\[RDS.26\] Le istanze DB RDS devono essere protette da un piano di backup](#)
- [\[RDS.27\] I cluster RDS DB devono essere crittografati quando sono inattivi](#)
- [\[RDS.28\] I cluster RDS DB devono essere etichettati](#)
- [\[RDS.29\] Gli snapshot del cluster RDS DB devono essere etichettati](#)
- [\[RDS.30\] Le istanze DB RDS devono essere etichettate](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[RDS.32\] Gli snapshot RDS DB devono essere etichettati](#)
- [\[RDS.33\] I gruppi di sottoreti RDS DB devono essere etichettati](#)
- [\[RDS.34\] I cluster Aurora MySQL DB devono pubblicare i log di controllo nei registri CloudWatch](#)
- [\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Redshift.7\] I cluster Redshift devono utilizzare un routing VPC avanzato](#)
- [\[Redshift.10\] I cluster Redshift devono essere crittografati a riposo](#)
- [\[Redshift.11\] I cluster Redshift devono essere etichettati](#)
- [\[Redshift.12\] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate](#)
- [\[Redshift.13\] Le istantanee del cluster Redshift devono essere etichettate](#)
- [\[Redshift.14\] I gruppi di sottoreti del cluster Redshift devono essere etichettati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)
- [\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)

- [\[S3.14\] I bucket generici S3 devono avere il controllo delle versioni abilitato](#)
- [\[S3.22\] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto](#)
- [\[S3.23\] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[SES.1\] Gli elenchi di contatti SES devono essere etichettati](#)
- [\[SES.2\] I set di configurazione SES devono essere etichettati](#)
- [\[SecretsManager.3\] Rimuovi i segreti inutilizzati di Secrets Manager](#)
- [\[SecretsManager.4\] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni](#)
- [\[SecretsManager.5\] I segreti di Secrets Manager devono essere etichettati](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SNS.3\] Gli argomenti SNS devono essere etichettati](#)
- [\[SQS.2\] Le code SQS devono essere etichettate](#)
- [\[StepFunctions.2\] Le attività di Step Functions devono essere etichettate](#)
- [I AWS Transfer Family flussi di lavoro \[Transfer.1\] devono essere etichettati](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

Cina (Ningxia)

I seguenti controlli non sono supportati in Cina (Ningxia).

- [\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)
- [\[ACM.2\] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit](#)
- [\[ACM.3\] I certificati ACM devono essere etichettati](#)
- [\[Account.2\] Account AWS deve far parte di un'organizzazione AWS Organizations](#)
- [\[ApiGateway.2\] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend](#)
- [\[ApiGateway.3\] Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray](#)
- [\[ApiGateway.4\] L'API Gateway deve essere associato a un ACL Web WAF](#)
- [\[AppSync.4\] Le API AWS AppSync GraphQL devono essere taggate](#)
- [\[Athena.2\] I cataloghi di dati Athena devono essere etichettati](#)
- [\[Athena.3\] I gruppi di lavoro Athena devono essere etichettati](#)
- [\[AutoScaling.10\] I gruppi di Auto Scaling EC2 devono essere etichettati](#)
- [\[Backup.1\] i punti di AWS Backup ripristino devono essere crittografati a riposo](#)
- [\[Backup.2\] i punti di AWS Backup ripristino devono essere etichettati](#)
- [I AWS Backup vault \[Backup.3\] devono essere etichettati](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[Backup.5\] i piani di AWS Backup backup devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)

- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CloudTrail.9\] i percorsi devono essere etichettati CloudTrail](#)
- [\[CloudWatch.15\] gli CloudWatch allarmi devono avere azioni specificate configurate](#)
- [\[CloudWatch.16\] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.2\] I certificati DMS devono essere etichettati](#)
- [\[DMS.3\] Le sottoscrizioni agli eventi DMS devono essere contrassegnate](#)
- [\[DMS.4\] Le istanze di replica DMS devono essere contrassegnate](#)
- [\[DMS.5\] I sottoreti di replica DMS devono essere etichettati](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)
- [\[DynamoDB.5\] Le tabelle DynamoDB devono essere etichettate](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.15\] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici](#)
- [\[EC2.16\] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse](#)
- [\[EC2.20\] Entrambi i tunnel VPN per una connessione VPN da sito a sito devono essere AWS attivi](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)

- [\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)
- [\[EC2.33\] Gli allegati del gateway di transito EC2 devono essere etichettati](#)
- [\[EC2.34\] Le tabelle delle rotte dei gateway di transito EC2 devono essere etichettate](#)
- [\[EC2.35\] Le interfacce di rete EC2 devono essere etichettate](#)
- [\[EC2.36\] I gateway per i clienti EC2 devono essere etichettati](#)
- [\[EC2.37\] Gli indirizzi IP elastici EC2 devono essere etichettati](#)
- [\[EC2.38\] Le istanze EC2 devono essere etichettate](#)
- [\[EC2.39\] I gateway Internet EC2 devono essere etichettati](#)
- [\[EC2.40\] I gateway NAT EC2 devono essere etichettati](#)
- [\[EC2.41\] Gli ACL di rete EC2 devono essere etichettati](#)
- [\[EC2.42\] Le tabelle di routing EC2 devono essere etichettate](#)
- [\[EC2.43\] I gruppi di sicurezza EC2 devono essere etichettati](#)
- [\[EC2.44\] Le sottoreti EC2 devono essere etichettate](#)
- [\[EC2.45\] I volumi EC2 devono essere etichettati](#)
- [\[EC2.46\] I VPC Amazon devono essere etichettati](#)
- [\[EC2.47\] I servizi endpoint Amazon VPC devono essere etichettati](#)
- [\[EC2.48\] I log di flusso di Amazon VPC devono essere etichettati](#)
- [\[EC2.49\] Le connessioni peering Amazon VPC devono essere etichettate](#)
- [\[EC2.50\] I gateway VPN EC2 devono essere etichettati](#)
- [\[EC2.51\] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata](#)
- [\[EC2.52\] I gateway di transito EC2 devono essere etichettati](#)
- [\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)
- [\[ECS.13\] I servizi ECS devono essere etichettati](#)
- [\[ECS.14\] I cluster ECS devono essere etichettati](#)
- [\[ECS.15\] Le definizioni delle attività ECS devono essere contrassegnate](#)
- [\[EFS.3\] I punti di accesso EFS devono applicare una directory principale](#)

- [\[EFS.4\] I punti di accesso EFS devono applicare un'identità utente](#)
- [\[EFS.5\] I punti di accesso EFS devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[EKS.6\] I cluster EKS devono essere etichettati](#)
- [\[EKS.7\] Le configurazioni dei provider di identità EKS devono essere contrassegnate](#)
- [\[ELB.2\] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager](#)
- [\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF](#)
- [\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)
- [\[EMR.2\] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata](#)
- [\[ES.1\] I domini Elasticsearch devono avere la crittografia a riposo abilitata](#)
- [\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)
- [\[ES.4\] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch](#)
- [\[ES.9\] I domini Elasticsearch devono essere etichettati](#)
- [\[EventBridge.2\] i bus EventBridge degli eventi devono essere etichettati](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[Glue.1\] i AWS Glue lavori devono essere etichettati](#)
- [\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)
- [\[GuardDuty.2\] GuardDuty i filtri devono essere etichettati](#)
- [\[GuardDuty.3\] Gli GuardDuty IPSet devono essere etichettati](#)

- [\[GuardDuty.4\] i GuardDuty rilevatori devono essere etichettati](#)
- [\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)
- [\[IAM.9\] L'MFA deve essere abilitata per l'utente root](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)
- [\[IAM.23\] Gli analizzatori IAM Access Analyzer devono essere etichettati](#)
- [\[IAM.24\] I ruoli IAM devono essere etichettati](#)
- [\[IAM.25\] Gli utenti IAM devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IAM.27\] Le identità IAM non devono avere la policy allegata AWSCloudShellFullAccess](#)
- [\[IAM.28\] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)
- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[Kinesis.2\] Gli stream Kinesis devono essere etichettati](#)
- [\[Lambda.1\] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico](#)
- [\[Lambda.2\] Le funzioni Lambda devono utilizzare runtime supportati](#)
- [\[Lambda.3\] Le funzioni Lambda devono trovarsi in un VPC](#)
- [\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)
- [\[Lambda.6\] Le funzioni Lambda devono essere etichettate](#)
- [\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)
- [\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[MQ.4\] I broker Amazon MQ devono essere etichettati](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)

- [\[NetworkFirewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.2\] La registrazione del Network Firewall deve essere abilitata](#)
- [\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)
- [\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)
- [\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)
- [\[NetworkFirewall.6\] Il gruppo di regole Stateless Network Firewall non deve essere vuoto](#)
- [\[NetworkFirewall.7\] I firewall Network Firewall devono essere etichettati](#)
- [\[NetworkFirewall.8\] Le politiche firewall di Network Firewall devono essere etichettate](#)
- [\[NetworkFirewall.9\] I firewall Network Firewall devono avere la protezione da eliminazione abilitata](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)
- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)
- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)
- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [I OpenSearch domini \[Opensearch.9\] devono essere etichettati](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [L'autorità di certificazione AWS Private CA principale \[PCA.1\] deve essere disabilitata](#)
- [\[RDS.7\] I cluster RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.9\] Le istanze DB RDS devono pubblicare i log nei registri CloudWatch](#)
- [\[RDS.10\] L'autenticazione IAM deve essere configurata per le istanze RDS](#)
- [\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)
- [\[RDS.13\] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)

- [\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)
- [\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)
- [\[RDS.25\] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato](#)
- [\[RDS.26\] Le istanze DB RDS devono essere protette da un piano di backup](#)
- [\[RDS.28\] I cluster RDS DB devono essere etichettati](#)
- [\[RDS.29\] Gli snapshot del cluster RDS DB devono essere etichettati](#)
- [\[RDS.30\] Le istanze DB RDS devono essere etichettate](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[RDS.32\] Gli snapshot RDS DB devono essere etichettati](#)
- [\[RDS.33\] I gruppi di sottoreti RDS DB devono essere etichettati](#)
- [\[RDS.34\] I cluster Aurora MySQL DB devono pubblicare i log di controllo nei registri CloudWatch](#)
- [\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Redshift.3\] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate](#)
- [\[Redshift.7\] I cluster Redshift devono utilizzare un routing VPC avanzato](#)
- [\[Redshift.10\] I cluster Redshift devono essere crittografati a riposo](#)
- [\[Redshift.11\] I cluster Redshift devono essere etichettati](#)
- [\[Redshift.12\] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate](#)
- [\[Redshift.13\] Le istantanee del cluster Redshift devono essere etichettate](#)
- [\[Redshift.14\] I gruppi di sottoreti del cluster Redshift devono essere etichettati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)
- [\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)
- [\[S3.14\] I bucket generici S3 devono avere il controllo delle versioni abilitato](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)

- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[SES.1\] Gli elenchi di contatti SES devono essere etichettati](#)
- [\[SES.2\] I set di configurazione SES devono essere etichettati](#)
- [\[SecretsManager.3\] Rimuovi i segreti inutilizzati di Secrets Manager](#)
- [\[SecretsManager.4\] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni](#)
- [\[SecretsManager.5\] I segreti di Secrets Manager devono essere etichettati](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SNS.3\] Gli argomenti SNS devono essere etichettati](#)
- [\[SQS.2\] Le code SQS devono essere etichettate](#)
- [\[StepFunctions.2\] Le attività di Step Functions devono essere etichettate](#)
- [I AWS Transfer Family flussi di lavoro \[Transfer.1\] devono essere etichettati](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

Europa (Francoforte)

I seguenti controlli non sono supportati in Europa (Francoforte).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)

- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Europa (Irlanda)

I seguenti controlli non sono supportati in Europa (Irlanda).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)

- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)

- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Europa (Londra)

I seguenti controlli non sono supportati in Europa (Londra).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)

- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Europa (Milano)

I seguenti controlli non sono supportati in Europa (Milano).

- [\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)
- [\[ApiGateway.1\] API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)

- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)
- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.3\] I volumi Amazon EBS collegati devono essere crittografati a riposo](#)
- [\[EC2.4\] Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato](#)
- [\[EC2.8\] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 \(IMDSv2\)](#)
- [\[EC2.12\] Gli EIP Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22](#)
- [\[EC2.14\] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389](#)

- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.12\] I cluster ECS devono utilizzare Container Insights](#)
- [\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)
- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[ELB.1\] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS](#)
- [\[ELB.2\] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager](#)
- [\[ELB.4\] L'Application Load Balancer deve essere configurato per eliminare le intestazioni http](#)
- [\[ELB.8\] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita con una durata elevata AWS Config](#)
- [\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF](#)
- [\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)
- [\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)
- [\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)
- [\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)

- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)
- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[KMS.3\] AWS KMS keys non deve essere eliminato involontariamente](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)
- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)
- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)
- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)
- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.1\] L'istananea RDS deve essere privata](#)
- [\[RDS.4\] Le istantanee dei cluster RDS e le istantanee del database devono essere crittografate quando sono inattive](#)

- [\[RDS.9\] Le istanze DB RDS devono pubblicare i log nei registri CloudWatch](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[Redshift.2\] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito](#)
- [\[Redshift.3\] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)
- [\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

Europa (Parigi)

I seguenti controlli non sono supportati in Europa (Parigi).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)

- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)

- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Europa (Spagna)

I seguenti controlli non sono supportati in Europa (Spagna).

- [\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)
- [\[ACM.2\] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit](#)
- [\[Account.2\] Account AWS deve far parte di un'organizzazione AWS Organizations](#)
- [\[ApiGateway.1\] API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati](#)
- [\[ApiGateway.2\] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend](#)
- [\[ApiGateway.3\] Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray](#)
- [\[ApiGateway.4\] L'API Gateway deve essere associato a un ACL Web WAF](#)
- [\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione](#)

- [\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages](#)
- [\[AppSync.2\] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata](#)
- [\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)
- [\[Athena.2\] I cataloghi di dati Athena devono essere etichettati](#)
- [\[Athena.3\] I gruppi di lavoro Athena devono essere etichettati](#)
- [\[AutoScaling.1\] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB](#)
- [\[Autoscaling.5\] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici](#)
- [\[Backup.1\] i punti di AWS Backup ripristino devono essere crittografati a riposo](#)
- [\[Backup.2\] i punti di AWS Backup ripristino devono essere etichettati](#)
- [I AWS Backup vault \[Backup.3\] devono essere etichettati](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[Backup.5\] i piani di AWS Backup backup devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CloudTrail.6\] Assicurati che il bucket S3 utilizzato per archiviare i log non sia accessibile al pubblico CloudTrail](#)

- [\[CloudTrail.7\] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail](#)
- [\[CloudWatch.16\] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)
- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)
- [\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)
- [\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)
- [\[DMS.2\] I certificati DMS devono essere etichettati](#)
- [\[DMS.3\] Le sottoscrizioni agli eventi DMS devono essere contrassegnate](#)
- [\[DMS.4\] Le istanze di replica DMS devono essere contrassegnate](#)
- [\[DMS.5\] I sottoreti di replica DMS devono essere etichettati](#)
- [\[DMS.6\] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato](#)
- [\[DMS.7\] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata](#)
- [\[DMS.8\] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata](#)
- [\[DMS.9\] Gli endpoint DMS devono utilizzare SSL](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)

- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.1\] Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda](#)
- [\[DynamoDB.2\] Le tabelle DynamoDB dovrebbero avere il ripristino abilitato point-in-time](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.1\] Gli snapshot di Amazon EBS non devono essere ripristinabili pubblicamente](#)
- [\[EC2.2\] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita](#)
- [\[EC2.3\] I volumi Amazon EBS collegati devono essere crittografati a riposo](#)
- [\[EC2.4\] Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato](#)
- [\[EC2.6\] La registrazione del flusso VPC deve essere abilitata in tutti i VPC](#)
- [\[EC2.7\] La crittografia predefinita di EBS deve essere abilitata](#)
- [\[EC2.8\] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 \(IMDSv2\)](#)
- [\[EC2.9\] Le istanze Amazon EC2 non devono avere un indirizzo IPv4 pubblico](#)
- [\[EC2.10\] Amazon EC2 deve essere configurato per utilizzare endpoint VPC creati per il servizio Amazon EC2](#)
- [\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22](#)
- [\[EC2.14\] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389](#)
- [\[EC2.15\] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici](#)
- [\[EC2.16\] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse](#)
- [\[EC2.17\] Le istanze Amazon EC2 non devono utilizzare più ENI](#)
- [\[EC2.18\] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate](#)

- [\[EC2.20\] Entrambi i tunnel VPN per una connessione VPN da sito a sito devono essere AWS attivi](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[EC2.25\] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete](#)
- [\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)
- [\[EC2.34\] Le tabelle delle rotte dei gateway di transito EC2 devono essere etichettate](#)
- [\[EC2.40\] I gateway NAT EC2 devono essere etichettati](#)
- [\[EC2.48\] I log di flusso di Amazon VPC devono essere etichettati](#)
- [\[EC2.51\] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata](#)
- [\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)
- [\[ECR.2\] I repository privati ECR devono avere l'immutabilità dei tag configurata](#)
- [\[ECR.3\] I repository ECR devono avere almeno una politica del ciclo di vita configurata](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)
- [\[ECS.9\] Le definizioni delle attività ECS devono avere una configurazione di registrazione](#)
- [\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)
- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)
- [\[EFS.3\] I punti di accesso EFS devono applicare una directory principale](#)
- [\[EFS.4\] I punti di accesso EFS devono applicare un'identità utente](#)
- [\[EFS.5\] I punti di accesso EFS devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.2\] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[ELB.1\] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS](#)

- [\[ELB.2\] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager](#)
- [\[ELB.3\] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS](#)
- [\[ELB.4\] L'Application Load Balancer deve essere configurato per eliminare le intestazioni http](#)
- [\[ELB.5\] La registrazione delle applicazioni e dei sistemi Classic Load Balancers deve essere abilitata](#)
- [\[ELB.6\] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata](#)
- [\[ELB.8\] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita con una durata elevata AWS Config](#)
- [\[ELB.9\] I Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato](#)
- [\[ELB.14\] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF](#)
- [\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)
- [\[ElastiCache.6\] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH](#)
- [\[ElastiCache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)
- [\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)
- [\[ES.1\] I domini Elasticsearch devono avere la crittografia a riposo abilitata](#)
- [\[ES.2\] I domini Elasticsearch non devono essere accessibili al pubblico](#)
- [\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)
- [\[ES.4\] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch](#)
- [\[EventBridge.2\] i bus EventBridge degli eventi devono essere etichettati](#)
- [\[EventBridge.3\] i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata](#)

- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[Glue.1\] i AWS Glue lavori devono essere etichettati](#)
- [\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)
- [\[GuardDuty.2\] GuardDuty i filtri devono essere etichettati](#)
- [\[GuardDuty.3\] Gli GuardDuty IPSet devono essere etichettati](#)
- [\[GuardDuty.4\] i GuardDuty rilevatori devono essere etichettati](#)
- [\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)
- [\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)
- [\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)
- [\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)
- [\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)
- [\[IAM.8\] Le credenziali utente IAM non utilizzate devono essere rimosse](#)
- [\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)
- [\[IAM.19\] L'MFA deve essere abilitata per tutti gli utenti IAM](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)
- [\[IAM.22\] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse](#)
- [\[IAM.24\] I ruoli IAM devono essere etichettati](#)
- [\[IAM.25\] Gli utenti IAM devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IAM.27\] Le identità IAM non devono avere la policy allegata AWSCloudShellFullAccess](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)

- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)
- [\[KMS.1\] Le politiche gestite dai clienti di IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS](#)
- [\[KMS.2\] I principali IAM non devono disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS](#)
- [\[KMS.4\] la rotazione dei tasti dovrebbe essere abilitata AWS KMS](#)
- [\[Lambda.1\] Le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico](#)
- [\[Lambda.2\] Le funzioni Lambda devono utilizzare runtime supportati](#)
- [\[Lambda.3\] Le funzioni Lambda devono trovarsi in un VPC](#)
- [\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)
- [\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)
- [\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[MQ.4\] I broker Amazon MQ devono essere etichettati](#)
- [\[MQ.5\] I broker ActiveMQ devono utilizzare la modalità di distribuzione attiva/standby](#)
- [\[MQ.6\] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster](#)
- [\[MSK.1\] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker](#)
- [\[MSK.2\] Per i cluster MSK dovrebbe essere configurato un monitoraggio avanzato](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)
- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)

- [\[NetworkFirewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.2\] La registrazione del Network Firewall deve essere abilitata](#)
- [\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)
- [\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)
- [\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)
- [\[NetworkFirewall.6\] Il gruppo di regole Stateless Network Firewall non deve essere vuoto](#)
- [\[NetworkFirewall.9\] I firewall Network Firewall devono avere la protezione da eliminazione abilitata](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)
- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)
- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)
- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [I OpenSearch domini \[Opensearch.9\] devono essere etichettati](#)
- [Nei OpenSearch domini \[Opensearch.10\] deve essere installato l'ultimo aggiornamento software](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.1\] L'istanza RDS deve essere privata](#)
- [\[RDS.2\] Le istanze DB RDS dovrebbero vietare l'accesso pubblico, in base alla durata PubliclyAccessible AWS Config](#)
- [\[RDS.3\] Le istanze database RDS devono avere la crittografia dei dati inattivi abilitata](#)
- [\[RDS.4\] Le istantanee dei cluster RDS e le istantanee del database devono essere crittografate quando sono inattive](#)
- [\[RDS.5\] Le istanze DB RDS devono essere configurate con più zone di disponibilità](#)
- [\[RDS.6\] Il monitoraggio avanzato deve essere configurato per le istanze DB RDS](#)
- [\[RDS.7\] I cluster RDS devono avere la protezione da eliminazione abilitata](#)

- [\[RDS.8\] Le istanze DB RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.9\] Le istanze DB RDS devono pubblicare i log nei registri CloudWatch](#)
- [\[RDS.10\] L'autenticazione IAM deve essere configurata per le istanze RDS](#)
- [\[RDS.11\] Le istanze RDS devono avere i backup automatici abilitati](#)
- [\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)
- [\[RDS.13\] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)
- [\[RDS.16\] I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)
- [\[RDS.26\] Le istanze DB RDS devono essere protette da un piano di backup](#)
- [\[RDS.27\] I cluster RDS DB devono essere crittografati quando sono inattivi](#)
- [\[RDS.28\] I cluster RDS DB devono essere etichettati](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[RDS.34\] I cluster Aurora MySQL DB devono pubblicare i log di controllo nei registri CloudWatch](#)
- [\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Redshift.1\] I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico](#)
- [\[Redshift.2\] Le connessioni ai cluster Amazon Redshift devono essere crittografate in transito](#)
- [\[Redshift.3\] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate](#)
- [\[Redshift.6\] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati](#)
- [\[Redshift.7\] I cluster Redshift devono utilizzare un routing VPC avanzato](#)
- [\[Redshift.10\] I cluster Redshift devono essere crittografati a riposo](#)
- [\[Redshift.12\] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)
- [\[S3.5\] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL](#)

- [\[S3.6\] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS](#)
- [\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)
- [\[S3.9\] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata](#)
- [\[S3.15\] I bucket generici S3 devono avere Object Lock abilitato](#)
- [\[S3.17\] I bucket generici S3 devono essere crittografati quando sono inattivi con AWS KMS keys](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)
- [\[SageMaker.2\] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato](#)
- [\[SageMaker.3\] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[SES.1\] Gli elenchi di contatti SES devono essere etichettati](#)
- [\[SES.2\] I set di configurazione SES devono essere etichettati](#)
- [\[SecretsManager.2\] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SNS.1\] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS](#)
- [\[SNS.3\] Gli argomenti SNS devono essere etichettati](#)
- [\[SQS.1\] Le code di Amazon SQS devono essere crittografate quando sono inattive](#)
- [\[SQS.2\] Le code SQS devono essere etichettate](#)
- [\[SSM.1\] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager](#)
- [\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)
- [\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)
- [\[StepFunctions.1\] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata](#)
- [I AWS Transfer Family flussi di lavoro \[Transfer.1\] devono essere etichettati](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)

- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.2\] Le regole regionali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.4\] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.10\] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

Europa (Stoccolma)

I seguenti controlli non sono supportati in Europa (Stoccolma).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)

- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)

- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Europa (Zurigo)

I seguenti controlli non sono supportati in Europa (Zurigo).

- [\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)
- [\[ACM.2\] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit](#)
- [\[ApiGateway.1\] API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati](#)
- [\[ApiGateway.2\] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend](#)
- [\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione](#)
- [\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages](#)
- [\[AppSync.2\] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata](#)
- [\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)
- [\[Athena.2\] I cataloghi di dati Athena devono essere etichettati](#)
- [\[Athena.3\] I gruppi di lavoro Athena devono essere etichettati](#)
- [\[AutoScaling.1\] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB](#)
- [\[Autoscaling.5\] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici](#)
- [\[Backup.1\] i punti di AWS Backup ripristino devono essere crittografati a riposo](#)

- [\[Backup.2\] i punti di AWS Backup ripristino devono essere etichettati](#)
- [I AWS Backup vault \[Backup.3\] devono essere etichettati](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[Backup.5\] i piani di AWS Backup backup devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CloudTrail.6\] Assicurati che il bucket S3 utilizzato per archiviare i log non sia accessibile al pubblico CloudTrail](#)
- [\[CloudTrail.7\] Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)
- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)
- [\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)
- [\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)

- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)
- [\[DMS.2\] I certificati DMS devono essere etichettati](#)
- [\[DMS.3\] Le sottoscrizioni agli eventi DMS devono essere contrassegnate](#)
- [\[DMS.4\] Le istanze di replica DMS devono essere contrassegnate](#)
- [\[DMS.5\] I sottoreti di replica DMS devono essere etichettati](#)
- [\[DMS.6\] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato](#)
- [\[DMS.7\] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata](#)
- [\[DMS.8\] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata](#)
- [\[DMS.9\] Gli endpoint DMS devono utilizzare SSL](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.1\] Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda](#)
- [\[DynamoDB.2\] Le tabelle DynamoDB dovrebbero avere il ripristino abilitato point-in-time](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)

- [\[EC2.2\] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita](#)
- [\[EC2.3\] I volumi Amazon EBS collegati devono essere crittografati a riposo](#)
- [\[EC2.4\] Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato](#)
- [\[EC2.6\] La registrazione del flusso VPC deve essere abilitata in tutti i VPC](#)
- [\[EC2.8\] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 \(IMDSv2\)](#)
- [\[EC2.9\] Le istanze Amazon EC2 non devono avere un indirizzo IPv4 pubblico](#)
- [\[EC2.10\] Amazon EC2 deve essere configurato per utilizzare endpoint VPC creati per il servizio Amazon EC2](#)
- [\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22](#)
- [\[EC2.14\] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389](#)
- [\[EC2.15\] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici](#)
- [\[EC2.16\] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse](#)
- [\[EC2.17\] Le istanze Amazon EC2 non devono utilizzare più ENI](#)
- [\[EC2.18\] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate](#)
- [\[EC2.20\] Entrambi i tunnel VPN per una connessione VPN da sito a sito devono essere AWS attivi](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[EC2.25\] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete](#)
- [\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)
- [\[EC2.51\] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata](#)
- [\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)
- [\[ECR.2\] I repository privati ECR devono avere l'immutabilità dei tag configurata](#)
- [\[ECR.3\] I repository ECR devono avere almeno una politica del ciclo di vita configurata](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)

- [\[ECS.9\] Le definizioni delle attività ECS devono avere una configurazione di registrazione](#)
- [\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)
- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)
- [\[EFS.3\] I punti di accesso EFS devono applicare una directory principale](#)
- [\[EFS.4\] I punti di accesso EFS devono applicare un'identità utente](#)
- [\[EFS.5\] I punti di accesso EFS devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.2\] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[ELB.1\] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS](#)
- [\[ELB.2\] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager](#)
- [\[ELB.3\] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS](#)
- [\[ELB.4\] L'Application Load Balancer deve essere configurato per eliminare le intestazioni http](#)
- [\[ELB.8\] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita con una durata elevata AWS Config](#)
- [\[ELB.9\] I Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato](#)
- [\[ELB.14\] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF](#)
- [\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)
- [\[ElastiCache.6\] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH](#)
- [\[ElastiCache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)

- [\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)
- [\[ES.1\] I domini Elasticsearch devono avere la crittografia a riposo abilitata](#)
- [\[ES.2\] I domini Elasticsearch non devono essere accessibili al pubblico](#)
- [\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)
- [\[ES.4\] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch](#)
- [\[EventBridge.2\] i bus EventBridge degli eventi devono essere etichettati](#)
- [\[EventBridge.3\] i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[Glue.1\] i AWS Glue lavori devono essere etichettati](#)
- [\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)
- [\[GuardDuty.2\] GuardDuty i filtri devono essere etichettati](#)
- [\[GuardDuty.3\] Gli GuardDuty IPSet devono essere etichettati](#)
- [\[GuardDuty.4\] i GuardDuty rilevatori devono essere etichettati](#)
- [\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)
- [\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)
- [\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)
- [\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)
- [\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)
- [\[IAM.8\] Le credenziali utente IAM non utilizzate devono essere rimosse](#)
- [\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)
- [\[IAM.19\] L'MFA deve essere abilitata per tutti gli utenti IAM](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)

- [\[IAM.22\] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse](#)
- [\[IAM.24\] I ruoli IAM devono essere etichettati](#)
- [\[IAM.25\] Gli utenti IAM devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IAM.27\] Le identità IAM non devono avere la policy allegata AWSCloudShellFullAccess](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)
- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)
- [\[KMS.1\] Le politiche gestite dai clienti di IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS](#)
- [\[KMS.2\] I principali IAM non devono disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS](#)
- [\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)
- [\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)
- [\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[MQ.4\] I broker Amazon MQ devono essere etichettati](#)
- [\[MQ.5\] I broker ActiveMQ devono utilizzare la modalità di distribuzione attiva/standby](#)
- [\[MQ.6\] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster](#)
- [\[MSK.1\] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker](#)
- [\[MSK.2\] Per i cluster MSK dovrebbe essere configurato un monitoraggio avanzato](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)

- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)
- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.2\] La registrazione del Network Firewall deve essere abilitata](#)
- [\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)
- [\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)
- [\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)
- [\[NetworkFirewall.6\] Il gruppo di regole Stateless Network Firewall non deve essere vuoto](#)
- [\[NetworkFirewall.9\] I firewall Network Firewall devono avere la protezione da eliminazione abilitata](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)
- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)
- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)
- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [I OpenSearch domini \[Opensearch.9\] devono essere etichettati](#)
- [Nei OpenSearch domini \[Opensearch.10\] deve essere installato l'ultimo aggiornamento software](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.1\] L'istanza RDS deve essere privata](#)
- [\[RDS.3\] Le istanze database RDS devono avere la crittografia dei dati inattivi abilitata](#)
- [\[RDS.5\] Le istanze DB RDS devono essere configurate con più zone di disponibilità](#)

- [\[RDS.8\] Le istanze DB RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.16\] I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)
- [\[RDS.26\] Le istanze DB RDS devono essere protette da un piano di backup](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Redshift.3\] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate](#)
- [\[Redshift.12\] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)
- [\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)
- [\[SageMaker.2\] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato](#)
- [\[SageMaker.3\] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[SES.1\] Gli elenchi di contatti SES devono essere etichettati](#)
- [\[SES.2\] I set di configurazione SES devono essere etichettati](#)
- [\[SecretsManager.2\] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SNS.1\] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS](#)
- [\[SNS.3\] Gli argomenti SNS devono essere etichettati](#)

- [\[SQS.1\] Le code di Amazon SQS devono essere crittografate quando sono inattive](#)
- [\[SQS.2\] Le code SQS devono essere etichettate](#)
- [\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)
- [\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)
- [\[StepFunctions.1\] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata](#)
- [I AWS Transfer Family flussi di lavoro \[Transfer.1\] devono essere etichettati](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.2\] Le regole regionali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.4\] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.10\] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

Israele (Tel Aviv)

I seguenti controlli non sono supportati in Israele (Tel Aviv).

- [\[ACM.1\] I certificati importati ed emessi da ACM devono essere rinnovati dopo un periodo di tempo specificato](#)
- [\[ACM.2\] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit](#)
- [\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione](#)
- [\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages](#)
- [\[AppSync.2\] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata](#)

- [\[AppSync.4\] Le API AWS AppSync GraphQL devono essere taggate](#)
- [\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)
- [\[Athena.2\] I cataloghi di dati Athena devono essere etichettati](#)
- [\[Athena.3\] I gruppi di lavoro Athena devono essere etichettati](#)
- [\[Autoscaling.5\] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici](#)
- [\[Backup.1\] i punti di AWS Backup ripristino devono essere crittografati a riposo](#)
- [\[Backup.2\] i punti di AWS Backup ripristino devono essere etichettati](#)
- [I AWS Backup vault \[Backup.3\] devono essere etichettati](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[Backup.5\] i piani di AWS Backup backup devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)
- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)
- [\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)

- [\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)
- [\[DMS.2\] I certificati DMS devono essere etichettati](#)
- [\[DMS.3\] Le sottoscrizioni agli eventi DMS devono essere contrassegnate](#)
- [\[DMS.4\] Le istanze di replica DMS devono essere contrassegnate](#)
- [\[DMS.5\] I sottoreti di replica DMS devono essere etichettati](#)
- [\[DMS.6\] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato](#)
- [\[DMS.7\] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata](#)
- [\[DMS.8\] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata](#)
- [\[DMS.9\] Gli endpoint DMS devono utilizzare SSL](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.3\] I volumi Amazon EBS collegati devono essere crittografati a riposo](#)

- [\[EC2.4\] Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato](#)
- [\[EC2.6\] La registrazione del flusso VPC deve essere abilitata in tutti i VPC](#)
- [\[EC2.10\] Amazon EC2 deve essere configurato per utilizzare endpoint VPC creati per il servizio Amazon EC2](#)
- [\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22](#)
- [\[EC2.14\] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389](#)
- [\[EC2.18\] I gruppi di sicurezza devono consentire il traffico in entrata senza restrizioni solo per le porte autorizzate](#)
- [\[EC2.20\] Entrambi i tunnel VPN per una connessione VPN da sito a sito devono essere AWS attivi](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[EC2.25\] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete](#)
- [\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)
- [\[EC2.33\] Gli allegati del gateway di transito EC2 devono essere etichettati](#)
- [\[EC2.34\] Le tabelle delle rotte dei gateway di transito EC2 devono essere etichettate](#)
- [\[EC2.40\] I gateway NAT EC2 devono essere etichettati](#)
- [\[EC2.48\] I log di flusso di Amazon VPC devono essere etichettati](#)
- [\[EC2.51\] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata](#)
- [\[EC2.52\] I gateway di transito EC2 devono essere etichettati](#)
- [\[ECR.2\] I repository privati ECR devono avere l'immutabilità dei tag configurata](#)
- [\[ECR.3\] I repository ECR devono avere almeno una politica del ciclo di vita configurata](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)
- [\[ECS.9\] Le definizioni delle attività ECS devono avere una configurazione di registrazione](#)
- [\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)

- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)
- [\[EFS.3\] I punti di accesso EFS devono applicare una directory principale](#)
- [\[EFS.4\] I punti di accesso EFS devono applicare un'identità utente](#)
- [\[EFS.5\] I punti di accesso EFS devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.2\] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[EKS.6\] I cluster EKS devono essere etichettati](#)
- [\[EKS.7\] Le configurazioni dei provider di identità EKS devono essere contrassegnate](#)
- [\[EKS.8\] I cluster EKS devono avere la registrazione di controllo abilitata](#)
- [\[ELB.1\] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS](#)
- [\[ELB.2\] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager](#)
- [\[ELB.4\] L'Application Load Balancer deve essere configurato per eliminare le intestazioni http](#)
- [\[ELB.6\] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata](#)
- [\[ELB.8\] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita con una durata elevata AWS Config](#)
- [\[ELB.13\] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità](#)
- [\[ELB.14\] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF](#)
- [\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)
- [\[ElastiCache.2\] ElastiCache per i cluster di cache Redis dovrebbe avere l'aggiornamento automatico della versione secondaria abilitato](#)
- [\[ElastiCache.3\] ElastiCache per i gruppi di replica Redis dovrebbe avere il failover automatico abilitato](#)
- [\[ElastiCache.4\] ElastiCache per i gruppi di replica Redis deve essere crittografato a riposo](#)
- [\[ElastiCache.5\] ElastiCache per i gruppi di replica Redis devono essere crittografati in transito](#)

- [\[ElastiCache.6\] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH](#)
- [\[ElastiCache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)
- [\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)
- [\[ES.1\] I domini Elasticsearch devono avere la crittografia a riposo abilitata](#)
- [\[ES.2\] I domini Elasticsearch non devono essere accessibili al pubblico](#)
- [\[ES.3\] I domini Elasticsearch devono crittografare i dati inviati tra i nodi](#)
- [\[ES.4\] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch](#)
- [\[EventBridge.2\] i bus EventBridge degli eventi devono essere etichettati](#)
- [\[EventBridge.3\] i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)
- [\[GuardDuty.2\] GuardDuty i filtri devono essere etichettati](#)
- [\[GuardDuty.3\] Gli GuardDuty IPSet devono essere etichettati](#)
- [\[GuardDuty.4\] i GuardDuty rilevatori devono essere etichettati](#)
- [\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)
- [\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)
- [\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)
- [\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)
- [\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)

- [\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)
- [\[IAM.7\] Le politiche relative alle password per gli utenti IAM dovrebbero avere configurazioni solide](#)
- [\[IAM.8\] Le credenziali utente IAM non utilizzate devono essere rimosse](#)
- [\[IAM.9\] L'MFA deve essere abilitata per l'utente root](#)
- [\[IAM.10\] Le politiche relative alle password per gli utenti IAM dovrebbero avere durate elevate AWS Config](#)
- [\[IAM.11\] Assicuratevi che la politica delle password IAM richieda almeno una lettera maiuscola](#)
- [\[IAM.12\] Assicuratevi che la politica delle password IAM richieda almeno una lettera minuscola](#)
- [\[IAM.13\] Assicuratevi che la politica delle password IAM richieda almeno un simbolo](#)
- [\[IAM.14\] Assicuratevi che la politica delle password IAM richieda almeno un numero](#)
- [\[IAM.15\] Assicuratevi che la politica delle password di IAM richieda una lunghezza minima della password pari o superiore a 14](#)
- [\[IAM.16\] Assicuratevi che la politica delle password di IAM impedisca il riutilizzo delle password](#)
- [\[IAM.17\] Assicuratevi che la policy sulle password di IAM faccia scadere le password entro 90 giorni o meno](#)
- [\[IAM.18\] Assicuratevi che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)
- [\[IAM.19\] L'MFA deve essere abilitata per tutti gli utenti IAM](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)
- [\[IAM.22\] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse](#)
- [\[IAM.23\] Gli analizzatori IAM Access Analyzer devono essere etichettati](#)
- [\[IAM.24\] I ruoli IAM devono essere etichettati](#)
- [\[IAM.25\] Gli utenti IAM devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IAM.27\] Le identità IAM non devono avere la policy allegata AWSCloudShellFullAccess](#)
- [\[IAM.28\] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)

- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)
- [\[Kinesis.2\] Gli stream Kinesis devono essere etichettati](#)
- [\[KMS.1\] Le politiche gestite dai clienti di IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS](#)
- [\[KMS.2\] I principali IAM non devono disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS](#)
- [\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)
- [\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[MQ.4\] I broker Amazon MQ devono essere etichettati](#)
- [\[MQ.5\] I broker ActiveMQ devono utilizzare la modalità di distribuzione attiva/standby](#)
- [\[MQ.6\] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster](#)
- [\[MSK.1\] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker](#)
- [\[MSK.2\] Per i cluster MSK dovrebbe essere configurato un monitoraggio avanzato](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)
- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.2\] La registrazione del Network Firewall deve essere abilitata](#)
- [\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)

- [\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)
- [\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)
- [\[NetworkFirewall.6\] Il gruppo di regole Stateless Network Firewall non deve essere vuoto](#)
- [\[NetworkFirewall.9\] I firewall Network Firewall devono avere la protezione da eliminazione abilitata](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)
- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)
- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)
- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [I OpenSearch domini \[Opensearch.9\] devono essere etichettati](#)
- [Nei OpenSearch domini \[Opensearch.10\] deve essere installato l'ultimo aggiornamento software](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [L'autorità di certificazione AWS Private CA principale \[PCA.1\] deve essere disabilitata](#)
- [\[RDS.1\] L'istanza RDS deve essere privata](#)
- [\[RDS.4\] Le istantanee dei cluster RDS e le istantanee del database devono essere crittografate quando sono inattive](#)
- [\[RDS.7\] I cluster RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.8\] Le istanze DB RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)
- [\[RDS.16\] I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)

- [\[RDS.26\] Le istanze DB RDS devono essere protette da un piano di backup](#)
- [\[RDS.27\] I cluster RDS DB devono essere crittografati quando sono inattivi](#)
- [\[RDS.28\] I cluster RDS DB devono essere etichettati](#)
- [\[RDS.29\] Gli snapshot del cluster RDS DB devono essere etichettati](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[RDS.34\] I cluster Aurora MySQL DB devono pubblicare i log di controllo nei registri CloudWatch](#)
- [\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Redshift.3\] I cluster Amazon Redshift devono avere le istantanee automatiche abilitate](#)
- [\[Redshift.8\] I cluster Amazon Redshift non devono utilizzare il nome utente predefinito di amministratore](#)
- [\[Redshift.9\] I cluster Redshift non devono utilizzare il nome di database predefinito](#)
- [\[Redshift.12\] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)
- [\[S3.2\] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura](#)
- [\[S3.3\] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura](#)
- [\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)
- [\[S3.9\] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)
- [\[SageMaker.2\] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato](#)
- [\[SageMaker.3\] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[SES.1\] Gli elenchi di contatti SES devono essere etichettati](#)
- [\[SES.2\] I set di configurazione SES devono essere etichettati](#)

- [\[SecretsManager.1\] I segreti di Secrets Manager devono avere la rotazione automatica abilitata](#)
- [\[SecretsManager.2\] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente](#)
- [\[SecretsManager.3\] Rimuovi i segreti inutilizzati di Secrets Manager](#)
- [\[SecretsManager.4\] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SNS.1\] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS](#)
- [\[SNS.3\] Gli argomenti SNS devono essere etichettati](#)
- [\[SQS.1\] Le code di Amazon SQS devono essere crittografate quando sono inattive](#)
- [\[SQS.2\] Le code SQS devono essere etichettate](#)
- [\[SSM.1\] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager](#)
- [\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)
- [\[SSM.3\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità dell'associazione pari a COMPLIANT](#)
- [\[SSM.4\] I documenti SSM non devono essere pubblici](#)
- [\[StepFunctions.1\] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata](#)
- [\[StepFunctions.2\] Le attività di Step Functions devono essere etichettate](#)
- [I AWS Transfer Family flussi di lavoro \[Transfer.1\] devono essere etichettati](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.2\] Le regole regionali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.4\] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)
- [Le regole \[WAF.12\] devono avere le metriche abilitate AWS WAF CloudWatch](#)

Medio Oriente (Bahrein)

I seguenti controlli non sono supportati in Medio Oriente (Bahrain).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)

- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.20\] Entrambi i tunnel VPN per una connessione VPN da sito a sito devono essere AWS attivi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.7\] I cluster RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)
- [\[RDS.16\] I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee](#)

- [\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[Redshift.6\] Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali abilitati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SSM.2\] Le istanze Amazon EC2 gestite da Systems Manager devono avere uno stato di conformità delle patch pari a CONFORME dopo l'installazione della patch](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

Medio Oriente (Emirati Arabi Uniti)

I seguenti controlli non sono supportati in Medio Oriente (Emirati Arabi Uniti).

- [\[ACM.2\] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit](#)
- [\[ApiGateway.1\] API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati](#)
- [\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione](#)
- [\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages](#)
- [\[AppSync.2\] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata](#)

- [\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)
- [\[Athena.2\] I cataloghi di dati Athena devono essere etichettati](#)
- [\[Athena.3\] I gruppi di lavoro Athena devono essere etichettati](#)
- [\[AutoScaling.1\] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB](#)
- [\[Backup.1\] i punti di AWS Backup ripristino devono essere crittografati a riposo](#)
- [\[Backup.2\] i punti di AWS Backup ripristino devono essere etichettati](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[Backup.5\] i piani di AWS Backup backup devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CloudTrail.1\] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura](#)
- [\[CloudTrail.6\] Assicurati che il bucket S3 utilizzato per archiviare i log non sia accessibile al pubblico CloudTrail](#)
- [\[CloudWatch.15\] gli CloudWatch allarmi devono avere azioni specificate configurate](#)
- [\[CloudWatch.16\] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato](#)
- [\[CloudWatch.17\] le azioni di CloudWatch allarme devono essere attivate](#)

- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)
- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)
- [\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)
- [\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.1\] Le istanze di replica del Database Migration Service non devono essere pubbliche](#)
- [\[DMS.2\] I certificati DMS devono essere etichettati](#)
- [\[DMS.3\] Le sottoscrizioni agli eventi DMS devono essere contrassegnate](#)
- [\[DMS.4\] Le istanze di replica DMS devono essere contrassegnate](#)
- [\[DMS.5\] I sottoreti di replica DMS devono essere etichettati](#)
- [\[DMS.6\] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato](#)
- [\[DMS.7\] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata](#)
- [\[DMS.8\] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata](#)
- [\[DMS.9\] Gli endpoint DMS devono utilizzare SSL](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)

- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.3\] I volumi Amazon EBS collegati devono essere crittografati a riposo](#)
- [\[EC2.4\] Le istanze EC2 arrestate devono essere rimosse dopo un periodo di tempo specificato](#)
- [\[EC2.6\] La registrazione del flusso VPC deve essere abilitata in tutti i VPC](#)
- [\[EC2.8\] Le istanze EC2 devono utilizzare Instance Metadata Service Version 2 \(IMDSv2\)](#)
- [\[EC2.12\] Gli EIP Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.13\] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22](#)
- [\[EC2.14\] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[EC2.25\] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete](#)
- [\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)
- [\[EC2.51\] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata](#)
- [\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)
- [\[ECR.2\] I repository privati ECR devono avere l'immutabilità dei tag configurata](#)
- [\[ECR.3\] I repository ECR devono avere almeno una politica del ciclo di vita configurata](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)
- [\[ECS.9\] Le definizioni delle attività ECS devono avere una configurazione di registrazione](#)
- [\[EFS.1\] Elastic File System deve essere configurato per crittografare i dati dei file inattivi utilizzando AWS KMS](#)
- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)

- [\[EFS.3\] I punti di accesso EFS devono applicare una directory principale](#)
- [\[EFS.4\] I punti di accesso EFS devono applicare un'identità utente](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.2\] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[ELB.1\] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS](#)
- [\[ELB.3\] I listener Classic Load Balancer devono essere configurati con terminazione HTTPS o TLS](#)
- [\[ELB.9\] I Classic Load Balancer devono avere il bilanciamento del carico tra zone abilitato](#)
- [\[ELB.14\] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF](#)
- [\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)
- [\[ElastiCache.2\] ElastiCache per i cluster di cache Redis dovrebbe avere l'aggiornamento automatico della versione secondaria abilitato](#)
- [\[ElastiCache.3\] ElastiCache per i gruppi di replica Redis dovrebbe avere il failover automatico abilitato](#)
- [\[ElastiCache.4\] ElastiCache per i gruppi di replica Redis deve essere crittografato a riposo](#)
- [\[ElastiCache.5\] ElastiCache per i gruppi di replica Redis devono essere crittografati in transito](#)
- [\[ElastiCache.6\] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH](#)
- [\[ElastiCache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)
- [\[EMR.1\] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici](#)
- [\[EventBridge.2\] i bus EventBridge degli eventi devono essere etichettati](#)
- [\[EventBridge.3\] i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata](#)

- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)
- [\[GuardDuty.2\] GuardDuty i filtri devono essere etichettati](#)
- [\[GuardDuty.3\] Gli GuardDuty IPSet devono essere etichettati](#)
- [\[GuardDuty.4\] i GuardDuty rilevatori devono essere etichettati](#)
- [\[IAM.1\] Le politiche IAM non dovrebbero consentire privilegi amministrativi «*» completi](#)
- [\[IAM.2\] Gli utenti IAM non devono avere policy IAM allegate](#)
- [\[IAM.3\] Le chiavi di accesso degli utenti IAM devono essere ruotate ogni 90 giorni o meno](#)
- [\[IAM.4\] La chiave di accesso utente root IAM non dovrebbe esistere](#)
- [\[IAM.5\] MFA deve essere abilitata per tutti gli utenti IAM che dispongono di una password della console](#)
- [\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)
- [\[IAM.8\] Le credenziali utente IAM non utilizzate devono essere rimosse](#)
- [\[IAM.9\] L'MFA deve essere abilitata per l'utente root](#)
- [\[IAM.18\] Assicurati che sia stato creato un ruolo di supporto per gestire gli incidenti con AWS Support](#)
- [\[IAM.19\] L'MFA deve essere abilitata per tutti gli utenti IAM](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)
- [\[IAM.22\] Le credenziali utente IAM non utilizzate per 45 giorni devono essere rimosse](#)
- [\[IAM.24\] I ruoli IAM devono essere etichettati](#)
- [\[IAM.25\] Gli utenti IAM devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IAM.27\] Le identità IAM non devono avere la policy allegata AWSCloudShellFullAccess](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)

- [\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)
- [\[KMS.1\] Le politiche gestite dai clienti di IAM non dovrebbero consentire azioni di decrittografia su tutte le chiavi KMS](#)
- [\[KMS.2\] I principali IAM non devono disporre di policy IAM in linea che consentano azioni di decrittografia su tutte le chiavi KMS](#)
- [\[KMS.4\] la rotazione dei tasti dovrebbe essere abilitata AWS KMS](#)
- [\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)
- [\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)
- [\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[MSK.1\] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker](#)
- [\[MSK.2\] Per i cluster MSK dovrebbe essere configurato un monitoraggio avanzato](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)
- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.2\] La registrazione del Network Firewall deve essere abilitata](#)
- [\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)
- [\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)
- [\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)

- [\[NetworkFirewall.6\]](#) Il gruppo di regole Stateless Network Firewall non deve essere vuoto
- [\[NetworkFirewall.7\]](#) I firewall Network Firewall devono essere etichettati
- [\[NetworkFirewall.8\]](#) Le politiche firewall di Network Firewall devono essere etichettate
- [\[NetworkFirewall.9\]](#) I firewall Network Firewall devono avere la protezione da eliminazione abilitata
- [I OpenSearch domini \[Opensearch.1\]](#) devono avere la crittografia a riposo abilitata
- [I OpenSearch domini \[Opensearch.2\]](#) non devono essere accessibili al pubblico
- [I OpenSearch domini \[Opensearch.3\]](#) devono crittografare i dati inviati tra i nodi
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\]](#) nei log dovrebbe essere abilitata CloudWatch
- [I OpenSearch domini \[Opensearch.5\]](#) devono avere la registrazione di controllo abilitata
- [I OpenSearch domini \[Opensearch.6\]](#) devono avere almeno tre nodi di dati
- [I OpenSearch domini \[Opensearch.7\]](#) devono avere un controllo degli accessi granulare abilitato
- [\[Opensearch.8\]](#) Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS
- [I OpenSearch domini \[Opensearch.9\]](#) devono essere etichettati
- [Nei OpenSearch domini \[Opensearch.10\]](#) deve essere installato l'ultimo aggiornamento software
- [I OpenSearch domini \[Opensearch.11\]](#) devono avere almeno tre nodi primari dedicati
- [\[RDS.1\]](#) L'istanza RDS deve essere privata
- [\[RDS.2\]](#) Le istanze DB RDS dovrebbero vietare l'accesso pubblico, in base alla durata PubliclyAccessible AWS Config
- [\[RDS.3\]](#) Le istanze database RDS devono avere la crittografia dei dati inattivi abilitata
- [\[RDS.5\]](#) Le istanze DB RDS devono essere configurate con più zone di disponibilità
- [\[RDS.6\]](#) Il monitoraggio avanzato deve essere configurato per le istanze DB RDS
- [\[RDS.8\]](#) Le istanze DB RDS devono avere la protezione da eliminazione abilitata
- [\[RDS.11\]](#) Le istanze RDS devono avere i backup automatici abilitati
- [\[RDS.14\]](#) I cluster Amazon Aurora devono avere il backtracking abilitato
- [\[RDS.16\]](#) I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee
- [\[RDS.24\]](#) I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato
- [\[RDS.26\]](#) Le istanze DB RDS devono essere protette da un piano di backup
- [\[RDS.31\]](#) I gruppi di sicurezza RDS DB devono essere etichettati

- [\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Redshift.9\] I cluster Redshift non devono utilizzare il nome di database predefinito](#)
- [\[Redshift.12\] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[S3.2\] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura](#)
- [\[S3.3\] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura](#)
- [\[S3.5\] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL](#)
- [\[S3.6\] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS](#)
- [\[S3.14\] I bucket generici S3 devono avere il controllo delle versioni abilitato](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)
- [\[SageMaker.2\] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato](#)
- [\[SageMaker.3\] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[SES.1\] Gli elenchi di contatti SES devono essere etichettati](#)
- [\[SES.2\] I set di configurazione SES devono essere etichettati](#)
- [\[SecretsManager.1\] I segreti di Secrets Manager devono avere la rotazione automatica abilitata](#)
- [\[SecretsManager.2\] I segreti di Secrets Manager configurati con rotazione automatica dovrebbero ruotare correttamente](#)
- [\[SecretsManager.3\] Rimuovi i segreti inutilizzati di Secrets Manager](#)
- [\[SecretsManager.4\] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SNS.1\] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS](#)

- [\[SNS.3\] Gli argomenti SNS devono essere etichettati](#)
- [\[SQS.1\] Le code di Amazon SQS devono essere crittografate quando sono inattive](#)
- [\[SQS.2\] Le code SQS devono essere etichettate](#)
- [\[SSM.1\] Le istanze Amazon EC2 devono essere gestite da AWS Systems Manager](#)
- [\[StepFunctions.1\] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata](#)
- [I AWS Transfer Family flussi di lavoro \[Transfer.1\] devono essere etichettati](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.2\] Le regole regionali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.4\] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.10\] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)

Sud America (San Paolo)

I seguenti controlli non sono supportati in Sud America (San Paolo).

- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)

- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [\[RDS.7\] I cluster RDS devono avere la protezione da eliminazione abilitata](#)
- [\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)
- [\[RDS.16\] I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee](#)

- [\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)

AWS GovCloud (Stati Uniti orientali)

I seguenti controlli non sono supportati in AWS GovCloud (Stati Uniti orientali).

- [\[ACM.2\] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit](#)
- [\[ACM.3\] I certificati ACM devono essere etichettati](#)
- [\[Account.1\] Le informazioni di contatto di sicurezza devono essere fornite per un Account AWS](#)
- [\[Account.2\] Account AWS deve far parte di un'organizzazione AWS Organizations](#)
- [\[ApiGateway.2\] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend](#)
- [\[ApiGateway.3\] Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray](#)
- [\[ApiGateway.4\] L'API Gateway deve essere associato a un ACL Web WAF](#)
- [\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione](#)
- [\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages](#)

- [\[AppSync.2\] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata](#)
- [\[AppSync.4\] Le API AWS AppSync GraphQL devono essere taggate](#)
- [\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)
- [\[Athena.2\] I cataloghi di dati Athena devono essere etichettati](#)
- [\[Athena.3\] I gruppi di lavoro Athena devono essere etichettati](#)
- [\[AutoScaling.2\] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità](#)
- [\[AutoScaling.3\] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 \(IMDSv2\)](#)
- [\[AutoScaling.6\] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità](#)
- [\[AutoScaling.9\] I gruppi di Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2](#)
- [\[AutoScaling.10\] I gruppi di Auto Scaling EC2 devono essere etichettati](#)
- [\[Autoscaling.5\] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici](#)
- [\[Backup.2\] i punti di AWS Backup ripristino devono essere etichettati](#)
- [I AWS Backup vault \[Backup.3\] devono essere etichettati](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[Backup.5\] i piani di AWS Backup backup devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)

- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CloudTrail.9\] i percorsi devono essere etichettati CloudTrail](#)
- [\[CloudWatch.15\] gli CloudWatch allarmi devono avere azioni specificate configurate](#)
- [\[CloudWatch.16\] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato](#)
- [\[CloudWatch.17\] le azioni di CloudWatch allarme devono essere attivate](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)
- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)
- [\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)
- [\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.2\] I certificati DMS devono essere etichettati](#)
- [\[DMS.3\] Le sottoscrizioni agli eventi DMS devono essere contrassegnate](#)
- [\[DMS.4\] Le istanze di replica DMS devono essere contrassegnate](#)
- [\[DMS.5\] I sottoreti di replica DMS devono essere etichettati](#)
- [\[DMS.6\] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato](#)
- [\[DMS.7\] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata](#)
- [\[DMS.8\] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata](#)
- [\[DMS.9\] Gli endpoint DMS devono utilizzare SSL](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)

- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.1\] Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)
- [\[DynamoDB.5\] Le tabelle DynamoDB devono essere etichettate](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.15\] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici](#)
- [\[EC2.16\] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse](#)
- [\[EC2.17\] Le istanze Amazon EC2 non devono utilizzare più ENI](#)
- [\[EC2.21\] Gli ACL di rete non dovrebbero consentire l'ingresso dalla porta 0.0.0.0/0 alla porta 22 o alla porta 3389](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[EC2.25\] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete](#)
- [\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)
- [\[EC2.33\] Gli allegati del gateway di transito EC2 devono essere etichettati](#)
- [\[EC2.34\] Le tabelle delle rotte dei gateway di transito EC2 devono essere etichettate](#)
- [\[EC2.35\] Le interfacce di rete EC2 devono essere etichettate](#)
- [\[EC2.36\] I gateway per i clienti EC2 devono essere etichettati](#)
- [\[EC2.37\] Gli indirizzi IP elastici EC2 devono essere etichettati](#)
- [\[EC2.38\] Le istanze EC2 devono essere etichettate](#)

- [\[EC2.39\] I gateway Internet EC2 devono essere etichettati](#)
- [\[EC2.40\] I gateway NAT EC2 devono essere etichettati](#)
- [\[EC2.41\] Gli ACL di rete EC2 devono essere etichettati](#)
- [\[EC2.42\] Le tabelle di routing EC2 devono essere etichettate](#)
- [\[EC2.43\] I gruppi di sicurezza EC2 devono essere etichettati](#)
- [\[EC2.44\] Le sottoreti EC2 devono essere etichettate](#)
- [\[EC2.45\] I volumi EC2 devono essere etichettati](#)
- [\[EC2.46\] I VPC Amazon devono essere etichettati](#)
- [\[EC2.47\] I servizi endpoint Amazon VPC devono essere etichettati](#)
- [\[EC2.48\] I log di flusso di Amazon VPC devono essere etichettati](#)
- [\[EC2.49\] Le connessioni peering Amazon VPC devono essere etichettate](#)
- [\[EC2.50\] I gateway VPN EC2 devono essere etichettati](#)
- [\[EC2.52\] I gateway di transito EC2 devono essere etichettati](#)
- [\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)
- [\[ECR.2\] I repository privati ECR devono avere l'immutabilità dei tag configurata](#)
- [\[ECR.3\] I repository ECR devono avere almeno una politica del ciclo di vita configurata](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)
- [\[ECS.3\] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host](#)
- [\[ECS.4\] I contenitori ECS devono essere eseguiti come non privilegiati](#)
- [\[ECS.5\] I contenitori ECS devono essere limitati all'accesso in sola lettura ai filesystem root](#)
- [\[ECS.8\] I segreti non devono essere passati come variabili di ambiente del contenitore](#)
- [\[ECS.9\] Le definizioni delle attività ECS devono avere una configurazione di registrazione](#)
- [\[ECS.10\] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate](#)
- [\[ECS.12\] I cluster ECS devono utilizzare Container Insights](#)
- [\[ECS.13\] I servizi ECS devono essere etichettati](#)
- [\[ECS.14\] I cluster ECS devono essere etichettati](#)
- [\[ECS.15\] Le definizioni delle attività ECS devono essere contrassegnate](#)

- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)
- [\[EFS.3\] I punti di accesso EFS devono applicare una directory principale](#)
- [\[EFS.4\] I punti di accesso EFS devono applicare un'identità utente](#)
- [\[EFS.5\] I punti di accesso EFS devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.2\] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[EKS.6\] I cluster EKS devono essere etichettati](#)
- [\[EKS.7\] Le configurazioni dei provider di identità EKS devono essere contrassegnate](#)
- [\[EKS.8\] I cluster EKS devono avere la registrazione di controllo abilitata](#)
- [\[ELB.2\] I sistemi Classic Load Balancer con listener SSL/HTTPS devono utilizzare un certificato fornito da AWS Certificate Manager](#)
- [\[ELB.8\] I Classic Load Balancer con listener SSL devono utilizzare una politica di sicurezza predefinita con una durata elevata AWS Config](#)
- [\[ELB.10\] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità](#)
- [\[ELB.12\] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[ELB.13\] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità](#)
- [\[ELB.14\] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF](#)
- [\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)
- [\[ElastiCache.2\] ElastiCache per i cluster di cache Redis dovrebbe avere l'aggiornamento automatico della versione secondaria abilitato](#)
- [\[ElastiCache.3\] ElastiCache per i gruppi di replica Redis dovrebbe avere il failover automatico abilitato](#)
- [\[ElastiCache.4\] ElastiCache per i gruppi di replica Redis deve essere crittografato a riposo](#)
- [\[ElastiCache.5\] ElastiCache per i gruppi di replica Redis devono essere crittografati in transito](#)
- [\[ElastiCache.6\] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH](#)

- [\[ElastiCache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)
- [\[EMR.2\] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata](#)
- [\[ES.4\] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch](#)
- [\[ES.9\] I domini Elasticsearch devono essere etichettati](#)
- [\[EventBridge.2\] i bus EventBridge degli eventi devono essere etichettati](#)
- [\[EventBridge.3\] i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)
- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[Glue.1\] i AWS Glue lavori devono essere etichettati](#)
- [\[GuardDuty.1\] GuardDuty dovrebbe essere abilitato](#)
- [\[GuardDuty.2\] GuardDuty i filtri devono essere etichettati](#)
- [\[GuardDuty.3\] Gli GuardDuty IPSet devono essere etichettati](#)
- [\[GuardDuty.4\] i GuardDuty rilevatori devono essere etichettati](#)
- [\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)
- [\[IAM.9\] L'MFA deve essere abilitata per l'utente root](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)
- [\[IAM.23\] Gli analizzatori IAM Access Analyzer devono essere etichettati](#)
- [\[IAM.24\] I ruoli IAM devono essere etichettati](#)
- [\[IAM.25\] Gli utenti IAM devono essere etichettati](#)
- [\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi](#)

- [\[IAM.28\] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)
- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)
- [\[Kinesis.2\] Gli stream Kinesis devono essere etichettati](#)
- [\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)
- [\[Lambda.6\] Le funzioni Lambda devono essere etichettate](#)
- [\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)
- [\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[MQ.4\] I broker Amazon MQ devono essere etichettati](#)
- [\[MQ.5\] I broker ActiveMQ devono utilizzare la modalità di distribuzione attiva/standby](#)
- [\[MQ.6\] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster](#)
- [\[MSK.1\] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker](#)
- [\[MSK.2\] Per i cluster MSK dovrebbe essere configurato un monitoraggio avanzato](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)
- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità](#)

- [\[NetworkFirewall.2\] La registrazione del Network Firewall deve essere abilitata](#)
- [\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)
- [\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)
- [\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)
- [\[NetworkFirewall.6\] Il gruppo di regole Stateless Network Firewall non deve essere vuoto](#)
- [\[NetworkFirewall.7\] I firewall Network Firewall devono essere etichettati](#)
- [\[NetworkFirewall.8\] Le politiche firewall di Network Firewall devono essere etichettate](#)
- [\[NetworkFirewall.9\] I firewall Network Firewall devono avere la protezione da eliminazione abilitata](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)
- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)
- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)
- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [I OpenSearch domini \[Opensearch.9\] devono essere etichettati](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [L'autorità di certificazione AWS Private CA principale \[PCA.1\] deve essere disabilitata](#)
- [\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)
- [\[RDS.13\] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)
- [\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)
- [\[RDS.25\] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato](#)

- [\[RDS.26\] Le istanze DB RDS devono essere protette da un piano di backup](#)
- [\[RDS.27\] I cluster RDS DB devono essere crittografati quando sono inattivi](#)
- [\[RDS.28\] I cluster RDS DB devono essere etichettati](#)
- [\[RDS.29\] Gli snapshot del cluster RDS DB devono essere etichettati](#)
- [\[RDS.30\] Le istanze DB RDS devono essere etichettate](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[RDS.32\] Gli snapshot RDS DB devono essere etichettati](#)
- [\[RDS.33\] I gruppi di sottoreti RDS DB devono essere etichettati](#)
- [\[RDS.34\] I cluster Aurora MySQL DB devono pubblicare i log di controllo nei registri CloudWatch](#)
- [\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Redshift.7\] I cluster Redshift devono utilizzare un routing VPC avanzato](#)
- [\[Redshift.8\] I cluster Amazon Redshift non devono utilizzare il nome utente predefinito di amministratore](#)
- [\[Redshift.9\] I cluster Redshift non devono utilizzare il nome di database predefinito](#)
- [\[Redshift.10\] I cluster Redshift devono essere crittografati a riposo](#)
- [\[Redshift.11\] I cluster Redshift devono essere etichettati](#)
- [\[Redshift.12\] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate](#)
- [\[Redshift.13\] Le istantanee del cluster Redshift devono essere etichettate](#)
- [\[Redshift.14\] I gruppi di sottoreti del cluster Redshift devono essere etichettati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)
- [\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)
- [\[S3.10\] I bucket generici S3 con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita](#)
- [\[S3.11\] I bucket generici S3 devono avere le notifiche degli eventi abilitate](#)
- [\[S3.12\] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3](#)
- [\[S3.13\] I bucket generici S3 devono avere configurazioni del ciclo di vita](#)

- [\[S3.14\] I bucket generici S3 devono avere il controllo delle versioni abilitato](#)
- [\[S3.20\] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata](#)
- [\[SageMaker.1\] Le istanze di SageMaker notebook Amazon non devono avere accesso diretto a Internet](#)
- [\[SageMaker.2\] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato](#)
- [\[SageMaker.3\] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[SES.1\] Gli elenchi di contatti SES devono essere etichettati](#)
- [\[SES.2\] I set di configurazione SES devono essere etichettati](#)
- [\[SecretsManager.3\] Rimuovi i segreti inutilizzati di Secrets Manager](#)
- [\[SecretsManager.4\] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni](#)
- [\[SecretsManager.5\] I segreti di Secrets Manager devono essere etichettati](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SNS.3\] Gli argomenti SNS devono essere etichettati](#)
- [\[SQS.2\] Le code SQS devono essere etichettate](#)
- [\[SSM.4\] I documenti SSM non devono essere pubblici](#)
- [\[StepFunctions.1\] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata](#)
- [\[StepFunctions.2\] Le attività di Step Functions devono essere etichettate](#)
- [I AWS Transfer Family flussi di lavoro \[Transfer.1\] devono essere etichettati](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.2\] Le regole regionali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.4\] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)

- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.10\] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)
- [Le regole \[WAF.12\] devono avere le metriche abilitate AWS WAF CloudWatch](#)

AWS GovCloud (Stati Uniti occidentali)

I seguenti controlli non sono supportati in AWS GovCloud (Stati Uniti occidentali).

- [\[ACM.2\] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit](#)
- [\[ACM.3\] I certificati ACM devono essere etichettati](#)
- [\[Account.1\] Le informazioni di contatto di sicurezza devono essere fornite per un Account AWS](#)
- [\[Account.2\] Account AWS deve far parte di un'organizzazione AWS Organizations](#)
- [\[ApiGateway.2\] Le fasi API REST API Gateway devono essere configurate per utilizzare i certificati SSL per l'autenticazione del backend](#)
- [\[ApiGateway.3\] Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray](#)
- [\[ApiGateway.4\] L'API Gateway deve essere associato a un ACL Web WAF](#)
- [\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione](#)
- [\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages](#)
- [\[AppSync.2\] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata](#)
- [\[AppSync.4\] Le API AWS AppSync GraphQL devono essere taggate](#)
- [\[AppSync.5\] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API](#)
- [\[Athena.2\] I cataloghi di dati Athena devono essere etichettati](#)
- [\[Athena.3\] I gruppi di lavoro Athena devono essere etichettati](#)
- [\[AutoScaling.2\] Il gruppo Amazon EC2 Auto Scaling dovrebbe coprire più zone di disponibilità](#)
- [\[AutoScaling.3\] Le configurazioni di avvio del gruppo Auto Scaling devono configurare le istanze EC2 in modo che richiedano Instance Metadata Service Version 2 \(IMDSv2\)](#)
- [\[AutoScaling.6\] I gruppi di Auto Scaling devono utilizzare più tipi di istanze in più zone di disponibilità](#)
- [\[AutoScaling.9\] I gruppi di Amazon EC2 Auto Scaling devono utilizzare i modelli di lancio di Amazon EC2](#)

- [\[AutoScaling.10\] I gruppi di Auto Scaling EC2 devono essere etichettati](#)
- [\[Autoscaling.5\] Le istanze Amazon EC2 avviate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici](#)
- [\[Backup.2\] i punti di AWS Backup ripristino devono essere etichettati](#)
- [I AWS Backup vault \[Backup.3\] devono essere etichettati](#)
- [\[Backup.4\] i piani di AWS Backup report devono essere etichettati](#)
- [\[Backup.5\] i piani di AWS Backup backup devono essere etichettati](#)
- [\[CloudFormation.2\] CloudFormation gli stack devono essere etichettati](#)
- [\[CloudFront.1\] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato](#)
- [\[CloudFront.3\] CloudFront le distribuzioni dovrebbero richiedere la crittografia in transito](#)
- [\[CloudFront.4\] le CloudFront distribuzioni devono avere configurato il failover di origine](#)
- [\[CloudFront.5\] le CloudFront distribuzioni dovrebbero avere la registrazione abilitata](#)
- [\[CloudFront.6\] CloudFront le distribuzioni devono avere WAF abilitato](#)
- [\[CloudFront.7\] le CloudFront distribuzioni devono utilizzare certificati SSL/TLS personalizzati](#)
- [\[CloudFront.8\] le CloudFront distribuzioni devono utilizzare SNI per soddisfare le richieste HTTPS](#)
- [\[CloudFront.9\] le CloudFront distribuzioni devono crittografare il traffico verso origini personalizzate](#)
- [\[CloudFront.10\] CloudFront le distribuzioni non devono utilizzare protocolli SSL obsoleti tra edge location e origini personalizzate](#)
- [\[CloudFront.12\] CloudFront le distribuzioni non devono puntare a origini S3 inesistenti](#)
- [\[CloudFront.13\] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine](#)
- [\[CloudFront.14\] le distribuzioni devono essere etichettate CloudFront](#)
- [\[CloudTrail.9\] i percorsi devono essere etichettati CloudTrail](#)
- [\[CloudWatch.15\] gli CloudWatch allarmi devono avere azioni specificate configurate](#)
- [\[CloudWatch.16\] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato](#)
- [\[CloudWatch.17\] le azioni di CloudWatch allarme devono essere attivate](#)
- [\[CodeArtifact.1\] i CodeArtifact repository devono essere etichettati](#)
- [\[CodeBuild.1\] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili](#)
- [\[CodeBuild.2\] Le variabili di ambiente CodeBuild del progetto non devono contenere credenziali di testo non crittografato](#)

- [\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati](#)
- [\[CodeBuild.4\] Gli ambienti di CodeBuild progetto devono avere una durata di registrazione AWS Config](#)
- [\[DataFirehose.1\] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi](#)
- [\[Detective.1\] I grafici del comportamento dei Detective devono essere etichettati](#)
- [\[DMS.2\] I certificati DMS devono essere etichettati](#)
- [\[DMS.3\] Le sottoscrizioni agli eventi DMS devono essere contrassegnate](#)
- [\[DMS.4\] Le istanze di replica DMS devono essere contrassegnate](#)
- [\[DMS.5\] I sottoreti di replica DMS devono essere etichettati](#)
- [\[DMS.6\] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato](#)
- [\[DMS.7\] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata](#)
- [\[DMS.8\] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata](#)
- [\[DMS.9\] Gli endpoint DMS devono utilizzare SSL](#)
- [\[DMS.10\] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata](#)
- [\[DMS.11\] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato](#)
- [\[DMS.12\] Gli endpoint DMS per Redis devono avere TLS abilitato](#)
- [\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi](#)
- [\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato](#)
- [\[DocumentDB.3\] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche](#)
- [\[DocumentDB.4\] I cluster Amazon DocumentDB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[DocumentDB.5\] I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata](#)
- [\[DynamoDB.1\] Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda](#)
- [\[DynamoDB.3\] I cluster DynamoDB Accelerator \(DAX\) devono essere crittografati quando sono inattivi](#)
- [\[DynamoDB.4\] Le tabelle DynamoDB devono essere presenti in un piano di backup](#)

- [\[DynamoDB.5\] Le tabelle DynamoDB devono essere etichettate](#)
- [\[DynamoDB.7\] I cluster DynamoDB Accelerator devono essere crittografati in transito](#)
- [\[EC2.15\] Le sottoreti Amazon EC2 non devono assegnare automaticamente indirizzi IP pubblici](#)
- [\[EC2.16\] Le liste di controllo degli accessi alla rete non utilizzate devono essere rimosse](#)
- [\[EC2.17\] Le istanze Amazon EC2 non devono utilizzare più ENI](#)
- [\[EC2.21\] Gli ACL di rete non dovrebbero consentire l'ingresso dalla porta 0.0.0.0/0 alla porta 22 o alla porta 3389](#)
- [\[EC2.22\] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi](#)
- [\[EC2.23\] I gateway di transito Amazon EC2 non devono accettare automaticamente le richieste di allegati VPC](#)
- [\[EC2.24\] I tipi di istanze paravirtuali di Amazon EC2 non devono essere utilizzati](#)
- [\[EC2.25\] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete](#)
- [\[EC2.28\] I volumi EBS devono essere coperti da un piano di backup](#)
- [\[EC2.33\] Gli allegati del gateway di transito EC2 devono essere etichettati](#)
- [\[EC2.34\] Le tabelle delle rotte dei gateway di transito EC2 devono essere etichettate](#)
- [\[EC2.35\] Le interfacce di rete EC2 devono essere etichettate](#)
- [\[EC2.36\] I gateway per i clienti EC2 devono essere etichettati](#)
- [\[EC2.37\] Gli indirizzi IP elastici EC2 devono essere etichettati](#)
- [\[EC2.38\] Le istanze EC2 devono essere etichettate](#)
- [\[EC2.39\] I gateway Internet EC2 devono essere etichettati](#)
- [\[EC2.40\] I gateway NAT EC2 devono essere etichettati](#)
- [\[EC2.41\] Gli ACL di rete EC2 devono essere etichettati](#)
- [\[EC2.42\] Le tabelle di routing EC2 devono essere etichettate](#)
- [\[EC2.43\] I gruppi di sicurezza EC2 devono essere etichettati](#)
- [\[EC2.44\] Le sottoreti EC2 devono essere etichettate](#)
- [\[EC2.45\] I volumi EC2 devono essere etichettati](#)
- [\[EC2.46\] I VPC Amazon devono essere etichettati](#)
- [\[EC2.47\] I servizi endpoint Amazon VPC devono essere etichettati](#)
- [\[EC2.48\] I log di flusso di Amazon VPC devono essere etichettati](#)
- [\[EC2.49\] Le connessioni peering Amazon VPC devono essere etichettate](#)
- [\[EC2.50\] I gateway VPN EC2 devono essere etichettati](#)

- [\[EC2.52\] I gateway di transito EC2 devono essere etichettati](#)
- [\[ECR.1\] Gli archivi privati ECR devono avere la scansione delle immagini configurata](#)
- [\[ECR.2\] I repository privati ECR devono avere l'immutabilità dei tag configurata](#)
- [\[ECR.3\] I repository ECR devono avere almeno una politica del ciclo di vita configurata](#)
- [\[ECR.4\] Gli archivi pubblici ECR devono essere etichettati](#)
- [\[ECS.1\] Le definizioni delle attività di Amazon ECS devono avere modalità di rete e definizioni utente sicure.](#)
- [\[ECS.3\] Le definizioni delle attività ECS non devono condividere lo spazio dei nomi dei processi dell'host](#)
- [\[ECS.4\] I contenitori ECS devono essere eseguiti come non privilegiati](#)
- [\[ECS.5\] I contenitori ECS devono essere limitati all'accesso in sola lettura ai filesystem root](#)
- [\[ECS.8\] I segreti non devono essere passati come variabili di ambiente del contenitore](#)
- [\[ECS.9\] Le definizioni delle attività ECS devono avere una configurazione di registrazione](#)
- [\[ECS.10\] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate](#)
- [\[ECS.12\] I cluster ECS devono utilizzare Container Insights](#)
- [\[ECS.13\] I servizi ECS devono essere etichettati](#)
- [\[ECS.14\] I cluster ECS devono essere etichettati](#)
- [\[ECS.15\] Le definizioni delle attività ECS devono essere contrassegnate](#)
- [\[EFS.2\] I volumi Amazon EFS devono essere inclusi nei piani di backup](#)
- [\[EFS.3\] I punti di accesso EFS devono applicare una directory principale](#)
- [\[EFS.4\] I punti di accesso EFS devono applicare un'identità utente](#)
- [\[EFS.5\] I punti di accesso EFS devono essere etichettati](#)
- [\[EFS.6\] I target di montaggio EFS non devono essere associati a una sottorete pubblica](#)
- [\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico](#)
- [\[EKS.2\] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata](#)
- [\[EKS.3\] I cluster EKS devono utilizzare segreti Kubernetes crittografati](#)
- [\[EKS.6\] I cluster EKS devono essere etichettati](#)
- [\[EKS.7\] Le configurazioni dei provider di identità EKS devono essere contrassegnate](#)
- [\[EKS.8\] I cluster EKS devono avere la registrazione di controllo abilitata](#)
- [\[ELB.10\] Classic Load Balancer dovrebbe estendersi su più zone di disponibilità](#)

- [\[ELB.12\] Application Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[ELB.13\] I Load Balancer per applicazioni, reti e gateway devono estendersi su più zone di disponibilità](#)
- [\[ELB.14\] Classic Load Balancer deve essere configurato con la modalità di mitigazione della desincronizzazione difensiva o più rigorosa](#)
- [\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF](#)
- [\[ElastiCache.1\] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato](#)
- [\[ElastiCache.2\] ElastiCache per i cluster di cache Redis dovrebbe avere l'aggiornamento automatico della versione secondaria abilitato](#)
- [\[ElastiCache.3\] ElastiCache per i gruppi di replica Redis dovrebbe avere il failover automatico abilitato](#)
- [\[ElastiCache.4\] ElastiCache per i gruppi di replica Redis deve essere crittografato a riposo](#)
- [\[ElastiCache.5\] ElastiCache per i gruppi di replica Redis devono essere crittografati in transito](#)
- [\[ElastiCache.6\] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0 è necessario utilizzare Redis AUTH](#)
- [\[ElastiCache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito](#)
- [\[ElasticBeanstalk.1\] Gli ambienti Elastic Beanstalk dovrebbero avere la reportistica sullo stato avanzata abilitata](#)
- [\[ElasticBeanstalk.2\] Gli aggiornamenti della piattaforma gestita da Elastic Beanstalk devono essere abilitati](#)
- [\[ElasticBeanstalk.3\] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch](#)
- [\[EMR.2\] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata](#)
- [\[ES.4\] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch](#)
- [\[ES.9\] I domini Elasticsearch devono essere etichettati](#)
- [\[EventBridge.2\] i bus EventBridge degli eventi devono essere etichettati](#)
- [\[EventBridge.3\] i bus di eventi EventBridge personalizzati devono avere una politica basata sulle risorse allegata](#)
- [\[EventBridge.4\] gli endpoint EventBridge globali dovrebbero avere la replica degli eventi abilitata](#)
- [\[FSx.1\] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi](#)

- [\[FSX.2\] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup](#)
- [\[GlobalAccelerator.1\] Gli acceleratori Global Accelerator devono essere etichettati](#)
- [\[Glue.1\] i AWS Glue lavori devono essere etichettati](#)
- [\[GuardDuty.2\] GuardDuty i filtri devono essere etichettati](#)
- [\[GuardDuty.3\] Gli GuardDuty IPSet devono essere etichettati](#)
- [\[GuardDuty.4\] i GuardDuty rilevatori devono essere etichettati](#)
- [\[IAM.6\] L'autenticazione MFA per l'hardware deve essere abilitata per l'utente root](#)
- [\[IAM.9\] L'MFA deve essere abilitata per l'utente root](#)
- [\[IAM.21\] Le policy gestite dai clienti IAM che create non dovrebbero consentire azioni jolly per i servizi](#)
- [\[IAM.23\] Gli analizzatori IAM Access Analyzer devono essere etichettati](#)
- [\[IAM.24\] I ruoli IAM devono essere etichettati](#)
- [\[IAM.25\] Gli utenti IAM devono essere etichettati](#)
- [\[IAM.28\] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato](#)
- [\[IoT.1\] i profili di AWS IoT Core sicurezza devono essere etichettati](#)
- [\[IoT.2\] le azioni di AWS IoT Core mitigazione devono essere etichettate](#)
- [\[IoT.3\] le AWS IoT Core dimensioni devono essere etichettate](#)
- [gli AWS IoT Core autorizzatori \[IoT.4\] devono essere etichettati](#)
- [\[IoT.5\] gli alias dei AWS IoT Core ruoli devono essere etichettati](#)
- [\[IoT.6\] AWS IoT Core le politiche devono essere etichettate](#)
- [\[Kinesis.1\] Gli stream Kinesis devono essere crittografati quando sono inattivi](#)
- [\[Kinesis.2\] Gli stream Kinesis devono essere etichettati](#)
- [\[Lambda.5\] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità](#)
- [\[Lambda.6\] Le funzioni Lambda devono essere etichettate](#)
- [\[Macie.1\] Amazon Macie dovrebbe essere abilitato](#)
- [\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie deve essere abilitato](#)
- [\[MQ.2\] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch](#)
- [\[MQ.3\] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[MQ.4\] I broker Amazon MQ devono essere etichettati](#)
- [\[MQ.5\] I broker ActiveMQ devono utilizzare la modalità di distribuzione attiva/standby](#)

- [\[MQ.6\] I broker RabbitMQ dovrebbero utilizzare la modalità di distribuzione del cluster](#)
- [\[MSK.1\] I cluster MSK devono essere crittografati durante il transito tra i nodi del broker](#)
- [\[MSK.2\] Per i cluster MSK dovrebbe essere configurato un monitoraggio avanzato](#)
- [\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo](#)
- [\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch](#)
- [\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche](#)
- [\[Neptune.4\] I cluster Neptune DB devono avere la protezione da eliminazione abilitata](#)
- [\[Neptune.5\] I cluster Neptune DB devono avere i backup automatici abilitati](#)
- [\[Neptune.6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive](#)
- [\[Neptune.7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata](#)
- [\[Neptune.8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee](#)
- [\[Neptune.9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità](#)
- [\[NetworkFirewall.2\] La registrazione del Network Firewall deve essere abilitata](#)
- [\[NetworkFirewall.3\] Le policy di Network Firewall devono avere almeno un gruppo di regole associato](#)
- [\[NetworkFirewall.4\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per pacchetti completi](#)
- [\[NetworkFirewall.5\] L'azione stateless predefinita per le policy del Network Firewall dovrebbe essere drop or forward per i pacchetti frammentati](#)
- [\[NetworkFirewall.6\] Il gruppo di regole Stateless Network Firewall non deve essere vuoto](#)
- [\[NetworkFirewall.7\] I firewall Network Firewall devono essere etichettati](#)
- [\[NetworkFirewall.8\] Le politiche firewall di Network Firewall devono essere etichettate](#)
- [\[NetworkFirewall.9\] I firewall Network Firewall devono avere la protezione da eliminazione abilitata](#)
- [I OpenSearch domini \[Opensearch.1\] devono avere la crittografia a riposo abilitata](#)
- [I OpenSearch domini \[Opensearch.2\] non devono essere accessibili al pubblico](#)
- [I OpenSearch domini \[Opensearch.3\] devono crittografare i dati inviati tra i nodi](#)
- [La registrazione degli errori del OpenSearch dominio \[Opensearch.4\] nei log dovrebbe essere abilitata CloudWatch](#)
- [I OpenSearch domini \[Opensearch.5\] devono avere la registrazione di controllo abilitata](#)
- [I OpenSearch domini \[Opensearch.6\] devono avere almeno tre nodi di dati](#)

- [I OpenSearch domini \[Opensearch.7\] devono avere un controllo degli accessi granulare abilitato](#)
- [\[Opensearch.8\] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS](#)
- [I OpenSearch domini \[Opensearch.9\] devono essere etichettati](#)
- [I OpenSearch domini \[Opensearch.11\] devono avere almeno tre nodi primari dedicati](#)
- [L'autorità di certificazione AWS Private CA principale \[PCA.1\] deve essere disabilitata](#)
- [\[RDS.12\] L'autenticazione IAM deve essere configurata per i cluster RDS](#)
- [\[RDS.13\] Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere abilitati](#)
- [\[RDS.14\] I cluster Amazon Aurora devono avere il backtracking abilitato](#)
- [\[RDS.15\] I cluster RDS DB devono essere configurati per più zone di disponibilità](#)
- [\[RDS.24\] I cluster di database RDS devono utilizzare un nome utente di amministratore personalizzato](#)
- [\[RDS.25\] Le istanze del database RDS devono utilizzare un nome utente amministratore personalizzato](#)
- [\[RDS.26\] Le istanze DB RDS devono essere protette da un piano di backup](#)
- [\[RDS.27\] I cluster RDS DB devono essere crittografati quando sono inattivi](#)
- [\[RDS.28\] I cluster RDS DB devono essere etichettati](#)
- [\[RDS.29\] Gli snapshot del cluster RDS DB devono essere etichettati](#)
- [\[RDS.30\] Le istanze DB RDS devono essere etichettate](#)
- [\[RDS.31\] I gruppi di sicurezza RDS DB devono essere etichettati](#)
- [\[RDS.32\] Gli snapshot RDS DB devono essere etichettati](#)
- [\[RDS.33\] I gruppi di sottoreti RDS DB devono essere etichettati](#)
- [\[RDS.34\] I cluster Aurora MySQL DB devono pubblicare i log di controllo nei registri CloudWatch](#)
- [\[RDS.35\] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie](#)
- [\[Redshift.7\] I cluster Redshift devono utilizzare un routing VPC avanzato](#)
- [\[Redshift.8\] I cluster Amazon Redshift non devono utilizzare il nome utente predefinito di amministratore](#)
- [\[Redshift.9\] I cluster Redshift non devono utilizzare il nome di database predefinito](#)
- [\[Redshift.10\] I cluster Redshift devono essere crittografati a riposo](#)
- [\[Redshift.11\] I cluster Redshift devono essere etichettati](#)

- [\[Redshift.12\] Le sottoscrizioni alle notifiche degli eventi Redshift devono essere contrassegnate](#)
- [\[Redshift.13\] Le istantanee del cluster Redshift devono essere etichettate](#)
- [\[Redshift.14\] I gruppi di sottoreti del cluster Redshift devono essere etichettati](#)
- [\[Redshift.15\] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate](#)
- [\[Route53.1\] I controlli sanitari della Route 53 devono essere etichettati](#)
- [\[Route53.2\] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS](#)
- [\[S3.1\] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate](#)
- [\[S3.8\] I bucket generici S3 dovrebbero bloccare l'accesso pubblico](#)
- [\[S3.10\] I bucket generici S3 con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita](#)
- [\[S3.11\] I bucket generici S3 devono avere le notifiche degli eventi abilitate](#)
- [\[S3.12\] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3](#)
- [\[S3.13\] I bucket generici S3 devono avere configurazioni del ciclo di vita](#)
- [\[S3.14\] I bucket generici S3 devono avere il controllo delle versioni abilitato](#)
- [\[S3.20\] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata](#)
- [\[SageMaker.2\] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato](#)
- [\[SageMaker.3\] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook](#)
- [\[SageMaker.4\] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1](#)
- [\[SES.1\] Gli elenchi di contatti SES devono essere etichettati](#)
- [\[SES.2\] I set di configurazione SES devono essere etichettati](#)
- [\[SecretsManager.3\] Rimuovi i segreti inutilizzati di Secrets Manager](#)
- [\[SecretsManager.4\] I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni](#)
- [\[SecretsManager.5\] I segreti di Secrets Manager devono essere etichettati](#)
- [\[ServiceCatalog.1\] I portafogli Service Catalog devono essere condivisi solo all'interno di un'organizzazione AWS](#)
- [\[SNS.3\] Gli argomenti SNS devono essere etichettati](#)
- [\[SQS.2\] Le code SQS devono essere etichettate](#)

- [\[SSM.4\] I documenti SSM non devono essere pubblici](#)
- [\[StepFunctions.1\] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata](#)
- [\[StepFunctions.2\] Le attività di Step Functions devono essere etichettate](#)
- [I AWS Transfer Family flussi di lavoro \[Transfer.1\] devono essere etichettati](#)
- [\[Transfer.2\] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint](#)
- [\[WAF.1\] La registrazione AWS WAF classica Global Web ACL deve essere abilitata](#)
- [\[WAF.2\] Le regole regionali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.3\] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.4\] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.6\] Le regole globali AWS WAF classiche devono avere almeno una condizione](#)
- [\[WAF.7\] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola](#)
- [\[WAF.8\] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.10\] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole](#)
- [\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF](#)
- [Le regole \[WAF.12\] devono avere le metriche abilitate AWS WAF CloudWatch](#)

Disabilitazione del Security Hub

Note

Se si utilizza la configurazione centrale, l'amministratore delegato AWS di Security Hub può creare policy di configurazione che disabilitano Security Hub in account e unità organizzative (OU) specifici e lo mantengono abilitato in altri. Le politiche di configurazione hanno effetto nella regione di origine e in tutte le regioni collegate. Per ulteriori informazioni, consulta [Come funziona la configurazione centrale](#).

È possibile utilizzare la console Security Hub, l'API Security Hub o AWS CLI disabilitare Security Hub.

Quando si disattiva Security Hub per un account, si verifica quanto segue:

- Non sono in corso nuove scoperte per l'account.
- Dopo 90 giorni, i risultati e gli approfondimenti esistenti e tutte le impostazioni di configurazione del Security Hub vengono eliminati e non possono essere ripristinati.

Se desideri salvare i risultati esistenti, devi esportarli prima di disabilitare Security Hub. Per ulteriori informazioni, consulta [the section called "Effetto delle azioni dell'account sui dati del Security Hub"](#).

- Tutti gli standard e i controlli abilitati sono disabilitati.

Non puoi disabilitare Security Hub nei seguenti casi:

- Il tuo account è l'account amministratore di Security Hub designato per un'organizzazione. Se si utilizza la configurazione centrale, non è possibile associare una politica di configurazione che disabiliti Security Hub all'account amministratore delegato. L'associazione può avere successo per altri account, ma Security Hub non applica tale politica all'account amministratore delegato.
- Il tuo account è un account amministratore di Security Hub su invito e disponi di account membro abilitati. Prima di poter disattivare Security Hub, devi dissociare tutti i tuoi account membro. Consulta [the section called "Dissociazione degli account dei membri"](#).

Prima di poter disabilitare Security Hub per un account membro, è necessario dissociare l'account dal relativo account amministratore. Per un account dell'organizzazione, solo l'account amministratore può dissociare gli account dei membri. Per ulteriori informazioni, consulta [the section called](#)

[“Dissociazione degli account dei membri dell'organizzazione”](#). Per gli account invitati manualmente, l'account amministratore o l'account membro possono dissociare l'account membro. Per ulteriori informazioni, consulta [the section called “Dissociazione degli account dei membri”](#) o [the section called “Dissociarsi dal proprio account amministratore”](#). La dissociazione non è richiesta se si utilizza la configurazione centrale perché è possibile creare una politica che disabilita Security Hub in account membri specifici.

Quando disabiliti Security Hub in un account, viene disabilitato solo nella regione corrente. Tuttavia, se si utilizza la configurazione centrale per disabilitare Security Hub in account specifici, viene disabilitato nella regione di origine e in tutte le regioni collegate.

Scegli il tuo metodo preferito e segui i passaggi per disabilitare Security Hub.

Security Hub console

Per disabilitare Security Hub

1. Aprire la console AWS Security Hub all'[indirizzo https://console.aws.amazon.com/securityhub/](https://console.aws.amazon.com/securityhub/).
2. Nel riquadro di navigazione, seleziona Impostazioni.
3. Nella pagina Impostazioni, scegli Generale.
4. In Disabilita AWS Security Hub, scegli Disabilita AWS Security Hub. Quindi scegli nuovamente Disabilita AWS Security Hub.

Security Hub API

Per disabilitare Security Hub

Invoca l'[DisableSecurityHubAPI](#).

AWS CLI

Per disabilitare Security Hub

Esegui il comando [disable-security-hub](#).

Comando di esempio:

```
aws securityhub disable-security-hub
```

Registro delle modifiche per i controlli del Security Hub

Il seguente registro delle modifiche tiene traccia delle modifiche sostanziali ai controlli di AWS Security Hub sicurezza esistenti, che possono comportare modifiche allo stato generale di un controllo e allo stato di conformità dei risultati. Per informazioni su come Security Hub valuta lo stato del controllo, vedere [Stato di conformità e stato di controllo](#). Le modifiche possono richiedere alcuni giorni dopo la loro immissione in questo registro per avere effetto su tutte le Regioni AWS aree in cui il controllo è disponibile.

Questo registro tiene traccia delle modifiche avvenute dall'aprile 2023.

Seleziona un controllo per visualizzarne ulteriori dettagli. Le modifiche al titolo vengono annotate nella descrizione dettagliata di ogni controllo per 90 giorni.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
8 maggio 2024	[S3.20] I bucket S3 per uso generico devono avere l'eliminazione MFA abilitata	Questo controllo verifica se un bucket con versione generica di Amazon S3 è abilitata l'eliminazione dell'autenticazione a più fattori (MFA). In precedenza, il controllo produceva una FAILED ricerca di bucket con una configurazione del ciclo di vita. Tuttavia, l'eliminazione MFA con controllo delle versioni non può essere abilitata su un bucket con una configurazione del ciclo di vita. Security

Data di modifica	ID e titolo del controllo	Descrizione della modifica
		<p>Hub ha aggiornato il controllo per non produrre risultati per i bucket con una configurazione del ciclo di vita. La descrizione del controllo è stata aggiornata per riflettere il comportamento corrente.</p>
2 maggio 2024	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	<p>Security Hub ha aggiornato la versione più vecchia supportata di Kubernetes su cui può essere eseguito il cluster Amazon EKS per produrre un risultato superato. La versione più vecchia attualmente supportata è Kubernetes. 1.26</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
30 aprile 2024	[CloudTrail.3] Almeno un trail deve essere abilitato CloudTrail	<p>Il titolo di controllo modificato da CloudTrail dovrebbe essere abilitato a Dovrebbe essere abilitato almeno un CloudTrail percorso. Questo controllo attualmente produce un PASSED risultato se un Account AWS ha almeno un CloudTrail percorso abilitato. Il titolo e la descrizione sono stati modificati per riflettere accuratamente il comportamento attuale.</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
29 aprile 2024	[AutoScaling.1] I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli di integrità ELB	<p>La modifica del titolo di controllo dai gruppi Auto Scaling associati a un Classic Load Balancer dovrebbe utilizzare i controlli dello stato del bilanciamento del carico, mentre i gruppi Auto Scaling associati a un sistema di bilanciamento del carico dovrebbero utilizzare i controlli di integrità ELB. Questo controllo attualmente valuta Application, Gateway, Network e Classic Load Balancer. Il titolo e la descrizione sono stati modificati per riflettere accuratamente il comportamento corrente.</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
19 aprile 2024	[CloudTrail.1] CloudTrail deve essere abilitato e configurato con almeno un percorso multiregionale che includa eventi di gestione di lettura e scrittura	<p>Il controllo verifica se AWS CloudTrail è abilitato e configurato con almeno un percorso multiregionale che include eventi di gestione di lettura e scrittura . In precedenza, il controllo generava erroneamente PASSED i risultati quando un account aveva CloudTrail abilitato e configurato almeno un percorso multiregionale, anche se nessun trail includeva eventi di gestione di lettura e scrittura. Il controllo ora genera un PASSED risultato solo quando CloudTrail è abilitato e configurato con almeno un percorso multiregionale che acquisisce gli eventi di gestione di lettura e scrittura.</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 aprile 2024	[Athena.1] I gruppi di lavoro Athena devono essere crittografati quando sono inattivi	Security Hub ha ritirato questo controllo e lo ha rimosso da tutti gli standard. I gruppi di lavoro Athena inviano i log ai bucket Amazon Simple Storage Service (Amazon S3). Amazon S3 ora fornisce la crittografia predefinita con chiavi gestite S3 (SS3-S3) su bucket S3 nuovi ed esistenti.
10 aprile 2024	[AutoScaling.4] La configurazione di avvio del gruppo Auto Scaling non deve avere un limite di hop di risposta ai metadati superiore a 1	Security Hub ha ritirato questo controllo e lo ha rimosso da tutti gli standard. I limiti degli hop di risposta ai metadati per le istanze Amazon Elastic Compute Cloud (Amazon EC2) dipendono dal carico di lavoro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 aprile 2024	[CloudFormation.1] gli CloudFormation stack devono essere integrati con Simple Notification Service (SNS)	Security Hub ha ritirato questo controllo e lo ha rimosso da tutti gli standard. L'integrazione degli AWS CloudFormation stack con gli argomenti di Amazon SNS non è più una best practice di sicurezza. Sebbene l'integrazione di CloudFormation stack importanti con argomenti SNS possa essere utile, non è necessaria per tutti gli stack.
10 aprile 2024	[CodeBuild.5] gli ambienti di CodeBuild progetto non dovrebbero avere la modalità privilegiata abilitata	Security Hub ha ritirato questo controllo e lo ha rimosso da tutti gli standard. L'attivazione della modalità privilegiata in un CodeBuild progetto non comporta un rischio aggiuntivo per l'ambiente del cliente.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 aprile 2024	[IAM.20] Evita l'uso dell'utente root	Security Hub ha ritirato questo controllo e lo ha rimosso da tutti gli standard. Lo scopo di questo controllo è coperto da un altro controllo, [CloudWatch.1] Dovrebbero esistere un filtro logmetrico e un allarme per l'utilizzo da parte dell'utente «root» .
10 aprile 2024	[SNS.2] La registrazione dello stato di consegna deve essere abilitata per i messaggi di notifica inviati a un argomento	Security Hub ha ritirato questo controllo e lo ha rimosso da tutti gli standard. La registrazione dello stato di consegna per gli argomenti SNS non è più una best practice di sicurezza. Sebbene la registrazione dello stato di consegna per importanti argomenti SNS possa essere utile, non è necessaria per tutti gli argomenti.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 aprile 2024	[S3.10] I bucket generici S3 con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita	<p>Security Hub ha rimosso questo controllo da AWS Foundational Security Best Practices e Service-Managed Standard:. AWS Control Tower Lo scopo di questo controllo è coperto da altri due controlli : e. [S3.13] I bucket generici S3 devono avere configurazioni del ciclo di vita [S3.14] I bucket generici S3 devono avere il controllo delle versioni abilitato Questo controllo fa ancora parte del NIST SP 800-53 Rev. 5.</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 aprile 2024	[S3.11] I bucket generici S3 devono avere le notifiche degli eventi abilitate	Security Hub ha rimosso questo controllo da AWS Foundational Security Best Practices e Service-Managed Standard:. AWS Control Tower Sebbene ci siano alcuni casi in cui le notifiche di eventi per i bucket S3 sono utili, questa non è una best practice di sicurezza universale. Questo controllo fa ancora parte del NIST SP 800-53 Rev. 5.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 aprile 2024	[SNS.1] Gli argomenti SNS devono essere crittografati quando sono inattivi utilizzando AWS KMS	Security Hub ha rimosso questo controllo da AWS Foundational Security Best Practices e Service-Managed Standard:. AWS Control Tower Poiché SNS crittografa già gli argomenti per impostazione predefinita, l'utilizzo o AWS KMS per crittografare gli argomenti non è più consigliato come best practice di sicurezza . Questo controllo fa ancora parte di NIST SP 800-53 Rev. 5.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
8 aprile 2024	[ELB.6] Application, Gateway e Network Load Balancer devono avere la protezione da eliminazione abilitata	<p>Il titolo di controllo modificato dalla protezione da eliminazione di Application Load Balancer deve essere abilitato a Application, Gateway e Network Load Balancer dovrebbe avere la protezione da eliminazione abilitata. Questo controllo attualmente valuta Application, Gateway e Network Load Balancer. Il titolo e la descrizione sono stati modificati per riflettere accuratamente il comportamento attuale.</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
22 marzo 2024	[Opensearch.8] Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS	<p>Il titolo di controllo modificato da Connessioni ai OpenSearch domini deve essere crittografato utilizzando TLS 1.2 a Le connessioni ai OpenSearch domini devono essere crittografate utilizzando la più recente politica di sicurezza TLS. In precedenza, il controllo controllava solo se le connessioni ai OpenSearch domini utilizzavano TLS 1.2. Il controllo ora consente di determinare se i OpenSearch domini sono crittografati utilizzando la più recente politica di sicurezza TLS.</p> <p>PASSED Il titolo e la descrizione del controllo sono stati aggiornati per riflettere il comportamento corrente.</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
22 marzo 2024	[ES.8] Le connessioni ai domini Elasticsearch devono essere crittografate utilizzando la più recente politica di sicurezza TLS	<p>Il titolo di controllo modificato da Connessioni ai domini Elasticsearch deve essere crittografato utilizzando TLS 1.2 a Connessioni ai domini Elasticsearch deve essere crittografato utilizzando la politica di sicurezza TLS più recente. In precedenza, il controllo controllava solo se le connessioni ai domini Elasticsearch utilizzavano TLS 1.2. Il controllo ora determina se i domini Elasticsearch sono crittografati utilizzando la più recente politica di sicurezza TLS. PASSED Il titolo e la descrizione del controllo sono stati aggiornati per riflettere il comportamento corrente.</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.1] I bucket generici S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate	Il titolo modificato dall'impostazione S3 Block Public Access deve essere abilitato ai bucket generici S3 devono avere le impostazioni di accesso pubblico a blocchi abilitate . Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.2] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in lettura	La modifica del titolo dei bucket S3 dovrebbe vietare l'accesso pubblico in lettura ai bucket S3 generici e dovrebbe bloccare l'accesso pubblico in lettura. Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.3] I bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico in scrittura	La modifica del titolo dei bucket S3 dovrebbe vietare l'accesso pubblico in scrittura ai bucket S3 generici e dovrebbe bloccare l'accesso pubblico in scrittura . Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.5] I bucket S3 per uso generico devono richiedere l'utilizzo di SSL	Il titolo modificato dai bucket S3 dovrebbe richiedere richieste di utilizzo di Secure Socket Layer, mentre i bucket S3 per uso generico dovrebbero o richiedere l'utilizzo di SSL. Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.6] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS	Il titolo modificato dalle autorizzazioni S3 concesse ad altre politiche Account AWS in bucket dovrebbe essere limitato alle policy dei bucket per uso generico di S3 dovrebbero limitare l'accesso ad altri. Account AWS Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni	Il titolo modificato dai bucket S3 dovrebbe avere la replica tra regioni abilitata, mentre i bucket S3 per uso generico dovrebbero utilizzare la replica tra regioni. Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni	Il titolo modificato dai bucket S3 dovrebbe avere la replica tra regioni abilitata, mentre i bucket S3 per uso generico dovrebbero utilizzare la replica tra regioni. Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.8] I bucket generici S3 dovrebbero bloccare l'accesso pubblico	Il titolo modificato dall'impostazione S3 Block Public Access deve essere abilitato a livello di bucket, mentre i bucket S3 per uso generico dovrebbero bloccare l'accesso pubblico. Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.9] I bucket generici S3 devono avere la registrazione degli accessi al server abilitata	Il titolo modificato da S3 bucket La registrazione degli accessi al server deve essere abilitata a La registrazione degli accessi al server deve essere abilitata per i bucket S3 per uso generico. Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.10] I bucket generici S3 con il controllo delle versioni abilitato devono avere configurazioni del ciclo di vita	Il titolo modificato dai bucket S3 con il controllo delle versioni abilitato dovrebbe avere politiche del ciclo di vita configurate in base ai bucket S3 per uso generico con il controllo delle versioni abilitato dovrebbero avere configurazioni del ciclo di vita. Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.11] I bucket generici S3 devono avere le notifiche degli eventi abilitate	Il titolo modificato dai bucket S3 dovrebbe avere le notifiche degli eventi abilitate , mentre i bucket S3 per uso generico dovrebbero avere le notifiche degli eventi abilitate. Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.12] Gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3	Il titolo modificato o dagli elenchi di controllo degli accessi (ACL) di S3 non deve essere utilizzato per gestire l'accesso degli utenti ai bucket, mentre gli ACL non devono essere utilizzati per gestire l'accesso degli utenti ai bucket generici S3. Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.13] I bucket generici S3 devono avere configurazioni del ciclo di vita	Il titolo modificato dai bucket S3 dovrebbe avere politiche del ciclo di vita configurate in base ai bucket S3 per uso generico e i bucket S3 dovrebbero avere configurazioni del ciclo di vita. Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.14] I bucket generici S3 devono avere il controllo delle versioni abilitato	Il titolo modificato dai bucket S3 dovrebbe utilizzare il controllo delle versioni, mentre i bucket S3 per uso generico dovrebbero avere il controllo delle versioni abilitato. Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
12 marzo 2024	[S3.15] I bucket generici S3 devono avere Object Lock abilitato	Il titolo modificato dai bucket S3 deve essere configurato per utilizzare Object Lock, mentre i bucket per uso generico S3 devono avere Object Lock abilitato . Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.
12 marzo 2024	[S3.17] I bucket generici S3 devono essere crittografati quando sono inattivi con AWS KMS keys	Il titolo modificato dai bucket S3 deve essere crittografato con i bucket AWS KMS keys inattivi con i bucket S3 per uso generico. AWS KMS keys Security Hub ha cambiato il titolo per tenere conto di un nuovo tipo di bucket S3.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
7 marzo 2024	[Lambda.2] Le funzioni Lambda devono utilizzare runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub ora supporta <code>nodejs20.x</code> e <code>ruby3.3</code> come parametro.
22 febbraio 2024	[Lambda.2] Le funzioni Lambda devono utilizzare runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub ora supporta <code>dotnet8</code> come parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
5 febbraio 2024	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Security Hub ha aggiornato la versione più vecchia supportata di Kubernetes su cui può essere eseguito il cluster Amazon EKS per produrre un risultato superato. La versione più vecchia attualmente supportata è Kubernetes. 1.25

Data di modifica	ID e titolo del controllo	Descrizione della modifica
10 gennaio 2024	[CodeBuild.1] Gli URL del repository di origine di CodeBuild Bitbucket non devono contenere credenziali sensibili	<p>Il titolo modificato CodeBuild GitHub o gli URL del repository di origine Bitbucket devono utilizzare OAuth, mentre gli URL del repository di origine CodeBuild Bitbucket non devono contenere credenziali riservate. Security Hub ha rimosso la menzione di OAuth perché anche altri metodi di connessione possono essere sicuri. Security Hub ha rimosso la menzione GitHub perché non è più possibile avere un token di accesso personale o un nome utente e una password negli URL del repository di GitHub origine.</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
8 gennaio 2024	[Lambda.2] Le funzioni Lambda devono utilizzare runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub non supporta più <code>go1.x</code> e <code>java8</code> come parametri perché si tratta di runtime ritirati.
29 dicembre 2023	[RDS.8] Le istanze DB RDS devono avere la protezione da eliminazione abilitata	RDS.8 verifica se un'istanza Amazon RDS DB che utilizza uno dei motori di database supportati ha la protezione e da eliminazione abilitata. Security Hub ora supporta <code>custom-oracle-ee</code> e <code>oracle-se2-cdb</code> come motori di database. <code>oracle-ee-cdb</code>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
22 dicembre 2023	[Lambda.2] Le funzioni Lambda devono utilizzare runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub ora supporta java21 e python3.12 come parametri. Security Hub non supporta più ruby2.7 come parametro.
15 dicembre 2023	[CloudFront.1] CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato	CloudFront.1 verifica se una CloudFront distribuzione Amazon ha un oggetto root predefinito configurato. Security Hub ha ridotto la severità di questo controllo da CRITICAL a HIGH perché l'aggiunta dell'oggetto root predefinito è una raccomandazione che dipende dall'applicazione dell'utente e dai requisiti specifici.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
5 dicembre 2023	[EC2.13] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22	Il titolo di controllo modificato dai gruppi di sicurezza non dovrebbe consentire l'ingresso da 0.0.0.0/0 alla porta 22 ai gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 22.
5 dicembre 2023	[EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389	Titolo di controllo modificato da Assicura che i gruppi di sicurezza non consentano l'ingresso o dalla porta 0.0.0.0/0 alla porta 3389 a I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o: :/0 alla porta 3389.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
5 dicembre 2023	[RDS.9] Le istanze DB RDS devono pubblicare i log nei registri CloudWatch	<p>Il titolo di controllo modificato dalla registrazione del database deve essere abilitato alle istanze DB RDS. Le istanze DB devono pubblicare i registri nei registri. CloudWatch Security Hub ha rilevato che questo controllo verifica solo se i log sono pubblicati su Amazon CloudWatch Logs e non verifica se i log RDS sono abilitati. Il controllo rileva se le istanze DB RDS sono configurate per pubblicare log su Logs. PASSED CloudWatch Il titolo del controllo è stato aggiornato per riflettere il comportamento corrente.</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
17 novembre 2023	[EC2.19] I gruppi di sicurezza non devono consentire l'accesso illimitato alle porte ad alto rischio	EC2.19 verifica se il traffico in entrata senza restrizioni per un gruppo di sicurezza è accessibile alle porte specificate considerate ad alto rischio. Security Hub ha aggiornato questo controllo per tenere conto degli elenchi di prefissi gestiti quando vengono forniti come origine per una regola del gruppo di sicurezza. Il controllo rileva se gli elenchi di prefissi contengono le stringhe '0.0.0.0/0' o ': :/0'. FAILED
16 novembre 2023	[CloudWatch.15] gli CloudWatch allarmi devono avere azioni specificate configurate	Il titolo di controllo modificato dagli CloudWatch allarmi dovrebbe avere un'azione configurata per lo stato ALARM, mentre gli allarmi dovrebbero avere delle azioni specificate configurate. CloudWatch

Data di modifica	ID e titolo del controllo	Descrizione della modifica
16 novembre 2023	[CloudWatch.16] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato	Il titolo di controllo modificato dei gruppi di CloudWatch log deve essere conservato per almeno 1 anno, mentre i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato.
16 novembre 2023	[Lambda.5] Le funzioni VPC Lambda devono funzionare in più zone di disponibilità	Il titolo di controllo modificato dalle funzioni VPC Lambda deve funzionare in più di una zona di disponibilità, mentre le funzioni VPC Lambda devono funzionare in più zone di disponibilità.
16 novembre 2023	[AppSync.2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata	La modifica del titolo di controllo da AWS AppSync dovrebbe avere la registrazione a livello di richiesta e di campo attivata a dovrebbe avere la registrazione a livello di campo abilitata .AWS AppSync

Data di modifica	ID e titolo del controllo	Descrizione della modifica
16 novembre 2023	[EMR.1] I nodi primari del cluster Amazon EMR non devono avere indirizzi IP pubblici	Il titolo di controllo modificato dai nodi master MapReduce del cluster Amazon Elastic non dovrebbe avere indirizzi IP pubblici, mentre i nodi primari del cluster Amazon EMR non dovrebbero avere indirizzi IP pubblici.
16 novembre 2023	I OpenSearch domini [Opensearch.2] non devono essere accessibili al pubblico	Il titolo di controllo modificato dai OpenSearch domini dovrebbe essere in un VPC, in quanto i domini non dovrebbero essere accessibili OpenSearch al pubblico.
16 novembre 2023	[ES.2] I domini Elasticsearch non devono essere accessibili al pubblico	Il titolo di controllo modificato dai domini Elasticsearch dovrebbe essere in un VPC, mentre i domini Elasticsearch non dovrebbero essere accessibili al pubblico.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
31 ottobre 2023	[ES.4] La registrazione degli errori del dominio Elasticsearch nei log deve essere abilitata CloudWatch	ES.4 verifica se i domini Elasticsearch sono configurati per inviare log di errore ad Amazon Logs. CloudWatch Il controllo in precedenza produceva una PASSED ricerca per un dominio Elasticsearch con tutti i log configurati per l'invio a Logs. CloudWatch Security Hub ha aggiornato il controllo per produrre un PASSED risultato solo per un dominio Elasticsearch configurato per inviare i log degli errori ai registri. CloudWatch Il controllo è stato inoltre aggiornato per escludere dalla valutazione le versioni di Elasticsearch che non supportano i log degli errori.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
16 ottobre 2023	[EC2.13] I gruppi di sicurezza non devono consentire l'ingresso da 0.0.0.0/0 o :/0 alla porta 22	EC2.13 verifica se i gruppi di sicurezza consentono l'accesso illimitato in ingresso alla porta 22. Security Hub ha aggiornato questo controllo per tenere conto degli elenchi di prefissi gestiti quando vengono forniti come origine per una regola del gruppo di sicurezza. Il controllo rileva se gli elenchi di prefissi contengono le stringhe '0.0.0.0/0' o ':/0'. FAILED

Data di modifica	ID e titolo del controllo	Descrizione della modifica
16 ottobre 2023	[EC2.14] I gruppi di sicurezza non dovrebbero consentire l'ingresso da 0.0.0.0/0 o :/0 alla porta 3389	EC2.14 verifica se i gruppi di sicurezza consentono l'accesso illimitato in ingresso alla porta 3389. Security Hub ha aggiornato questo controllo per tenere conto degli elenchi di prefissi gestiti quando vengono forniti come origine per una regola del gruppo di sicurezza. Il controllo rileva se gli elenchi di prefissi contengono le stringhe '0.0.0.0/0' o ':/0'. FAILED

Data di modifica	ID e titolo del controllo	Descrizione della modifica
16 ottobre 2023	[EC2.18] I gruppi di sicurezza devono consentire e il traffico in entrata senza restrizioni solo per le porte autorizzate	EC2.18 verifica se i gruppi di sicurezza in uso consentono il traffico in entrata senza restrizioni. Security Hub ha aggiornato questo controllo per tenere conto degli elenchi di prefissi gestiti quando vengono forniti come origine per una regola del gruppo di sicurezza. Il controllo rileva se gli elenchi di prefissi contengono le stringhe '0.0.0.0/0' o ': :/0'. FAILED
16 ottobre 2023	[Lambda.2] Le funzioni Lambda devono utilizzare runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub ora supporta python3.11 come parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
4 ottobre 2023	[S3.7] I bucket S3 per uso generico devono utilizzare la replica tra regioni	Security Hub ha aggiunto il parametro <code>ReplicationType</code> con un valore pari <code>CROSS-REGION</code> a per garantire che nei bucket S3 sia abilitata la replica tra regioni anziché la replica nella stessa regione.
27 settembre 2023	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	Security Hub ha aggiornato la versione più vecchia supportata di Kubernetes su cui può essere eseguito il cluster Amazon EKS per produrre un risultato superato. La versione più vecchia attualmente supportata è Kubernetes. 1.24

Data di modifica	ID e titolo del controllo	Descrizione della modifica
20 settembre 2023	CloudFront.2 — le CloudFront distribuzioni devono avere l'identità di accesso all'origine abilitata	<p>Security Hub ha ritirato questo controllo e lo ha rimosso da tutti gli standard. Altrimenti, consulta [CloudFront.13] CloudFront le distribuzioni devono utilizzare il controllo dell'accesso all'origine. Il controllo degli accessi Origin è l'attuale best practice di sicurezza. Questo controllo verrà rimosso dalla documentazione entro 90 giorni.</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
20 settembre 2023	[EC2.22] I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi	<p>Security Hub ha rimosso questo controllo da AWS Foundational Security Best Practices (FSBP) e National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5. Fa ancora parte di Service-Managed Standard: AWS Control Tower. Questo controllo produce un risultato positivo se i gruppi di sicurezza sono collegati a istanze EC2 o a un'interfaccia di rete elastica. Tuttavia, in alcuni casi d'uso, i gruppi di sicurezza non collegati non rappresentano un rischio per la sicurezza. Puoi utilizzare altri controlli EC2, come EC2.2, EC2.13, EC2.14, EC2.18 ed EC2.19, per monitorare i tuoi gruppi di sicurezza.</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
20 settembre 2023	EC2.29 — Le istanze EC2 devono essere avviate in un VPC	Security Hub ha ritirato questo controllo e lo ha rimosso da tutti gli standard. Amazon EC2 ha migrato le istanze EC2 Classic su un VPC. Questo controllo verrà rimosso dalla documentazione entro 90 giorni.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
20 settembre 2023	S3.4 — I bucket S3 devono avere la crittografia lato server abilitata	Security Hub ha ritirato questo controllo e lo ha rimosso da tutti gli standard. Amazon S3 ora fornisce la crittografia predefinita con chiavi gestite S3 (SS3-S3) su bucket S3 nuovi ed esistenti . Le impostazioni di crittografia sono invariate per i bucket esistenti crittografati con la crittografia lato server SS3-S3 o SS3-KMS. Questo controllo verrà rimosso dalla documentazione tra 90 giorni.
14 settembre 2023	[EC2.2] I gruppi di sicurezza VPC predefiniti non dovrebbero consentire il traffico in entrata o in uscita	Titolo di controllo modificato da Il gruppo di sicurezza predefinito VPC non dovrebbe consentire e il traffico in entrata e in uscita ai gruppi di sicurezza predefiniti VPC non dovrebbe consentire il traffico in entrata o in uscita.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 settembre 2023	[IAM.9] L'MFA deve essere abilitata per l'utente root	Il titolo di controllo modificato da Virtual MFA deve essere abilitato per l'utente root a MFA deve essere abilitato per l'utente root.
14 settembre 2023	[RDS.19] Le sottoscrizioni esistenti per le notifiche di eventi RDS devono essere configurate per gli eventi critici del cluster	Titolo di controllo modificato da Un abbonamento per le notifiche di eventi RDS deve essere configurato per gli eventi critici del cluster a Gli abbonamenti di notifica degli eventi RDS esistenti devono essere configurati per gli eventi critici del cluster.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 settembre 2023	[RDS.20] Le sottoscrizioni di notifica degli eventi RDS esistenti devono essere configurate per gli eventi critici delle istanze di database	Titolo di controllo modificato da Un abbonamento alle notifiche di eventi RDS deve essere configurato per gli eventi critici delle istanze di database Gli abbonamenti di notifica degli eventi RDS esistenti devono essere configurati per gli eventi critici delle istanze di database.
14 settembre 2023	[WAF.2] Le regole regionali AWS WAF classiche devono avere almeno una condizione	Il titolo di controllo modificato da una regola regionale WAF dovrebbe avere almeno una condizione e, mentre le regole regionali AWS WAF classiche dovrebbero avere almeno una condizione.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 settembre 2023	[WAF.3] I gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola	Il titolo di controllo modificato da Un gruppo di regole regionali WAF dovrebbe avere almeno una regola, mentre i gruppi di regole regionali AWS WAF classici dovrebbero avere almeno una regola.
14 settembre 2023	[WAF.4] Gli ACL web regionali AWS WAF classici devono avere almeno una regola o un gruppo di regole	Titolo di controllo modificato da Un ACL web regionale WAF dovrebbe avere almeno una regola o un gruppo di regole a un ACL web regionale AWS WAF classico gli ACL web regionali classici dovrebbero avere almeno una regola o un gruppo di regole.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 settembre 2023	[WAF.6] Le regole globali AWS WAF classiche devono avere almeno una condizione	Il titolo di controllo modificato da Una regola globale WAF dovrebbe avere almeno una condizione e a Le regole globali AWS WAF Classic dovrebbero avere almeno una condizione e.
14 settembre 2023	[WAF.7] I gruppi di regole globali AWS WAF classici dovrebbero avere almeno una regola	Il titolo di controllo modificato da Un gruppo di regole globale WAF dovrebbe avere almeno una regola, mentre i gruppi di regole globali AWS WAF Classic dovrebbero avere almeno una regola.
14 settembre 2023	[WAF.8] Gli ACL web globali AWS WAF classici devono avere almeno una regola o un gruppo di regole	Titolo di controllo modificato da Un ACL web globale WAF dovrebbe avere almeno una regola o un gruppo di regole a Gli ACL web globali AWS WAF classici dovrebbero avere almeno una regola o un gruppo di regole.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
14 settembre 2023	[WAF.10] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole	Il titolo di controllo modificato da Un ACL Web WAFv2 deve avere almeno una regola o un gruppo di regole, mentre gli ACL AWS WAF Web devono avere almeno una regola o un gruppo di regole.
14 settembre 2023	[WAF.11] la registrazione ACL web deve essere abilitata AWS WAF	Il titolo di controllo modificato dalla registrazione ACL Web AWS WAF v2 deve essere attivato alla registrazione ACL Web deve essere abilitata.AWS WAF

Data di modifica	ID e titolo del controllo	Descrizione della modifica
20 luglio 2023	S3.4 — I bucket S3 devono avere la crittografia lato server abilitata	<p>S3.4 verifica se un bucket Amazon S3 ha la crittografia lato server abilitata o se la policy del bucket S3 nega esplicitamente le richieste senza crittografia lato server. PutObject</p> <p>Security Hub ha aggiornato questo controllo per includere la crittografia lato server a doppio livello con chiavi KMS (DSSE-KMS). Il controllo produce un risultato superato quando un bucket S3 viene crittografato con SSE-S3, SSE-KMS o DSSE-KMS.</p>

Data di modifica	ID e titolo del controllo	Descrizione della modifica
17 luglio 2023	[S3.17] I bucket generici S3 devono essere crittografati quando sono inattivi con AWS KMS keys	S3.17 verifica se un bucket Amazon S3 è crittografato con un. AWS KMS key Security Hub ha aggiornato questo controllo per includere la crittografia lato server a doppio livello con chiavi KMS (DSSE-KMS). Il controllo produce un risultato superato quando un bucket S3 viene crittografato con SSE-KMS o DSSE-KMS.
9 giugno 2023	[EKS.2] I cluster EKS devono essere eseguiti su una versione Kubernetes supportata	EKS.2 verifica se un cluster Amazon EKS è in esecuzione e su una versione di Kubernetes supportata. La versione più vecchia supportata è ora. 1.23

Data di modifica	ID e titolo del controllo	Descrizione della modifica
9 giugno 2023	[Lambda.2] Le funzioni Lambda devono utilizzare runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub ora supporta ruby3.2 come parametro.
5 giugno 2023	[ApiGateway.5] I dati della cache dell'API REST API Gateway devono essere crittografati quando sono inattivi	apigateway.5. Verifica se tutti i metodi nelle fasi dell'API REST di Amazon API Gateway sono crittografati a riposo. Security Hub ha aggiornato il controllo per valutare la crittografia di un particolare metodo solo quando la memorizzazione nella cache è abilitata per quel metodo.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
18 maggio 2023	[Lambda.2] Le funzioni Lambda devono utilizzare runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub ora supporta <code>java17</code> come parametro.
18 maggio 2023	[Lambda.2] Le funzioni Lambda devono utilizzare runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub non supporta più <code>nodejs12.x</code> come parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
23 aprile 2023	[ECS.10] I servizi ECS Fargate devono essere eseguiti sulla versione più recente della piattaforma Fargate	ECS.10 verifica se i servizi Amazon ECS Fargate eseguono l'ultima versione della piattaforma Fargate. I clienti possono implementare Amazon ECS tramite ECS direttamente o utilizzando CodeDeploy Security Hub ha aggiornato questo controllo per produrre risultati Passed CodeDeploy da utilizzare per distribuire i servizi ECS Fargate.
20 aprile 2023	[S3.6] Le policy generiche relative ai bucket di S3 dovrebbero limitare l'accesso ad altri Account AWS	S3.6 verifica se una policy sui bucket di Amazon Simple Storage Service (Amazon S3) impedisce ai principali di eseguire azioni Account AWS negate sulle risorse nel bucket S3. Security Hub ha aggiornato il controllo per tenere conto dei condizionali in una policy bucket.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
18 aprile 2023	[Lambda.2] Le funzioni Lambda devono utilizzare runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub ora supporta python3.10 come parametro.
18 aprile 2023	[Lambda.2] Le funzioni Lambda devono utilizzare runtime supportati	Lambda.2 verifica se le impostazioni delle AWS Lambda funzioni per i runtime corrispondono ai valori previsti impostati per i runtime supportati in ogni lingua. Security Hub non supporta più dotnetcore3.1 come parametro.

Data di modifica	ID e titolo del controllo	Descrizione della modifica
17 aprile 2023	[RDS.11] Le istanze RDS devono avere i backup automatici abilitati	<p>RDS.11 verifica se nelle istanze Amazon RDS sono abilitati i backup automatici, con un periodo di conservazione dei backup maggiore o uguale a sette giorni. Security Hub ha aggiornato questo controllo per escludere le repliche di lettura dalla valutazione, poiché non tutti i motori supportano backup automatici sulle repliche di lettura. Inoltre, RDS non offre la possibilità di specificare un periodo di conservazione dei backup durante la creazione di repliche di lettura. Le repliche di lettura vengono create con un periodo di conservazione dei backup di 0 default.</p>

Cronologia dei documenti per la Guida per l'utente AWS di Security Hub

La tabella seguente descrive gli aggiornamenti alla documentazione per AWS Security Hub.

Note

Per le versioni dei controlli di sicurezza, la data specificata è la data in cui i controlli sono disponibili in tutti gli account e le regioni. Possono essere necessarie 1-2 settimane prima che i controlli raggiungano tutti gli account e le regioni.

Modifica	Descrizione	Data
Rilascio di CIS AWS Foundations Benchmark v3.0.0	<p>Security Hub ha rilasciato Center for Internet Security (CIS) AWS Foundations Benchmark v3.0.0. La versione include i seguenti nuovi controlli, oltre alla mappatura di diversi controlli esistenti.</p> <ul style="list-style-type: none">• the section called “[EC2.53] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da 0.0.0.0/0 alle porte di amministrazione remota del server”• the section called “[EC2.54] I gruppi di sicurezza EC2 non dovrebbero consentire l'accesso da: :/0 alle porte di amministrazione remota del server”	13 maggio 2024

- [the section called “\[IAM.26\] I certificati SSL/TLS scaduti gestiti in IAM devono essere rimossi”](#)
- [the section called “\[IAM.27\] Le identità IAM non devono avere la policy allegata AWSCloudShellFullAccess ”](#)
- [the section called “\[IAM.28\] L'analizzatore di accesso esterno IAM Access Analyzer deve essere abilitato”](#)
- [the section called “\[S3.22\] I bucket S3 per uso generico devono registrare gli eventi di scrittura a livello di oggetto”](#)
- [the section called “\[S3.23\] I bucket S3 per uso generico devono registrare gli eventi di lettura a livello di oggetto”](#)

Nuovi controlli di sicurezza

Sono disponibili i seguenti nuovi controlli del Security Hub:

3 maggio 2024

- the section called “[DataFirehose.1] I flussi di distribuzione di Firehose devono essere crittografati quando sono inattivi”
- the section called “[DMS.10] Gli endpoint DMS per i database Neptune devono avere l'autorizzazione IAM abilitata”
- the section called “[DMS.11] Gli endpoint DMS per MongoDB devono avere un meccanismo di autenticazione abilitato”
- the section called “[DMS.12] Gli endpoint DMS per Redis devono avere TLS abilitato”
- the section called “[DynamoDB.7] I cluster DynamoDB Accelerator devono essere crittografati in transito”
- the section called “[EFS.6] I target di montaggio EFS non devono essere associati a una sottorete pubblica”
- the section called “[EKS.3] I cluster EKS devono utilizzare segreti Kubernetes crittografati”

- the section called “[FSX.2] I file system FSx for Lustre devono essere configurati per copiare i tag nei backup”
- the section called “[MQ.2] I broker ActiveMQ devono trasmettere i log di controllo a CloudWatch”
- the section called “[MQ.3] I broker Amazon MQ dovrebbero avere abilitato l'aggiornamento automatico delle versioni secondarie”
- the section called “I OpenSearch domini [Opensearch.11] devono avere almeno tre nodi primari dedicati”
- the section called “[Redshift.15] I gruppi di sicurezza Redshift dovrebbero consentire l'ingresso sulla porta del cluster solo da origini limitate”
- the section called “[SageMaker.4] Le varianti di produzione di SageMaker endpoint devono avere un numero iniziale di istanze superiore a 1”
- the section called “[Service Catalog.1] I portafogli Service Catalog devono essere condivisi solo all'inter

	<p>no di un'organizzazione AWS”</p> <ul style="list-style-type: none"> • the section called “[Transfer.2] I server Transfer Family non devono utilizzare il protocollo FTP per la connessione agli endpoint” 	
AWS Standard di etichettatura delle risorse	Il AWS Resource Tagging Standard di Security Hub è ora disponibile a tutti, insieme ai nuovi controlli che si applicano allo standard.	30 aprile 2024
Aggiornamento alla politica gestita esistente	Security Hub ha aggiornato la politica AWS gestita denominata AmazonSecurityHubFullAccess per ottenere dettagli sui prezzi dei prodotti Servizi AWS e dei prodotti.	24 aprile 2024
Configurazione contestuale dei parametri di controllo	Se utilizzi la configurazione centrale, ora puoi configurare i parametri di controllo nel contesto , dalla pagina dei dettagli di un controllo sulla console Security Hub.	29 marzo 2024
Aggiornamento alla politica gestita esistente	Security Hub ha aggiornato la policy AWS gestita denominata AWSSecurityHubReadOnlyAccess aggiungendo un Sid campo.	22 febbraio 2024

[Nuovo controllo di sicurezza](#)

Il controllo [\[Macie.2\] Il rilevamento automatico dei dati sensibili di Macie dovrebbe essere abilitato](#) è ora disponibile. Per i limiti regionali relativi a questo controllo, vedi [Disponibilità dei controlli per regione](#).

19 febbraio 2024

[Security Hub disponibile in Canada occidentale \(Calgary\)](#)

Security Hub è ora disponibile in Canada occidentale (Calgary). Tutte le funzionalità del Security Hub sono ora disponibili in questa regione, ad eccezione di alcuni controlli di sicurezza. Per ulteriori informazioni, vedere [Disponibilità dei controlli per regione](#).

20 dicembre 2023

Nuovi controlli di sicurezza

Sono disponibili i seguenti nuovi controlli del Security Hub:

14 dicembre 2023

- the section called “[Backup.1] i punti di AWS Backup ripristino devono essere crittografati a riposo”
- the section called “[DynamoDB.6] Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata”
- the section called “[EC2.51] Gli endpoint EC2 Client VPN devono avere la registrazione delle connessioni client abilitata”
- the section called “[EKS.8] I cluster EKS devono avere la registrazione di controllo abilitata”
- the section called “[EMR.2] L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata”
- the section called “[FSx.1] I file system FSx per OpenZFS devono essere configurati per copiare i tag su backup e volumi”
- the section called “[Macie.1] Amazon Macie dovrebbe essere abilitato”

- [the section called “\[MSK.2\] Per i cluster MSK dovrebbe essere configurato un monitoraggio avanzato”](#)
- [the section called “\[Neptune .9\] I cluster Neptune DB devono essere distribuiti su più zone di disponibilità”](#)
- [the section called “\[Network Firewall.1\] I firewall Network Firewall devono essere distribuiti su più zone di disponibilità”](#)
- [the section called “\[Network Firewall.2\] La registrazione del Network Firewall deve essere abilitata”](#)
- [the section called “Nei OpenSearch domini \[Opensearch.10\] deve essere installato l'ultimo aggiornamento software”](#)
- [the section called “L'autorità di certificazione AWS Private CA principale \[PCA.1\] deve essere disabilitata”](#)
- [the section called “\[S3.19\] I punti di accesso S3 devono avere le impostazioni di blocco dell'accesso pubblico abilitate”](#)
- [the section called “\[S3.20\] I bucket S3 per uso generico](#)

[devono avere l'eliminazione
MFA abilitata”](#)

[Alla ricerca di un arricchimento](#)

Security Hub ha aggiunto i nuovi campi `AwsAccountName` di ricerca e `ApplicationName` al `AWS Security Finding Format (ASFF)`. `ApplicationArn`

27 novembre 2023

[Miglioramenti alla dashboard di riepilogo](#)

Ora puoi accedere a più widget della dashboard nella pagina di riepilogo della console Security Hub, salvare i set di filtri del dashboard per concentrarti rapidamente su problemi di sicurezza specifici e personalizzare il layout della dashboard.

27 novembre 2023

[Configurazione centrale](#)

La configurazione centrale è ora disponibile. Con la configurazione centrale, l'amministratore delegato di Security Hub può configurare Security Hub, standard e controlli su più account dell'organizzazione, unità organizzative (OU) e regioni.

27 novembre 2023

[Aggiornamenti alla politica gestita](#)

Security Hub ha aggiunto nuove autorizzazioni alla policy `AWSSecurityHubServiceRolePolicy` gestita che consentono a Security Hub di leggere e aggiornare le proprietà di controllo di sicurezza personalizzabili.

26 novembre 2023

[Parametri di controllo personalizzati](#)

È ora possibile personalizzare i valori dei parametri per determinati controlli del Security Hub. Ciò può rendere i risultati relativi a un controllo specifico più pertinenti ai requisiti aziendali e alle aspettative di sicurezza.

26 novembre 2023

[Aggiornamenti alle politiche gestite](#)

Security Hub ha aggiornato `AWSSecurityHubFullAccess` e `AWSSecurityHubOrganizationsAccess` gestito le politiche che consentono di utilizzare, rispettivamente, le funzionalità di Security Hub e l'integrazione con AWS Organizations.

16 novembre 2023

[Controlli di sicurezza esistenti aggiunti a Service-Managed Standard: AWS Control Tower](#)

I seguenti controlli Security Hub esistenti sono stati aggiunti a Service-Managed Standard: AWS Control Tower

14 novembre 2023

- ACM.2
- AppSync5.
- CloudTrail6.
- D.M. 9
- Documento DB.3
- DynamoDB.3
- EC2.23
- EKS.1
- ElastiCache3.
- ElastiCache4.
- ElastiCache5.
- ElastiCache6.
- EventBridge3.
- KMS.4
- Lambda.3
- MQ.5
- MQ.6
- MSK.1
- RDS.12
- RDS.15
- S3.17

[Aggiornamenti alla politica gestita](#)

Security Hub ha aggiunto una nuova autorizzazione di etichettatura alla politica `AWSecurityHubServiceRolePolicy` gestita che consente a Security Hub di leggere i tag delle risorse relativi ai risultati.

7 novembre 2023

Nuovi controlli di sicurezza

Sono disponibili i seguenti nuovi controlli del Security Hub:

10 ottobre 2023

- the section called “[AppSync .5] Le API AWS AppSync GraphQL non devono essere autenticate con chiavi API”
- the section called “[DMS.6] Le istanze di replica DMS devono avere l'aggiornamento automatico delle versioni secondarie abilitato”
- the section called “[DMS.7] Le attività di replica DMS per il database di destinazione devono avere la registrazione abilitata”
- the section called “[DMS.8] Le attività di replica DMS per il database di origine devono avere la registrazione abilitata”
- the section called “[DMS.9] Gli endpoint DMS devono utilizzare SSL”
- the section called “[DocumentDB.3] Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche”
- the section called “[DocumentDB.4] I cluster

Amazon DocumentDB
devono pubblicare i log di
controllo su Logs CloudWatc
h ”

- the section called
“[DocumentDB.5] I cluster
Amazon DocumentDB
devono avere la protezione
da eliminazione abilitata”
- the section called “[ECS.9]
Le definizioni delle attività
ECS devono avere una
configurazione di registraz
ione”
- the section called “[EventBr
idge.3] i bus di eventi
EventBridge personalizzati
devono avere una politica
basata sulle risorse allegata”
- the section called “[EventBr
idge.4] gli endpoint
EventBridge globali
dovrebbero avere la replica
degli eventi abilitata”
- the section called “[MSK.1]
I cluster MSK devono
essere crittografati durante il
transito tra i nodi del broker”
- the section called “[MQ.5]
I broker ActiveMQ devono
utilizzare la modalità di
distribuzione attiva/standby”
- the section called “[MQ.6] I
broker RabbitMQ dovrebber

- o utilizzare la modalità di distribuzione del cluster”
- the section called “[Network Firewall.9] I firewall Network Firewall devono avere la protezione da eliminazione abilitata”
 - the section called “[RDS.34] I cluster Aurora MySQL DB devono pubblicare i log di controllo nei registri CloudWatch ”
 - the section called “[RDS.35] Nei cluster RDS DB deve essere abilitato l'aggiornamento automatico delle versioni secondarie”
 - the section called “[Route53 .2] Le zone ospitate pubbliche di Route 53 devono registrare le query DNS”
 - the section called “Le regole [WAF.12] devono avere le metriche abilitate AWS WAF CloudWatch ”

[Aggiornamenti alla politica gestita](#)

Security Hub ha aggiunto nuove azioni Organizations alla policy `AWSecurityHubServiceRolePolicy` gestita che consentono a Security Hub di recuperare informazioni su account e unità organizzative (OU). Abbiamo anche aggiunto nuove azioni Security Hub che consentono a Security Hub di leggere e aggiornare le configurazioni dei servizi, inclusi standard e controlli.

27 settembre 2023

[Controlli di sicurezza esistenti aggiunti a Service-Managed Standard: AWS Control Tower](#)

I seguenti controlli Security Hub esistenti sono stati aggiunti a Service-Managed Standard: AWS Control Tower

26 settembre 2023

- [the section called “\[Athena.1\] I gruppi di lavoro Athena devono essere crittografati quando sono inattivi”](#)
- [the section called “\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi”](#)
- [the section called “\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato”](#)
- [the section called “\[Neptune .1\] I cluster Neptune DB devono essere crittografati a riposo”](#)
- [the section called “\[Neptune .2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch”](#)
- [the section called “\[Neptune .3\] Le istantanee del cluster Neptune DB non devono essere pubbliche”](#)
- [the section called “\[Neptune .4\] I cluster Neptune DB](#)

- devono avere la protezione da eliminazione abilitata”
- the section called “[Neptune .5] I cluster Neptune DB devono avere i backup automatici abilitati”
- the section called “[Neptune .6] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive”
- the section called “[Neptune .7] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata”
- the section called “[Neptune .8] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee”
- the section called “[RDS.27] I cluster RDS DB devono essere crittografati quando sono inattivi”

[Visualizzazione dei controlli consolidati e risultati del controllo consolidato disponibili in AWS GovCloud \(US\)](#)

La visualizzazione dei controlli consolidati e i risultati del controllo consolidato sono ora disponibili in. AWS GovCloud (US) Region La pagina Controlli della console Security Hub mostra tutti i controlli tra gli standard. Ogni controllo ha lo stesso ID di controllo per tutti gli standard. Quando attivi i risultati del controllo consolidato, ricevi un solo risultato per controllo di sicurezza anche quando un controllo si applica a più standard abilitati.

6 settembre 2023

[Visualizzazione dei controlli consolidati e risultati di controllo consolidati disponibili nelle regioni della Cina](#)

La visualizzazione dei controlli consolidati e i risultati del controllo consolidato sono ora disponibili nelle regioni cinesi. La pagina Controlli della console Security Hub mostra tutti i controlli tra gli standard. Ogni controllo ha lo stesso ID di controllo per tutti gli standard. Quando attivi i risultati del controllo consolidato, ricevi un solo risultato per controllo di sicurezza anche quando un controllo si applica a più standard abilitati.

28 agosto 2023

[Security Hub disponibile nella regione di Israele \(Tel Aviv\)](#)

Security Hub è ora disponibile in Israele (Tel Aviv). Tutte le funzionalità del Security Hub sono ora disponibili in questa regione, ad eccezione di alcuni controlli di sicurezza. Per ulteriori informazioni, vedere [Disponibilità dei controlli per regione](#).

8 agosto 2023

Nuovi controlli di sicurezza

Sono disponibili i seguenti nuovi controlli del Security Hub:

28 luglio 2023

- [the section called “\[Athena.1\] I gruppi di lavoro Athena devono essere crittografati quando sono inattivi”](#)
- [the section called “\[DocumentDB.1\] I cluster Amazon DocumentDB devono essere crittografati quando sono inattivi”](#)
- [the section called “\[DocumentDB.2\] I cluster Amazon DocumentDB devono avere un periodo di conservazione dei backup adeguato”](#)
- [the section called “\[Neptune.1\] I cluster Neptune DB devono essere crittografati a riposo”](#)
- [the section called “\[Neptune.2\] I cluster Neptune DB devono pubblicare i log di controllo su Logs CloudWatch”](#)
- [the section called “\[Neptune.3\] Le istantanee del cluster Neptune DB non devono essere pubbliche”](#)
- [the section called “\[Neptune.4\] I cluster Neptune DB](#)

- [devono avere la protezione da eliminazione abilitata”](#)
- [the section called “\[Neptune .5\] I cluster Neptune DB devono avere i backup automatici abilitati”](#)
- [the section called “\[Neptune .6\] Le istantanee del cluster Neptune DB devono essere crittografate quando sono inattive”](#)
- [the section called “\[Neptune .7\] I cluster Neptune DB devono avere l'autenticazione del database IAM abilitata”](#)
- [the section called “\[Neptune .8\] I cluster Neptune DB devono essere configurati per copiare i tag nelle istantanee”](#)
- [the section called “\[RDS.27\] I cluster RDS DB devono essere crittografati quando sono inattivi”](#)

[Nuovi operatori per i criteri delle regole di automazione](#)

Ora puoi utilizzare gli operatori di confronto CONTAINS e NOT_CONTAINS per la mappa delle regole di automazione e i criteri delle stringhe.

25 luglio 2023

[Regole di automazione](#)

Security Hub ora offre regole di automazione che aggiornano automaticamente i risultati in base a criteri specificati dall'utente.

13 giugno 2023

[Nuova integrazione con terze parti](#)

Snyk è una nuova integrazione di terze parti che invia i risultati a Security Hub.

12 giugno 2023

[Controlli di sicurezza esistenti aggiunti a Service-Managed Standard: AWS Control Tower](#)

I seguenti controlli Security Hub esistenti sono stati aggiunti a Service-Managed Standard: AWS Control Tower

12 giugno 2023

- [the section called “\[Account .1\] Le informazioni di contatto di sicurezza devono essere fornite per un Account AWS”](#)
- [the section called “\[ApiGateway.8\] Le rotte API Gateway devono specificare un tipo di autorizzazione”](#)
- [the section called “\[ApiGateway.9\] La registrazione degli accessi deve essere configurata per API Gateway V2 Stages”](#)
- [the section called “\[CodeBuild.3\] I log CodeBuild S3 devono essere crittografati”](#)
- [the section called “\[EC2.25\] I modelli di lancio di Amazon EC2 non devono assegnare IP pubblici alle interfacce di rete”](#)
- [the section called “\[ELB.1\] Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS”](#)
- [the section called “\[Redshift.10\] I cluster Redshift](#)

devono essere crittografati a riposo”

- the section called “[SageMaker.2] le istanze dei SageMaker notebook devono essere avviate in un VPC personalizzato”
- the section called “[SageMaker.3] Gli utenti non devono avere accesso root alle SageMaker istanze dei notebook”
- the section called “[WAF.10] Gli ACL AWS WAF web devono avere almeno una regola o un gruppo di regole”

Nuovi controlli di sicurezza

Sono disponibili i seguenti nuovi controlli del Security Hub:

6 giugno 2023

- the section called “[ACM.2] I certificati RSA gestiti da ACM devono utilizzare una lunghezza di chiave di almeno 2.048 bit”
- the section called “[AppSync .2] AWS AppSync dovrebbe avere la registrazione a livello di campo abilitata”
- the section called “[CloudFront.13] CloudFront le distribuzioni devono utilizzare e il controllo dell'accesso all'origine”
- the section called “[Elastic Beanstalk.3] Elastic Beanstalk dovrebbe trasmettere i log a CloudWatch”
- the section called “[S3.17] I bucket generici S3 devono essere crittografati quando sono inattivi con AWS KMS keys”
- the section called “[StepFunctions.1] Le macchine a stati Step Functions dovrebbero avere la registrazione attivata”

[Security Hub disponibile in Asia Pacifico \(Melbourne\)](#)

Security Hub è ora disponibile in Asia Pacifico (Melbourne). Tutte le funzionalità del Security Hub sono ora disponibili in questa regione, ad eccezione di alcuni controlli di sicurezza. Per ulteriori informazioni, vedere [Disponibilità dei controlli per regione](#).

25 maggio 2023

[Ricerca della cronologia](#)

Security Hub può ora tenere traccia della cronologia di un ritrovamento negli ultimi 90 giorni.

4 maggio 2023

[Nuovi controlli di sicurezza](#)

Sono disponibili i seguenti nuovi controlli del Security Hub:

29 marzo 2023

- [the section called “\[EKS.1\] Gli endpoint del cluster EKS non dovrebbero essere accessibili al pubblico”](#)
- [the section called “\[ELB.16\] Gli Application Load Balancer devono essere associati a un ACL web AWS WAF”](#)
- [the section called “\[Redshift.10\] I cluster Redshift devono essere crittografati a riposo”](#)
- [the section called “\[S3.15\] I bucket generici S3 devono avere Object Lock abilitato”](#)

Supporto esteso per risultati di controllo consolidati	L' Automated Security Response nella versione AWS 2.0.0 ora supporta i risultati di controllo consolidati.	24 marzo 2023
Security Hub disponibile in nuove versioni Regioni AWS	Security Hub è ora disponibile in Asia Pacifico (Hyderabad), Europa (Spagna) ed Europa (Zurigo). Esistono dei limiti ai controlli disponibili in queste regioni.	21 marzo 2023
Aggiornamento della politica gestita	Security Hub ha aggiornato un'autorizzazione esistente nella policy <code>AWSSecurityHubServiceRolePolicy</code> gestita.	17 marzo 2023

Nuovi controlli di sicurezza per lo standard NIST 800-53

Security Hub ha aggiunto i seguenti controlli di sicurezza , applicabili allo standard NIST 800-53:

3 marzo 2023

- the section called “[Account .2] Account AWS deve far parte di un'organizzazione AWS Organizations”
- the section called “[CloudWatch.15] gli CloudWatch allarmi devono avere azioni specificate configurate”
- the section called “[CloudWatch.16] i gruppi di CloudWatch log devono essere conservati per un periodo di tempo specificato”
- the section called “[CloudWatch.17] le azioni di CloudWatch allarme devono essere attivate”
- the section called “[DynamoDB.4] Le tabelle DynamoDB devono essere presenti in un piano di backup”
- the section called “[EC2.28] I volumi EBS devono essere coperti da un piano di backup”
- EC2.29 — Le istanze EC2 devono essere avviate in un VPC (ritirato)

- [the section called “\[RDS.26\] Le istanze DB RDS devono essere protette da un piano di backup”](#)
- [the section called “\[S3.14\] I bucket generici S3 devono avere il controllo delle versioni abilitato”](#)
- [the section called “\[WAF.11\] la registrazione ACL web deve essere abilitata AWS WAF”](#)

[Istituto nazionale di standard e tecnologia \(NIST\) 800-53 Rev. 5](#)

Security Hub ora supporta lo standard NIST 800-53 Rev. 5 con oltre 200 controlli di sicurezza applicabili.

28 febbraio 2023

[Controlli consolidati: visualizzazione e controllo dei risultati](#)

Con il rilascio della visualizzazione dei controlli consolidati, la pagina Controlli della console Security Hub mostra tutti i controlli tra gli standard. Ogni controllo ha lo stesso ID di controllo per tutti gli standard. Quando attivi i risultati del controllo consolidato, ricevi un solo risultato per controllo di sicurezza anche quando un controllo si applica a più standard abilitati.

23 febbraio 2023

Nuovi controlli di sicurezza

Sono disponibili i seguenti nuovi controlli del Security Hub. Alcuni controlli hanno limitazioni regionali.

16 febbraio 2023

- the section called “[ElastiC ache.1] I cluster ElastiCache Redis dovrebbero avere il backup automatico abilitato”
- the section called “[ElastiC ache.2] ElastiCache per i cluster di cache Redis dovrebbe avere l'aggiornamento automatico della versione secondaria abilitato”
-
- the section called “[ElastiC ache.3] ElastiCache per i gruppi di replica Redis dovrebbe avere il failover automatico abilitato”
- the section called “[ElastiC ache.4] ElastiCache per i gruppi di replica Redis deve essere crittografato a riposo”
- the section called “[ElastiC ache.5] ElastiCache per i gruppi di replica Redis devono essere crittografati in transito”
- the section called “[ElastiC ache.6] ElastiCache per i gruppi di replica Redis precedenti alla versione 6.0

[è necessario utilizzare Redis AUTH”](#)

- [the section called “\[Elasticache.7\] ElastiCache i cluster non devono utilizzare il gruppo di sottoreti predefinito”](#)

[Nuovi campi ASFF](#)

Security Hub è stato aggiunto ProductFields. ArchivalReasonsSecurity Hub ProductFields è stato aggiunto. ----sep----:0/Description and. ArchivalReasons:0/Description ReasonCode e. AWS ----sep-- --:0/ al Security Finding Format (ASFF).

8 febbraio 2023

[Nuovi campi ASFF](#)

Security Hub ha aggiunto la conformità. Associate dStandards e conformità. SecurityControlId al AWS Security Finding Format (ASFF).

31 gennaio 2023

[I dettagli sulla vulnerabilità sono ora disponibili](#)

Ora puoi visualizzare i dettagli delle vulnerabilità nella console Security Hub per conoscere i risultati che Amazon Inspector invia a Security Hub.

14 gennaio 2023

[Security Hub è disponibile in Medio Oriente \(Emirati Arabi Uniti\)](#)

Security Hub è ora disponibile in Medio Oriente (Emirati Arabi Uniti). Alcuni controlli hanno limiti regionali.

12 gennaio 2023

È stata aggiunta l'integrazione di terze parti con MetricStream	Security Hub ora supporta l'integrazione di terze parti MetricStream in tutte le regioni tranne Cina e AWS GovCloud (US).	11 gennaio 2023
Aumento del limite degli account organizzativi	Security Hub ora supporta fino a 11.000 account membro per ogni account amministratore di Security Hub per regione.	27 dicembre 2022
ElasticBeanstalk3. È stato ripristinato	Security Hub ha ripristinato il controllo [ElasticBeanstalk.3] Elastic Beanstalk dovrebbe trasmettere CloudWatch i log dallo standard FSBP in tutte le regioni.	21 dicembre 2022
Security Hub aggiunge nuovi controlli di sicurezza	I nuovi controlli Security Hub sono disponibili per i clienti che hanno abilitato lo standard FSBP. Alcuni controlli hanno limitazioni regionali .	15 dicembre 2022
Linee guida sulle funzionalità imminenti	Security Hub prevede di rilasciare due nuove funzionalità: visualizzazione dei controlli consolidati e risultati del controllo consolidato. Queste funzionalità imminenti potrebbero influire sui flussi di lavoro esistenti che si basano sul controllo della ricerca di campi e valori.	9 dicembre 2022

L'integrazione con Amazon Security Lake è ora disponibile	Security Lake ora si integra con Security Hub ricevendo i risultati del Security Hub.	29 novembre 2022
Support per Service-Managed Standard: AWS Control Tower	Security Hub supporta un nuovo standard di sicurezza chiamato Service-Managed Standard: AWS Control Tower. AWS Control Tower gestisce questo standard.	28 novembre 2022
CIS AWS Foundations Benchmark v1.4.0 è ora disponibile nelle regioni della Cina	Security Hub ora supporta CIS AWS Foundations Benchmark v1.4.0 nelle regioni cinesi.	18 novembre 2022
L'integrazione con Jira Service Management Cloud è ora disponibile	Jira Service Management Cloud ora riceve i risultati del Security Hub in tutte le regioni disponibili, ad eccezione delle regioni cinesi.	17 novembre 2022
AWS IoT Device Defender integrazione ora disponibile	AWS IoT Device Defender ora invia i risultati al Security Hub in tutte le regioni disponibili.	17 novembre 2022
Support per CIS AWS Foundations Benchmark v1.4.0	Security Hub ora fornisce controlli di sicurezza che supportano CIS AWS Foundations Benchmark v1.4.0. Questo standard è disponibile in tutte le regioni disponibili, ad eccezione delle regioni cinesi.	9 novembre 2022

[Supporto per gli annunci del Security Hub in AWS GovCloud \(US\)](#)

Ora puoi iscriverti agli annunci di Security Hub con Amazon Simple Notification Service (Amazon SNS) AWS GovCloud negli Stati Uniti orientali AWS GovCloud e negli Stati Uniti occidentali per ricevere notifiche su Security Hub.

3 ottobre 2022

[AWS Security Hub aggiunge un nuovo controllo di sicurezza](#)

Il nuovo controllo Security Hub AutoScaling9.9 è disponibile per i clienti che hanno abilitato lo standard FSBP. [I controlli possono avere limitazioni regionali.](#)

1 settembre 2022

[Iscriviti agli annunci di Security Hub](#)

Ora puoi iscriverti agli annunci di Security Hub con Amazon Simple Notification Service (Amazon SNS) per ricevere notifiche su Security Hub.

29 agosto 2022

[Espansione regionale per l'aggregazione tra regioni](#)

L'aggregazione tra regioni è ora disponibile per ottenere risultati, trovare aggiornamenti e approfondimenti in tutto il mondo. AWS GovCloud (US)

2 agosto 2022

[Nuove integrazioni di prodotti di terze parti](#)

Fortinet - FortiCNP è un'integrazione di terze parti che riceve i risultati di Security Hub e JFrog è un'integrazione di terze parti che invia i risultati a Security Hub.

26 luglio 2022

EC2.27 è stato ritirato	Security Hub ha ritirato EC2.27 - Le istanze EC2 in esecuzione non devono utilizzare coppie di chiavi, un controllo precedente dello standard AWS Foundatio nal Security Best Practices (FSBP).	20 luglio 2022
Lambda.2 non supporta più python3.6	Security Hub non supporta più python3.6 come parametro per Lambda.2 - Le funzioni Lambda devono utilizzare runtime supportati, un controllo nello standard Foundatio nal Security Best Practices (FSBP). AWS	19 luglio 2022
AWS Security Hub aggiunge nuovi controlli di sicurezza	I nuovi controlli Security Hub sono disponibili per i clienti che hanno abilitato lo standard FSBP. Alcuni controlli hanno limitazioni regionali .	22 giugno 2022
AWS Security Hub supporta una nuova regione	Security Hub è ora disponibi le in Asia Pacifico (Giacarta). Alcuni controlli non sono disponibili in questa regione.	7 luglio 2022
Migliore integrazione tra AWS Security Hub e AWS Config	Gli utenti di Security Hub possono vedere i risultati delle valutazioni delle AWS Config regole come risultati in Security Hub.	6 giugno 2022

<u>Aggiunta la possibilità di disattivare gli standard con attivazione automatica</u>	Per gli utenti che hanno effettuato l'integrazione con AWS Organizations, questa funzionalità consente di accedere all'account amministratore di Security Hub e disattivare gli account dei nuovi membri dagli standard di attivazione automatica.	25 aprile 2022
<u>Aggregazione estesa tra regioni</u>	Aggiunta l'aggregazione tra regioni per controllare gli stati e i punteggi di sicurezza.	20 aprile 2022
<u>CompanyName e ora ProductName sono attributi di primo livello</u>	Sono stati aggiunti nuovi attributi di primo livello per l'impostazione dei nomi di società e prodotti associati alle integrazioni personalizzate	1 aprile 2022
<u>Aggiunti nuovi controlli allo standard AWS Foundational Security Best Practices</u>	Sono stati aggiunti 5 nuovi controlli allo standard AWS Foundational Security Best Practices.	31 marzo 2022
<u>Aggiunti nuovi oggetti di dettaglio delle risorse ad ASFF</u>	È stato aggiunto un tipo di AwsRdsDbSecurityGroup risorsa ad ASFF.	25 marzo 2022
<u>Sono stati aggiunti dettagli aggiuntivi sulle risorse in ASFF</u>	Sono stati aggiunti ulteriori dettagli a AwsAutoScalingScalingGroup, AwsElasticLoadBalancing, AwsRedshiftCluster, e AwsCodeBuildProject.	25 marzo 2022

Sono stati aggiunti nuovi controlli allo standard AWS Foundational Security Best Practices	Aggiunti 15 nuovi controlli allo standard AWS Foundational Security Best Practices.	16 marzo 2022
Sono stati aggiunti nuovi controlli allo standard AWS Foundational Security Best Practices e al Payment Card Industry Data Security Standard (PCI DSS)	Sono stati aggiunti nuovi controlli per Amazon OpenSearch Service, Amazon RDS, Amazon EC2, Elastic Load Balancing e AWS allo standard Foundational CloudFront Security Best Practices. Sono stati inoltre aggiunti due nuovi controlli per OpenSearch Service al PCI DSS.	15 febbraio 2022
Aggiunto un nuovo campo ad ASFF	Nuovo campo aggiunto: Sample.	26 gennaio 2022
Aggiunta integrazione con AWS Health	AWS Health utilizza la messaggistica service-to-service degli eventi per inviare i risultati a Security Hub.	19 gennaio 2022
Aggiunta integrazione con AWS Trusted Advisor	Trusted Advisor invia i risultati dei controlli a Security Hub come risultati del Security Hub. Security Hub invia i risultati dei controlli relativi alle Buone Pratiche di Sicurezza AWS Fondamentali a Trusted Advisor.	18 gennaio 2022

[Oggetti aggiornati con i dettagli delle risorse in ASFF](#)

Aggiunti `MixedInstancesPolicy` e `AvailabilityZones` a `AwsAutoScalingAutoScalingGroup`. È stato aggiunto `MetadataOptions` a `AwsAutoScalingLaunchConfiguration`. È stato aggiunto `BucketVersioningConfiguration` a `AwsS3Bucket`.

20 dicembre 2021

[Output aggiornato per la documentazione ASFF](#)

Le descrizioni degli attributi ASFF erano precedentemente contenute in un unico argomento. Ogni oggetto di primo livello e ogni oggetto relativo ai dettagli delle risorse ora si trova in un argomento a sé stante. L'argomento sulla sintassi ASFF contiene collegamenti a tali argomenti.

20 dicembre 2021

[Sono stati aggiunti nuovi oggetti di dettaglio delle risorse ad ASFF per AWS Network Firewall](#)

Per AWS Network Firewall, sono stati aggiunti i seguenti oggetti di dettaglio delle risorse: `AwsNetworkFirewallFirewall`, `AwsNetworkFirewallPolicy`, e `AwsNetworkFirewallRuleGroup`.

20 dicembre 2021

È stato aggiunto il supporto per la nuova versione di Amazon Inspector	Security Hub è integrato con la nuova versione di Amazon Inspector e con Amazon Inspector Classic. Amazon Inspector invia i risultati a Security Hub.	29 novembre 2021
È stata modificata la gravità di EC2.19	La severità di EC2.19 (i gruppi di sicurezza non dovrebbero consentire l'accesso illimitato alle porte ad alto rischio) è stata modificata da Alta a Critica.	17 novembre 2021
Nuova integrazione con Sonrai Dig	Security Hub offre ora un'integrazione con Sonrai Dig. Sonrai Dig monitora gli ambienti cloud per identificare i rischi per la sicurezza. Sonrai Dig invia i risultati a Security Hub.	12 novembre 2021
Controllo aggiornato per i controlli CIS 2.1 e CloudTrail 2.1	Oltre a verificare che sia presente almeno un CloudTrail percorso multiregionale, CIS 2.1 e CloudTrail 2.1 ora controllano anche che il ExcludeManagementEventSources parametro sia vuoto in almeno uno dei percorsi multiregione. CloudTrail	9 novembre 2021
Aggiunto il supporto per gli endpoint VPC	Security Hub è ora integrato AWS PrivateLink e supporta gli endpoint VPC.	3 novembre 2021

Controlli aggiunti allo standard AWS Foundational Security Best Practices	Aggiunti nuovi controlli per Elastic Load Balancing (ELB.2 e ELB.8) e (SSM.4). AWS Systems Manager	2 novembre 2021
Porte aggiunte al controllo del controllo EC2.19	EC2.19 ora verifica anche che i gruppi di sicurezza non consentano l'accesso illimitato in ingresso alle seguenti porte: 3000 (framework di sviluppo web Go, Node.js e Ruby), 5000 (framework di sviluppo web Python), 8088 (porta HTTP legacy) e 8888 (porta HTTP alternativa)	27 ottobre 2021
È stata aggiunta l'integrazione con Logz.io Cloud SIEM	Logz.io è un fornitore di Cloud SIEM che fornisce una correlazione avanzata di dati di log ed eventi per aiutare i team di sicurezza a rilevare, analizzare e rispondere alle minacce alla sicurezza in tempo reale. Logz.io riceve i risultati dal Security Hub.	25 ottobre 2021

[È stato aggiunto il supporto per l'aggregazione dei risultati tra regioni](#)

L'aggregazione tra regioni consente di visualizzare tutti i risultati senza dover modificarle le regioni. Gli account amministratore scelgono una regione di aggregazione e le regioni collegate. I risultati relativi all'account amministratore e ai relativi account membro vengono aggregati dalle regioni collegate alla regione di aggregazione.

20 ottobre 2021

[Oggetti aggiornati con i dettagli delle risorse in ASFF](#)

Sono stati aggiunti i dettagli del certificato del visualizzatore a. `AwsCloudFrontDistribution` Sono stati aggiunti dettagli aggiuntivi a `AwsCodeBuildProject`. Sono stati aggiunti gli attributi del load balancer a. `AwsElasticLoadBalancingV2LoadBalancer` È stato aggiunto l'identificatore dell'account del proprietario del bucket S3 a. `AwsS3Bucket`

8 ottobre 2021

Aggiunti nuovi oggetti di dettaglio delle risorse ad ASFF	Sono stati aggiunti i seguenti nuovi oggetti di dettaglio delle risorse ad ASFF: AwsEc2VpcEndpointService, AwsEcrRepository, AwsEksCluster, AwsOpenSearchServiceDomain, AwsWafRateBasedRule, AwsWafRegionalRateBasedRule, AwsXrayEncryptionConfig	8 ottobre 2021
Runtime obsoleto rimosso dal controllo Lambda.2	Nello standard AWS Foundational Security Best Practices, il dotnetcore2.1 runtime è stato rimosso da [Lambda.2]. Le funzioni Lambda devono utilizzare i runtime supportati.	6 ottobre 2021
Nuovo nome per l'integrazione con Check Point	L'integrazione con Check Point Dome9 Arc è ora Check Point CloudGuard Posture Management. L'ARN di integrazione non è cambiato.	1° ottobre 2021
Rimossa l'integrazione con Alcide	L'integrazione con Alcide KAudit è stata interrotta.	30 settembre 2021
Modificata la gravità di EC2.19	La severità di [EC2.19] I gruppi di sicurezza non dovrebbero consentire l'accesso illimitato alle porte ad alto rischio è stata modificata da Media a Alta.	30 settembre 2021

L'integrazione con AWS Organizations è ora supportata nelle regioni cinesi	L'integrazione del Security Hub con Organizations è ora supportata in Cina (Pechino) e Cina (Ningxia).	20 settembre 2021
Nuova AWS Config regola per i controlli S3.1 e PCI.S3.6	Sia S3.1 che PCI.S3.6 verificano che l'impostazione Amazon S3 Block Public Access sia abilitata. La AWS Config regola per questi controlli viene modificata da <code>a. s3-account-level-public-access-block</code> a <code>s3-account-level-public-access-block-periodic</code> .	14 settembre 2021
Runtime obsoleti rimossi dal controllo Lambda.2	Nello standard AWS Foundational Security Best Practices, i <code>ruby2.5</code> runtime <code>nodejs10.x</code> and rimossi da [Lambda.2] Le funzioni Lambda devono utilizzare i runtime supportati.	13 settembre 2021
È stata modificata la gravità del controllo CIS 2.2	Nello standard CIS AWS Foundations Benchmark, la gravità per 2.2. — La verifica che la convalida dei file di CloudTrail registro sia abilitata viene modificata da Bassa a Media.	13 settembre 2021

[ECS.1, Lambda.2 e SSM.1 aggiornati nello standard Foundational Security Best Practices AWS](#)

Nello standard AWS Foundational Security Best Practices, ECS.1 ha ora un parametro impostato su `SkipInactiveTaskDefinitions` `true`. Ciò garantisce che il controllo controlli solo le definizioni delle attività attive. Per Lambda.2, è stato aggiunto Python 3.9 all'elenco dei runtime. SSM.1 ora controlla sia le istanze interrotte che quelle in esecuzione.

7 settembre 2021

[Il controllo PCI.Lambda.2 ora esclude le risorse Lambda @Edge](#)

Nello standard Payment Card Industry Data Security Standard (PCI DSS), il controllo PCI.Lambda.2 ora esclude le risorse Lambda @Edge.

7 settembre 2021

[È stata aggiunta l'integrazione con HackerOne Vulnerability Intelligence](#)

Security Hub offre ora un'integrazione con HackerOne Vulnerability Intelligence. L'integrazione invia i risultati a Security Hub.

7 settembre 2021

[Oggetti di dettaglio delle risorse aggiornati in ASFF](#)

Per `AwsKmsKey`, aggiunto `KeyRotationStatus`. Per `AwsS3Bucket`, ha aggiunto `AccessControlListBucketLoggingConfiguration`, `BucketNotificationConfiguration`, e `BucketWebsiteConfiguration`.

2 settembre 2021

Sono stati aggiunti nuovi oggetti di dettaglio delle risorse ad ASFF	Sono stati aggiunti i seguenti nuovi oggetti di dettaglio delle risorse ad ASFF: <code>AwsAutoScalingLaunchConfiguration</code> , <code>AwsEc2VpnConnection</code> , e <code>AwsEcrContainerImage</code>	2 settembre 2021
Sono stati aggiunti dettagli all'<code>Vulnerabilities</code> oggetto in ASFF	<code>InCvss</code> , aggiunto <code>Adjustments</code> e <code>Source InVulnerablePackages</code> , ha aggiunto il percorso del file e il gestore dei pacchetti.	2 settembre 2021
Systems Manager Explorer e OpsCenter l'integrazione sono ora supportati nelle regioni cinesi	Il Security Hub si integra con SSM Explorer ed OpsCenter è ora supportato in Cina (Pechino) e Cina (Ningxia).	31 agosto 2021
Ritiro del controllo Lambda.4	Security Hub sta ritirando il controllo [Lambda.4] Le funzioni Lambda dovrebbero avere una coda di lettere non scritte configurata. Quando un controllo viene ritirato, non viene più visualizzato sulla console e Security Hub non esegue controlli su di esso.	31 agosto 2021

[Ritiro del controllo PCI.EC2.3](#)

Security Hub sta ritirando il controllo [PCI.EC2.3] I gruppi di sicurezza EC2 non utilizzati devono essere rimossi. Quando un controllo viene ritirato, non viene più visualizzato sulla console e Security Hub non esegue controlli su di esso.

27 agosto 2021

[Modifica del modo in cui Security Hub invia i risultati alle azioni personalizzate](#)

Quando invii i risultati a un'azione personalizzata, Security Hub ora invia ogni risultato in un Security Hub Findings - Custom Action evento separato.

20 agosto 2021

[Aggiunto un nuovo codice motivo dello stato di conformità per i runtime Lambda personalizzati](#)

È stato aggiunto un nuovo codice motivo dello stato di LAMBDA_CUSTOM_RUNTIME_DETAILS_NOT_AVAILABLE conformità. Questo codice motivo indica che Security Hub non è riuscito a eseguire un controllo rispetto a un runtime Lambda personalizzato.

20 agosto 2021

[AWS Firewall Manager integrazione ora supportata nelle regioni cinesi](#)

L'integrazione del Security Hub con Firewall Manager è ora supportata in Cina (Pechino) e Cina (Ningxia).

19 agosto 2021

[Nuove integrazioni con e Caveonix CloudForcepoint Cloud Security Gateway](#)

Security Hub ora offre integrazioni con Caveonix Cloud eForcepoint Cloud Security Gateway. Entrambe le integrazioni inviano i risultati a Security Hub.

10 agosto 2021

[Aggiunti nuovi CompanyName Region attributi ProductName e ad ASFF](#)

Aggiunti CompanyName Region campi e al livello superiore dell'ASFF. ProductName Questi campi vengono compilati automaticamente e, ad eccezione delle integrazioni di prodotti personalizzati, non possono essere aggiornati utilizzando o. BatchImportFindings s BatchUpdateFindings s Sulla console, i filtri di ricerca utilizzano questi nuovi campi. Nell'API, i ProductName filtri CompanyName and utilizzano gli attributi sottostantiProductFields .

23 luglio 2021

[Oggetti di dettaglio delle risorse aggiunti e aggiornati in ASFF](#)

Sono stati aggiunti un nuovo tipo di AwsRdsEventSubscription risorsa e nuovi dettagli sulla risorsa. Sono stati aggiunti dettagli sulla risorsa per il tipo di AwsEcsService risorsa. Sono stati aggiunti attributi all'oggetto dei dettagli della AwsElasticsearchDomain risorsa.

23 luglio 2021

Sono stati aggiunti controlli allo standard AWS Foundational Security Best Practices	Aggiunti nuovi controlli per Amazon API Gateway (APIGateway.5), Amazon EC2 (EC2.19), Amazon ECS (ECS.2), Elastic Load Balancing (ELB.7), Amazon Service (da ES.5 a ES.8), Amazon RDS (da RDS.16 a RDS.23), OpenSearch Amazon Redshift (Redshift .4) e Amazon Amazon SQS (SQS.1).	20 luglio 2021
È stata spostata un'autorizzazione all'interno della policy gestita dei ruoli collegati al servizio	L'config:PutEvaluations autorizzazione è stata spostata all'interno della politica gestitaAWSSecurityHubServiceRolePolicy , in modo che venga applicata a tutte le risorse.	14 luglio 2021
Sono stati aggiunti controlli allo standard AWS Foundational Security Best Practices	Sono stati aggiunti nuovi controlli per Amazon API Gateway (APIGateway.4), Amazon CloudFront (.5 e CloudFront .6), CloudFront Amazon EC2 (EC2.17 ed EC2.18), Amazon ECS (ECS.1), Amazon Service AWS Identity and Access Management (ES.4), (IAM.21 OpenSearch), Amazon RDS (RDS.15) e Amazon S3 (S3.8).	8 luglio 2021

[Aggiunti nuovi codici di motivo dello stato di conformità per i risultati del controllo](#)

INTERNAL_SERVICE_ERROR indica che si è verificato un errore sconosciuto. SNS_TOPIC_CROSS_ACCOUNT_COUNT indica che l'argomento SNS è di proprietà di un account diverso. SNS_TOPIC_INVALID indica che l'argomento SNS associato non è valido.

6 luglio 2021

[È stata aggiunta l'integrazione con AWS Chatbot](#)

È stata aggiunta l'integrazione con AWS Chatbot. Security Hub invia i risultati a AWS Chatbot.

30 giugno 2021

[È stata aggiunta una nuova autorizzazione alla politica di gestione dei ruoli collegati al servizio](#)

È stata aggiunta una nuova autorizzazione alla policy gestita AWSecurityHubServiceRolePolicy per consentire al ruolo collegato al servizio di fornire risultati di valutazione a. AWS Config

29 giugno 2021

[Oggetti nuovi e aggiornati per i dettagli delle risorse in ASFF](#)

Sono stati aggiunti nuovi oggetti di dettaglio delle risorse per i cluster ECS e le definizioni delle attività ECS. È stato aggiornato l'oggetto dell'istanza EC2 per elencare le interfacce di rete associate. È stato aggiunto l'ID del certificato client per le fasi API Gateway V2. È stata aggiunta la configurazione del ciclo di vita per i bucket S3.

24 giugno 2021

[Aggiornato il calcolo degli stati di controllo aggregati e dei punteggi di sicurezza standard](#)

Security Hub ora calcola lo stato di controllo complessivo e il punteggio di sicurezza standard ogni 24 ore. Per gli account amministratore, il punteggio ora indica se ogni controllo è abilitato o disabilitato per ogni account.

23 giugno 2021

[Informazioni aggiornate sulla gestione degli account sospesi da parte di Security Hub](#)

Sono state aggiunte informazioni su come Security Hub gestisce gli account sospesi AWS.

23 giugno 2021

[Sono state aggiunte schede per visualizzare i controlli abilitati e disabilitati per il singolo account amministratore](#)

Per l'account amministratore, le schede principali della pagina dei dettagli standard contengono informazioni aggregate su tutti gli account. Le nuove schede Abilitato per questo account e Disabilitato per questo account elencano gli account abilitati o disabilitati per il singolo account amministratore.

23 giugno 2021

[Aggiunto java8.a12 ai parametri per Lambda.2](#)

Nello standard AWS Foundational Security Best Practices, aggiunto java8.a12 ai runtime supportati per il Lambda.2 controllo.

8 giugno 2021

[Nuove integrazioni con NETSCOUT Cyber MicroFocus ArcSight Investigator](#)

Aggiunte integrazioni con NETSCOUT Cyber Investigator. MicroFocus ArcSight MicroFocus ArcSight riceve i risultati da Security Hub. NETSCOUT Cyber Investigator invia i risultati al Security Hub.

7 giugno 2021

[Sono stati aggiunti dettagli per AWSecurityHubServiceRolePolicy](#)

È stata aggiornata la sezione delle politiche gestite per aggiungere dettagli per la politica gestita esistente AWSecurityHubServiceRolePolicy , utilizzato dal ruolo collegato al servizio Security Hub.

4 giugno 2021

[Nuova integrazione con Jira Service Management](#)

Il AWS Service Management Connector per Jira invia i risultati a Jira e li usa per creare problemi con Jira. Quando i problemi di Jira vengono aggiornati, vengono aggiornati anche i risultati corrispondenti in Security Hub.

26 maggio 2021

[È stato aggiornato l'elenco dei controlli supportati per la regione Asia Pacifico \(Osaka\)](#)

Sono stati aggiornati lo standard CIS AWS Foundations e il Payment Card Industry Data Security Standard (PCI DSS) per indicare i controlli che non sono supportati in Asia Pacifico (Osaka).

21 maggio 2021

<u>Nuova integrazione con Sysdig Secure per il cloud</u>	Aggiunta un'integrazione con Sysdig Secure per il cloud. L'integrazione invia i risultati a Security Hub.	14 maggio 2021
<u>Controlli aggiunti allo standard AWS Foundational Security Best Practices</u>	Aggiunti nuovi controlli per Amazon API Gateway (APIGateway.2 e APIGateway.3), (.4 e CloudTrail .5) CloudTrail, Amazon EC2 (EC2.15 AWS CloudTrail ed EC2.16), (.1 e .2), (Lambda.4), Amazon RDS (ElasticBeanstalkRDS.12 — RDS.14) ElasticBeanstalk, Amazon Redshift (Redshift.7), (AWS Elastic Beanstalk .3 e .4 AWS Lambda) e (WAF.1). AWS Secrets Manager SecretsManager AWS WAF	10 maggio 2021
<u>Aggiornamenti GuardDuty e controlli Amazon RDS</u>	È stata modificata la gravità GuardDuty.1 PCI.GuardDuty.1 da Media a Alta. È stato aggiunto un databaseEngines parametro aRDS.8.	4 maggio 2021
<u>Sono stati aggiunti nuovi dettagli sulle risorse all'ASFF</u>	NelResources.Details , sono stati aggiunti nuovi oggetti di dettaglio delle risorse per gli ACL di rete Amazon EC2, le sottoreti Amazon EC2 e gli ambienti. AWS Elastic Beanstalk	3 maggio 2021

Aggiunti campi della console per fornire valori di filtro per EventBridge le regole di Amazon	I nuovi modelli di filtro predefiniti per EventBridge le regole di Security Hub forniscono campi della console che è possibile utilizzare per specificare i valori del filtro.	30 aprile 2021
È stata aggiunta l'integrazione con AWS Systems Manager Explorer e OpsCenter	Security Hub ora supporta l'integrazione con Systems Manager Explorer e OpsCenter. L'integrazione riceve i risultati da Security Hub e li aggiorna in Security Hub.	26 Aprile 2021
Nuovo tipo di integrazione dei prodotti	Un nuovo tipo di integrazione indica che l'integrazione di un prodotto aggiorna i risultati ricevuti da Security Hub. UPDATE_FINDINGS_IN_SECURITY_HUB	22 Aprile 2021
Il termine "account principale" è stato modificato in "account amministratore"	Il termine "account principale" viene modificato in "account amministratore". Il termine viene modificato anche nella console e nell'API di Security Hub.	22 Aprile 2021
APIGateway.1 aggiornato o per sostituire HTTP con Websocket	Sono stati aggiornati il titolo, la descrizione e la correzione per APIGateway.1. Il controllo ora verifica la registrazione dell'esecuzione dell'API Websocket anziché la registrazione dell'esecuzione dell'API HTTP.	9 aprile 2021

GuardDuty L'integrazione con Amazon è ora supportata a Pechino e Ningxia	L'integrazione del Security Hub con GuardDuty è ora supportata nelle regioni Cina (Pechino) e Cina (Ningxia).	5 aprile 2021
Aggiunto nodejs14.x ai runtime supportati per il controllo Lambda.2	Il controllo Lambda.2 nello standard Foundational Security Best Practices ora supporta il runtime. nodejs14.x	30 marzo 2021
Lancio del Security Hub in Asia Pacifico (Osaka)	Security Hub è ora disponibile nella regione Asia Pacifico (Osaka).	29 marzo 2021
Sono stati aggiunti i campi di ricerca del fornitore alla ricerca dei dettagli	Nel pannello dei dettagli dei risultati, la nuova sezione Finding Provider Fields contiene i valori del provider di ricerca relativi a fiducia, criticità, risultati correlati, gravità e tipi.	24 marzo 2021
Aggiunta l'opzione per ricevere dati sensibili da Amazon Macie	L'integrazione con Macie può ora essere configurata per inviare risultati sensibili a Security Hub.	23 marzo 2021
Passaggio alla gestione degli AWS Organizations account	Per i clienti che dispongono di un account amministratore esistente con account membro, sono state aggiunte nuove informazioni su come passare dalla gestione degli account su invito alla gestione degli account tramite Organizations.	22 marzo 2021

[Nuovi oggetti in ASFF per informazioni sulla configurazione del blocco di accesso pubblico di Amazon S3](#)

NelResources , un nuovo tipo di AwsS3AccountPublicAccessBlock risorsa e un nuovo oggetto di dettaglio forniscono informazioni sulla configurazione del blocco di accesso pubblico di Amazon S3 per gli account. Nell'oggetto AwsS3Bucket Resource Details, l'PublicAccessBlockConfiguration oggetto fornisce la configurazione Public Access Block per il bucket S3.

18 marzo 2021

[Nuovo oggetto in ASFF per consentire ai provider di ricerca di aggiornare campi specifici](#)

Il nuovo FindingProviderFields oggetto in ASFF viene utilizzato per BatchImportFindings fornire valori perConfidence , Criticality RelatedFindings Severity, e. Types I campi originali devono essere aggiornati solo utilizzandoBatchUpdateFindings .

18 marzo 2021

[Nuovo DataClassification oggetto per le risorse in ASFF](#)

Il nuovo Resources .DataClassification oggetto in ASFF viene utilizzato per fornire informazioni sui dati sensibili rilevati sulla risorsa.

18 marzo 2021

CONFIG_RETURNS_NOT_APPLICABLE Valore aggiunto ai codici di stato di conformità disponibili	Per lo stato di NOT_AVAILABLE conformità, è stato rimosso il codice motivo RESOURCE_NO_LONGER_EXISTS e aggiunto il codice motivo CONFIG_RETURNS_NOT_APPLICABLE .	16 marzo 2021
Nuova politica gestita per l'integrazione con AWS Organizations	Una nuova policy gestita fornisce AWSSecurityHubOrganizationsAccess le autorizzazioni Organizations necessari e all'account di gestione dell'organizzazione e all'account amministratore delegato di Security Hub.	15 marzo 2021
Le informazioni sulla politica gestita e sui ruoli collegati ai servizi sono state spostate nel capitolo Sicurezza	Le informazioni sulle politiche gestite vengono riviste e ampliate. Sia le informazioni sulle policy gestite che le informazioni sui ruoli collegati ai servizi sono state spostate nel capitolo Sicurezza.	15 marzo 2021
Nuova integrazione con DB SecureCloud	Aggiunto SecureCloud DB all'elenco delle integrazioni di terze parti. SecureCloudDB è uno strumento di sicurezza dei database nativo del cloud che offre una visibilità completa delle posizioni e delle attività di sicurezza interne ed esterne. SecureCloudDB invia i risultati a Security Hub.	4 marzo 2021

Revisione della severità per i controlli CIS 1.1 e CIS 3.1 — CIS 3.14	La severità dei controlli CIS 1.1 e CIS 3.1 — CIS 3.14 è stata modificata in Bassa.	3 marzo 2021
Rimosso il controllo RDS.11	È stato rimosso il controllo RDS.11 dallo standard Foundational Security Best Practices.	3 marzo 2021
Integrazione aggiornata per Turbot	L'integrazione con Turbot viene aggiornata sia per l'invio che per la ricezione dei risultati .	26 febbraio 2021
Controlli aggiunti allo standard Foundational Security Best Practices	Sono stati aggiunti nuovi controlli per Amazon API Gateway (APIGateway.1), Amazon EC2 (EC2.9 ed EC2.10), Amazon Elastic File System (EFS.2), Amazon Service (ES.2 ed ES.3), Elastic Load Balancing OpenSearch (ELB.6) e () (KMS.3). AWS Key Management Service AWS KMS	11 febbraio 2021
È stato aggiunto ProductArn un filtro opzionale all'DescribeProducts API	Il funzionamento dell'DescribeProducts API ora include un ProductArn parametro opzionale. Il ProductArn parametro viene utilizzato per identificare l'integrazione specifica del prodotto per cui restituire i dettagli.	3 febbraio 2021

[Nuova integrazione con Antivirus per Amazon S3 di Cloud Storage Security](#)

L'integrazione con Antivirus for Amazon S3 invia i risultati della scansione antivirus a Security Hub come risultati.

27 gennaio 2021

[È stato aggiornato il processo di calcolo del punteggio di sicurezza per gli account degli amministratori](#)

Per un account amministratore, Security Hub utilizza un processo separato per calcolare il punteggio di sicurezza. Il nuovo processo garantisce che il punteggio includa controlli abilitati per gli account dei membri ma disabilitati per l'account amministratore.

21 gennaio 2021

[Nuovi campi e oggetti nell'ASFF](#)

È stato aggiunto un nuovo Action oggetto per tenere traccia delle azioni avvenute nei confronti di una risorsa. Sono stati aggiunti campi all'AwsEc2NetworkInterface oggetto per tenere traccia dei nomi DNS e degli indirizzi IP. È stato aggiunto un nuovo AwsSsmPatchCompliance oggetto ai dettagli della risorsa.

21 gennaio 2021

Aggiunti controlli allo standard Foundational Security Best Practices	Aggiunti nuovi controlli per Amazon CloudFront (da CloudFront .1 a CloudFront .4), Amazon DynamoDB (da DynamoDB.1 a DynamoDB.3), Elastic Load Balancing (da ELB.3 a ELB.5), Amazon RDS (da RDS.9 a RDS.11), Amazon Redshift (da Redshift.1 a Redshift.3 e Redshift.6) e Amazon SNS (SNS.1).	15 gennaio 2021
Lo stato del flusso di lavoro viene reimpostato in base allo stato del record o allo stato di conformità	Security Hub reimposta automaticamente lo stato del flusso di lavoro da NOTIFIED o RESOLVED verso NEW se un risultato archiviato viene reso attivo o se lo stato di conformità di un risultato cambia da PASSED a FAILEDWARNING, o. NOT_AVAILABLE. Queste modifiche indicano che sono necessarie ulteriori indagini.	7 gennaio 2021
ProductFields Informazioni aggiunte per i risultati basati sul controllo	Per i risultati generati dai controlli, sono state aggiunte informazioni sul contenuto dell'ProductFields oggetto nel AWS Security Finding Format (ASFF).	29 dicembre 2020
Aggiornamenti alle informazioni gestite	Modificato il titolo di insight 5. È stata aggiunta una nuova analisi, 32, che verifica la presenza di utenti IAM con attività sospette.	22 dicembre 2020

Aggiornamenti ai controlli IAM.7 e Lambda.1	Nello standard AWS Foundational Security Best Practices, sono stati aggiornati i parametri per IAM.7. Aggiornati il titolo e la descrizione di Lambda.1.	22 dicembre 2020
Integrazione estesa con ITSM ServiceNow	L'integrazione ServiceNow ITSM consente agli utenti di creare automaticamente incidenti o problemi quando viene ricevuto un risultato del Security Hub. Gli aggiornamenti a questi incidenti o problemi comportano aggiornamenti dei risultati in Security Hub.	11 dicembre 2020
Nuova integrazione con AWS Audit Manager	Security Hub offre ora un'integrazione con AWS Audit Manager. L'integrazione consente all'Audit Manager di ricevere risultati basati sul controllo da Security Hub.	8 dicembre 2020
Nuova integrazione con Aqua Security Kube-bench	Security Hub ha aggiunto un'integrazione con Aqua Security Kube-bench. L'integrazione invia i risultati a Security Hub.	24 novembre 2020
Cloud Custodian è ora disponibile nelle regioni cinesi	L'integrazione con Cloud Custodian è ora disponibile nelle regioni Cina (Pechino) e Cina (Ningxia).	24 novembre 2020

[BatchImportFindings ora può essere utilizzato per aggiornare campi aggiuntivi](#)

In precedenza, non era possibile BatchImportFindings utilizzare e per aggiornare i Types campi Confidence Criticality RelatedFindings ,Severity,, e. Ora, se questi campi non sono stati aggiornati daBatchUpdateFindings , possono essere aggiornati daBatchImportFindings . Una volta aggiornati daBatchUpdateFindings , non possono essere aggiornati daBatchImportFindings .

24 novembre 2020

[Security Hub è ora integrato con AWS Organizations](#)

I clienti possono ora gestire gli account dei membri utilizzando la configurazione dell'account Organizations. L'account di gestione dell'organizzazione designa l'account amministratore di Security Hub, che determina quali account dell'organizzazione abilitare in Security Hub. La procedura di invito manuale può ancora essere utilizzata per gli account che non fanno parte di un'organizzazione.

23 novembre 2020

[È stato rimosso il formato separato dell'elenco dei risultati per i controlli ad alto volume](#)

L'elenco dei risultati per un controllo non utilizza più il formato della pagina Findings quando è presente un numero molto elevato di risultati.

19 novembre 2020

[Integrazioni di terze parti nuove e aggiornate](#)

Security Hub ora supporta le integrazioni con cloudtamer.io, 3CoreSec, Prowler e Kubernetes Security. StackRox IBM QRadar non invia più i risultati. Riceve solo risultati.

30 ottobre 2020

[È stata aggiunta l'opzione per scaricare l'elenco dei risultati dalla pagina dei dettagli del controllo.](#)

Nella pagina dei dettagli del controllo, una nuova opzione di download consente di scaricare l'elenco dei risultati in un file.csv. L'elenco scaricato rispetta tutti i filtri presenti nell'elenco. Se hai selezionato risultati specifici, l'elenco scaricato include solo tali risultati.

26 ottobre 2020

[È stata aggiunta l'opzione per scaricare l'elenco dei controlli dalla pagina dei dettagli standard.](#)

Nella pagina dei dettagli standard, una nuova opzione di download consente di scaricare l'elenco dei controlli in un file.csv. L'elenco scaricato rispetta tutti i filtri presenti nell'elenco. Se hai selezionato un controllo specifico, l'elenco scaricato include solo quel controllo.

26 ottobre 2020

[Integrazioni con i partner nuove e aggiornate](#)

Security Hub è ora integrato con ThreatModeler. Sono state aggiornate le seguenti integrazioni con i partner in modo da rispecchiare i nuovi nomi di prodotto. Twistlock Enterprise Edition è ora Palo Alto Networks - Prisma Cloud Compute. Sempre di Palo Alto Networks, Demisto è ora Cortex XSOAR e Redlock è ora Prisma Cloud Enterprise.

23 ottobre 2020

[Security Hub lanciato in Cina \(Pechino\) e Cina \(Ningxia\)](#)

Security Hub è ora disponibile nelle regioni Cina (Pechino) e Cina (Ningxia).

21 ottobre 2020

[Formato rivisto per gli attributi ASFF e le integrazioni di terze parti](#)

Gli elenchi degli [attributi ASFF](#) e delle [integrazioni dei partner](#) ora utilizzano un formato basato su elenchi anziché su tabelle. La sintassi, gli attributi e la tassonomia dei tipi ASFF sono ora in argomenti separati.

15 ottobre 2020

[Pagina dei dettagli standard riprogettata](#)

La pagina dei dettagli standard per uno standard abilitato ora mostra un elenco a schede di controlli. Le schede filtrano l'elenco di controllo in base allo stato del controllo.

7 ottobre 2020

[CloudWatch Eventi sostituiti con EventBridge](#)

I riferimenti ad Amazon CloudWatch Events sono stati sostituiti con Amazon EventBridge.

1 ottobre 2020

[È stato aggiunto AWS Systems Manager Patch Manager alle integrazioni di servizi disponibili AWS](#)

AWS Systems Manager Patch Manager è ora integrato con Security Hub. Patch Manager invia i risultati a Security Hub quando le istanze del parco macchine di un cliente non sono conformi allo standard di conformità delle patch.

22 settembre 2020

[Sono stati aggiunti nuovi controlli allo standard AWS Foundational Security Best Practices](#)

Sono stati aggiunti nuovi controlli per i seguenti servizi: Amazon EC2 (EC2.7 ed EC2.8), Amazon EMR (EMR.1), IAM (IAM.8), Amazon RDS (da RDS.4 a RDS.8), Amazon S3 (S3.6) e (.1 e .2). AWS Secrets Manager SecretsManager SecretsManager

15 settembre 2020

[Nuove chiavi BatchUpdateFindings contestuali per la policy IAM per controllare l'accesso ai campi](#)

Le policy IAM possono ora essere configurate per limitare l'accesso ai campi e ai valori dei campi durante l'utilizzo di BatchUpdateFindings.

10 settembre 2020

[Accesso esteso agli account BatchUpdateFindings per i membri](#)

Per impostazione predefinita, gli account dei membri ora hanno lo stesso accesso agli account BatchUpdateFindings amministratore.

10 settembre 2020

Nuovi controlli per AWS KMS il Foundational Security Best Practices Standard	Aggiunti due nuovi controlli (KMS.1 e KMS.2) al Foundational Security Best Practices Standard. I nuovi controlli controllano se le politiche IAM limitano l'accesso alle azioni di decrittografia. AWS KMS	9 settembre 2020
Sono stati rimossi i risultati a livello di account per i controlli	Security Hub non genera più risultati a livello di account per un controllo. Vengono generati solo risultati a livello di risorsa.	1 settembre 2020
Nuovo oggetto in ASFF PatchSummary	Aggiunto l'PatchSummary oggetto all'ASFF. L'PatchSummary oggetto fornisce informazioni sulla conformità delle patch di una risorsa rispetto a uno standard di conformità selezionato.	1 settembre 2020
Pagina dei dettagli di controllo riprogettata	La pagina dei dettagli per i controlli è stata riprogettata. L'elenco di ricerca dei controlli fornisce schede che consentono di filtrare rapidamente l'elenco in base allo stato di conformità. È inoltre possibile visualizzare rapidamente i risultati soppressi. Ogni voce fornisce l'accesso a dettagli aggiuntivi sulla risorsa di ricerca, sulla AWS Config regola e sulle note di ricerca.	28 agosto 2020

[Nuove opzioni di filtro per i risultati](#)

Per trovare i filtri, puoi utilizzare il filtro `isnot` per trovare i risultati per i quali il valore di un campo non è uguale al valore del filtro. È possibile utilizzare il comando `non inizia con` per trovare risultati per i quali un valore di campo non inizia con il valore di filtro specificato.

28 agosto 2020

[Nuovi oggetti di dettaglio delle risorse in ASFF](#)

Sono stati aggiunti nuovi `Resources.Details` oggetti per i seguenti tipi di risorse: `AwsDynamoDbTable`, `AwsEc2Eip`, `AwsIamPolicy`, `AwsIamUser`, `AwsRdsDbCluster`, `AwsRdsDbClusterSnapshot`, `AwsRdsDbSnapshot`, `AwsSecretsManagerSecret`

18 agosto 2020

[Nuova integrazione con RSA Archer](#)

Security Hub è ora integrato con RSA Archer. RSA Archer riceve i risultati dal Security Hub.

18 agosto 2020

[Nuovo campo Descrizione per AwsKmsKey](#)

È stato aggiunto un `Description` campo all'`AwsKmsKey` oggetto sottostante `Resources.Details`.

18 agosto 2020

<u>Campi aggiunti a AwsRdsDbInstance</u>	Sono stati aggiunti diversi attributi all'AwsRdsDbInstance oggetto sottostanteResources.Details .	18 agosto 2020
<u>Aggiornato il modo in cui Security Hub determina lo stato generale di un controllo</u>	Per i controlli che non hanno risultati, lo stato è Nessun dato anziché Sconosciuto. Lo stato del controllo include sia i risultati a livello di account che a livello di risorsa. Lo stato del controllo non utilizza lo stato dei risultati del flusso di lavoro, tranne per ignorare i risultati soppressi.	13 agosto 2020
<u>Aggiornato il modo in cui Security Hub calcola il punteggio di sicurezza per uno standard</u>	Quando si calcola il punteggio di sicurezza per uno standard, Security Hub ora ignora i controlli con lo stato Nessun dato. Il punteggio di sicurezza è la proporzione dei controlli passati rispetto ai controlli abilitati, esclusi i controlli senza dati.	13 agosto 2020
<u>Nuova opzione per abilitare automaticamente nuovi controlli negli standard abilitati</u>	È stata aggiunta un'opzione e Impostazioni per abilitare automaticamente i nuovi controlli negli standard abilitati . Puoi anche utilizzare l'operazione UpdateSecurityHubConfiguration API per configurare questa opzione.	31 luglio 2020

<u>Nuovi controlli per lo standard PCI DSS (Payment Card Industry Data Security Standard)</u>	Aggiunti nuovi controlli allo standard PCI DSS. Gli identificatori dei nuovi controlli sono PCI.DMS.1, PCI.EC2.5, PCI.EC2.6, PCI.ELBV2.1, PCI. GuardDuty.1, PCI.IAM.7 , PCI.IAM.8, PCI.S3.5, PCI.S3.6, PCI. SageMaker.1, PCI.SSM.2 e PCI.SSM.3.	29 luglio 2020
<u>Controlli nuovi e aggiornati per lo standard Foundational Security Best Practices</u>	Aggiunti nuovi controlli allo standard Foundational Security Best Practices . Gli identificatori dei nuovi controlli sono AutoScaling .1, DMS.1, EC2.4, EC2.6, S3.5 e SSM.3. È stato aggiornato il titolo di ACM.1 e il valore del parametro è stato modificato in 30. daysToExpiration	29 luglio 2020
<u>Nuovo Vulnerabilities oggetto nell'ASFF</u>	È stato aggiunto l'Vulnerabilities oggetto, che fornisce informazioni sulle vulnerabilità associate alla scoperta.	1 luglio 2020
<u>Nuovi Resource.Details oggetti nei gruppi ASFF for Auto Scaling, nei volumi EC2 e nei VPC EC2</u>	Sono stati aggiunti gli oggettiAwsAutoScalingAutoScalingGroup , AWSEc2Volume e a. AwsEc2Vpc Resource.Details	1 luglio 2020
<u>Nuovo NetworkPath oggetto nell'ASFF</u>	È stato aggiunto l'NetworkPath oggetto, che fornisce informazioni su un percorso di rete correlato al risultato.	1 luglio 2020

[Risolvi automaticamente i risultati quando Compliance.Status è PASSED](#)

Per i risultati dei controlli, in caso Compliance.Status PASSED affermativo, Security Hub viene Workflow. Status impostato automaticamente suRESOLVED.

24 giugno 2020

[AWS Command Line Interface esempi](#)

AWS CLI Sintassi ed esempi aggiunti per diverse attività del Security Hub. Include l'abilitazione di Security Hub, la gestione degli approfondimenti, la gestione degli standard e dei controlli, la gestione delle integrazioni dei prodotti e la disabilitazione di Security Hub.

24 giugno 2020

[Nuovo Severity.Original attributo nell'ASFF](#)

Aggiunto l'attributo Severity.Original che corrisponde alla gravità originale del provider di risultati. Sostituisce l'attributo Severity.Product obsoleto.

20 maggio 2020

[Nuovo Compliance.StatusReasons oggetto nell'ASFF per i dettagli sullo stato di un controllo](#)

Aggiunto l'oggetto Compliance.StatusReasons che fornisce un contesto aggiuntivo per lo stato corrente di un controllo.

20 maggio 2020

[Nuovo standard AWS Foundational Security Best Practices](#)

È stato aggiunto il nuovo standard AWS Foundational Security Best Practices, che è un insieme di controlli che rilevano quando gli account e le risorse distribuiti si discostano dalle migliori pratiche di sicurezza.

22 aprile 2020

[Nuova opzione di console per aggiornare lo stato del flusso di lavoro per una ricerca](#)

Aggiunte informazioni per l'utilizzo della console o dell'API Security Hub per impostare lo stato del flusso di lavoro per i risultati.

16 aprile 2020

[Nuova BatchUpdateFindings API per gli aggiornamenti dei risultati da parte dei clienti](#)

Aggiunte informazioni sull'utilizzo di BatchUpdateFindings per aggiornare e le informazioni relative al processo di indagine di un risultato. BatchUpdateFindings sostituisce UpdateFindings che è obsoleto.

16 aprile 2020

[Aggiornamenti al AWS Security Finding Format \(ASFF\)](#)

Aggiunti diversi nuovi tipi di risorse. Aggiunto un nuovo attributo Label all'oggetto Severity. Label è destinato a sostituire il campo Normalized . Aggiunto un nuovo oggetto Workflow per tracciare il processo di un'indagine su un risultato . Workflow contiene un attributo Status che sostituisce l'attributo Workflows esistente.

12 marzo 2020

[Aggiornamenti alla pagina delle integrazioni](#)

Aggiornato per riflettere le modifiche apportate alla pagina Integrazioni. Per ogni integrazione, la pagina mostra ora la categoria di integrazione e se ogni integrazione invia o riceve i risultati da Security Hub. Fornisce inoltre i passaggi specifici necessari per abilitare ogni integrazione.

26 febbraio 2020

[Nuove integrazioni di prodotti di terze parti](#)

Sono state aggiunte le seguenti nuove integrazioni di prodotto: Cloud Custodian , FireEye Helix, Forcepoint CASB, Forcepoint DLP, Forcepoint NGFW, Rackspace Cloud Native Security e Vectra.ai Cognito Detect.

21 febbraio 2020

Nuovo standard di sicurezza per il Payment Card Industry Data Security Standard (PCI DSS)	È stato aggiunto lo standard di sicurezza Security Hub per il Payment Card Industry Data Security Standard (PCI DSS). Quando questo standard è abilitato, Security Hub esegue controlli automatici rispetto ai controlli relativi ai requisiti PCI DSS.	13 febbraio 2020
Aggiornamenti al AWS Security Finding Format (ASFF)	Aggiunto un campo per i requisiti correlati ai controlli degli standard . Aggiunti nuovi tipi di risorse e nuovi dettagli delle risorse . L'ASFF ora ti permette anche di offrire fino a 32 risorse.	5 febbraio 2020
Nuova opzione per disabilitare i singoli controlli standard di sicurezza	Aggiunte informazioni su come verificare se ogni singolo controllo degli standard di sicurezza è abilitato.	15 gennaio 2020
Aggiornamenti alla terminologia e ai concetti	Aggiornate alcune descrizioni e aggiunti nuovi termini a Concetti e terminologia .	21 settembre 2019
AWS Versione di disponibilità generale di Security Hub	Aggiornamenti dei contenuti per riflettere i miglioramenti apportati a Security Hub durante il periodo di anteprima.	25 giugno 2019
Sono state aggiunte fasi di correzione per i controlli di CIS Foundations AWS	Sono stati aggiunti passaggi di correzione agli standard di sicurezza supportati in AWS Security Hub .	15 aprile 2019

[Versione di anteprima di AWS Security Hub](#)

Publicata la versione di anteprima della AWS Security Hub User Guide.

18 novembre 2018

Le traduzioni sono generate tramite traduzione automatica. In caso di conflitto tra il contenuto di una traduzione e la versione originale in Inglese, quest'ultima prevarrà.