Informazioni di registrazione dell'account AMS Advanced

Guida avanzata all'onboarding AMS

Version February 11, 2026

Copyright © 2026 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Guida avanzata all'onboarding AMS: Informazioni di registrazione dell'account AMS Advanced

Copyright © 2026 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

Introduzione all'onboarding di AWS Managed Services 1
Informazioni su AMS 1
Termini chiave 2
Modalità AMS 8
Modalità e applicazioni o carichi di lavoro AMS 9
Guida prescrittiva AMS post-account 17
Cosa facciamo, cosa non facciamo 17
Gestione del traffico in uscita AMS 18
Ruolo utente IAM 19
MALZ: ruoli utente IAM predefiniti 20
SALZ: ruolo utente IAM predefinito 33
Regole firewall di accesso predefinite 41
Porte di istanze Linux Stack 41
Porte per istanze Windows Stack 42
Gestione di servizi 43
Governance degli account 43
Inizio del servizio 44
Gestione delle relazioni con i clienti (CRM) 44
Processo CRM 45
Riunioni CRM 46
Organizzazione delle riunioni CRM 47
Rapporti mensili CRM 48
Ottimizzazione dei costi 49
Framework di ottimizzazione dei costi 49
Matrice di responsabilità per l'ottimizzazione dei costi 51
Ore di servizio 54
Utilizzo della guida 54
Modifiche alle modalità di gestione 55
Panoramica delle modalità 56
Tipi di modalità e account in AMS 57
Modalità e applicazioni o carichi di lavoro AMS 61
Casi d'uso reali per le modalità AMS 68
modalità RFC 72
Scopri di più RFCs 72

Cosa sono i tipi di modifica? 113
Risoluzione dei problemi relativi agli errori RFC 126
modalità Direct Change 136
Guida introduttiva alla modalità Direct Change 137
Sicurezza e conformità 139
Gestione delle modifiche in modalità Direct Change 144
Creazione di pile utilizzando la modalità Direct Change 146
Casi d'uso della modalità Direct Change 150
modalità Sviluppatore 151
Guida introduttiva alla modalità Sviluppatore 152
Conformità e sicurezza 154
Gestione delle modifiche 156
Provisioning dell'infrastruttura 161
Controlli di rilevamento 162
Registrazione, monitoraggio e gestione degli eventi 162
Gestione degli incidenti 162
Gestione delle patch 163
Gestione della continuità 163
Gestione della sicurezza e degli accessi 163
Modalità Self-Service Provisioning in AMS 164
Guida introduttiva alla modalità SSP in AMS 165
Amazon API Gateway 165
Alexa for Business 166
WorkSpaces Applicazioni Amazon 168
Amazon Athena 171
Amazon Bedrock 172
Amazon CloudSearch 173
Amazon CloudWatch Synthetics 174
Amazon Cognito 175
Amazon Comprehend 177
Amazon Connect 178
Amazon Data Firehose 180
Amazon DevOps Guru 181
Amazon DocumentDB (compatibile con MongoDB) 182
Amazon DynamoDB 183
Amazon Elastic Container Registry 185

EC2 Image Builder 186
Amazon ECS su AWS Fargate 188
Amazon EKS su AWS Fargate 190
Amazon EMR 193
Amazon EventBridge 196
Amazon Forecast 198
Amazon FSx 201
Amazon FSx per OpenZFS 203
Amazon FSx per NetApp ONTAP 204
Amazon Inspector Classic 206
Amazon Kendra 207
Flusso di dati Amazon Kinesis 208
Amazon Kinesis Video Streams 209
Amazon Lex 210
Amazon MQ 210
Servizio gestito da Amazon per Apache Flink 212
Amazon Managed Streaming per Apache Kafka 213
Amazon Managed Service per Prometheus 214
Amazon Personalize 215
Amazon Quick 218
Amazon Rekognition 220
Amazon SageMaker AI 221
Amazon Simple Email Service 224
Amazon Simple Workflow Service 225
Amazon Textract 226
Amazon Transcribe 227
Amazon WorkSpaces 228
Servizi AMS Code 230
AWS Amplify 233
AWS AppSync 234
AWS App Mesh 235
AWS Audit Manager 236
AWS Batch 237
AWS Certificate Manager 239
AWS Autorità di certificazione privata 240
AWS CloudEndure 243

AWS CloudHSM 244
AWS CodeBuild 246
AWS CodeCommit 247
AWS CodeDeploy 249
AWS CodePipeline 250
AWS Compute Optimizer 252
AWS DataSync 253
AWS Device Farm 254
Ripristino di emergenza di elastico di AWS 255
AWS Elemental MediaConvert 257
AWS Elemental MediaLive 257
AWS Elemental MediaPackage 258
AWS Elemental MediaStore 259
AWS Elemental MediaTailor 260
AWS Global Accelerator 261
AWS Glue 262
AWS Lake Formation 264
AWS Lambda 265
AWS License Manager 266
AWS Migration Hub 267
AWS Outposts 268
AWS Resilience Hub 269
Gestione dei segreti AWS 270
AWS Security Hub CSPM 273
AWS Service Catalog AppRegistry 274
AWS Shield 275
AWS Snowball Edge 276
AWS Step Functions 277
AWS Systems Manager Parameter Store 278
Automazione di AWS Systems Manager 280
AWS Transfer Family 283
AWS Transit Gateway 285
AWS WAF 286
AWS Well-Architected Tool 287
AWS X-Ray 287
VM Import/Export 289

Modalità gestita dal cliente 290
Guida introduttiva alla modalità Customer Managed 290
AMS e AWS Service Catalog 291
Guida introduttiva a Service Catalog 291
Service Catalog in AMS prima di iniziare 292
Onboarding con AMS Multi-Account Landing Zone (MALZ) 296
Architettura di rete MALZ 296
Informazioni sull'architettura di rete multi-account landing zone 296
Scelta di MALZ singoli o multipli MALZs 298
Account Multi-Account Landing Zone 303
MALZ: onboarding dell'account principale 327
Crea un AWS account principale per la landing zone con più account 327
Crea un ruolo IAM per AMS per accedere al tuo account 329
Proteggi il nuovo account con l'autenticazione a più fattori (MFA) per l'utente root 330
Iscriviti a Marketplace AWS for EPS 330
Configurazione della rete 331
Configurare la gestione degli accessi 335
MALZ: onboarding dell'account dell'applicazione 340
Richiesta di un nuovo account per l'applicazione 341
Configurazione di Active Directory per federare l'accesso ai ruoli AMS IAM 342
Configurazione della rete con il nuovo account dell'applicazione 345
Configurazione aggiuntiva VPCs nell'account dell'applicazione 347
Appendice: lista di considerazioni relative all'onboarding zone di atterraggio multi-account (MALZ) 347
Configurazione dell'account 348
Avvisi di monitoraggio delle landing zone multi-account AMS 348
Configurazione di rete 349
Configurazione di Active Directory 350
Protezione degli endpoint Trend Micro (EPS) 350
Accesso: Bastions, SSH e RDP 351
Federazione 352
Onboarding con AMS Single Account Landing Zone (SALZ) 353
Procedura di onboarding con AMS SALZ 353
Architettura di rete SALZ 354
Servizi condivisi di landing zone con account singolo AMS 355
SALZ: crea un nuovo AWS account per AMS 356

Crea un Account AWS 356
Configura la fatturazione consolidata: collega il nuovo account all'account Payer 359
Configura il tuo accesso Account AWS per AMS 360
Iscriviti a Marketplace AWS for EPS 362
Abbonati Marketplace AWS a CentOS 7.6 363
Proteggi il nuovo account con l'autenticazione a più fattori (MFA) per l'utente root 363
SALZ: configura la rete 364
Alloca lo spazio IP per il tuo ambiente AMS 364
Stabilisci la connettività di rete privata con AWS 365
Configura il tuo firewall 366
Opzioni AMS Bastion durante le migrazioni e l'onboarding delle applicazioni 367
SALZ: configura la gestione degli accessi 368
Stabilire un trust Active Directory (AD) 369
Federa il tuo Active Directory con i ruoli AMS AWS Identity and Access Management 374
SALZ: impostazioni predefinite 380
Sicurezza degli endpoint (EPS) 380
Gruppi di sicurezza 385
EC2 Profilo dell'istanza IAM 390
Impostazioni predefinite delle metriche monitorate 398
Impostazioni predefinite di conservazione e rotazione dei log 415
Impostazioni predefinite per la gestione della continuità 416
Impostazioni predefinite per l'applicazione delle patch 417
Convalida il servizio AMS (SALZ) 419
Trova le impostazioni dell'account 419
Ricerca di un ID di istanza o di un indirizzo IP 423
Nomi bastioni compatibili con DNS 425
Individuazione degli indirizzi IP di Bastion 427
Istanze EC2: creazione 428
Accesso, richiesta 437
Altro | Altro RFC, creazione (CLI) 444
Qualsiasi pila: eliminazione, riavvio, avvio, arresto 446
Esempi di accesso 458
Segnalazione di un incidente 468
Creazione di una richiesta di assistenza 471
Fasi successive all'onboarding 474
Tutorial 474

Appendice: Questionario di onboarding SALZ 501
Riepilogo della distribuzione 501
Considerazioni sull'architettura dell'ambiente 502
Avvisi di monitoraggio della zona di atterraggio con account singolo 503
Finestra di manutenzione 503
Fasi successive 503
Appendice: Regola di reclamo di ActiveDirectory Federation Services (ADFS) e impostazioni SAML 505
Configurazioni delle regole di reclamo ADFS 505
Console Web 506
Accesso a API e CLI con SAML 506
Configurazione dello script 506
Configurazione di Windows 506
Configurazione Linux 509
Cronologia dei documenti 510
..... dxiii

Introduzione all'onboarding di AWS Managed Services

Benvenuto in AWS Managed Services (AMS). AMS è un servizio aziendale che fornisce la gestione continua dell'infrastruttura AWS. Questa guida è progettata per aiutarti a iniziare a utilizzare AMS, incluso come configurare un nuovo account per AMS, configurare la rete e l'accesso ad AMS e convalidare la configurazione di onboarding.

È destinato agli amministratori IT incaricati di preparare ed eseguire le attività necessarie per l'onboarding del servizio AMS su un nuovo account AWS. L'onboarding del servizio AMS richiede privilegi speciali per configurare i trust di Active Directory e completare altre attività a livello di rete. Per ricevere assistenza nella decisione se utilizzare account di landing zone con più account o account di landing zone con account singolo, visita Scegliere un MALZ singolo o multiplo. MALZs

> **Important**
>
> Dopo questa introduzione, questa guida è divisa in due parti: una per gli account di landing zone con più account e una per gli account di landing zone con account singolo. L'onboarding è molto diverso per le due situazioni, vai accanto alla sezione della guida che si riferisce alla tua situazione.

Argomenti

- Informazioni su AMS
- Termini chiave AMS
- Modalità AMS
- Guida prescrittiva AMS post-account
- Cosa facciamo, cosa non facciamo
- Gestione del traffico in uscita AMS
- Ruolo utente IAM in AMS
- Regole firewall di accesso predefinite

Informazioni su AMS

Per comprendere meglio AMS, consulta queste sezioni della Guida per l'utente AMS:

- What Is AWS Managed Services introduce il servizio AMS e descrive le caratteristiche, le operazioni e le interfacce principali, nonché una tipica architettura di rete gestita da AMS. Questo capitolo fornisce anche informazioni sulla gestione degli accessi, incluso come accedere alle risorse gestite da AMS e utilizzare i bastioni.
- Key Terms fornisce definizioni e spiegazioni per la terminologia AMS.
- Understanding AMS Defaults fornisce i valori predefiniti utilizzati da AMS, inclusi i valori predefiniti per i componenti di base dell'ambiente, IAM e i proxy, le metriche monitorate EC2, la registrazione, la sicurezza degli endpoint (EPS), i backup e l'applicazione di patch.
- Change Management fornisce dettagli su come funzionano le richieste di change () e change types (RFCs) e include esempi di utilizzo di AMS. CTs RFCs
- Diversi capitoli aggiuntivi riguardano l'accesso alla console AWS, l'AMS CLI, l'utilizzo del sistema di gestione delle modifiche AMS, AMS SKMS, la sicurezza, le richieste di servizio, gli incidenti, il monitoraggio, i log, l'EPS, i backup e la gestione delle patch.

Per saperne di più sull'architettura delle landing zone multi-account AMS, consulta Architettura di rete Multi-Account Landing Zone

Per saperne di più sull'architettura della landing zone a account singolo di AMS, consulta Architettura di rete Single-Account Landing Zone

Termini chiave AMS

- AMS Advanced: i servizi descritti nella sezione «Descrizione del servizio» della documentazione di AMS Advanced. Vedi Descrizione del servizio.
- Account AMS Advanced: AWS account che soddisfano sempre tutti i requisiti degli AMS Advanced Onboarding Requirements. Per informazioni sui vantaggi di AMS Advanced, sui case study e per contattare un addetto alle vendite, consulta AWS Managed Services.
- Account AMS Accelerate: AWS account che soddisfano in ogni momento tutti i requisiti degli AMS Accelerate Onboarding Requirements. Vedi Guida introduttiva ad AMS Accelerate.
- AWS Managed Services: AMS e/o AMS Accelerate.
- Account AWS Managed Services: gli account AMS e/o gli account AMS Accelerate.
- Raccomandazione critica: una raccomandazione emessa AWS tramite una richiesta di servizio che informa l'utente che è necessario intervenire per proteggersi da potenziali rischi o interruzioni delle risorse o del. Servizi AWS Se decidi di non seguire una raccomandazione critica entro la data specificata, sei l'unico responsabile di eventuali danni derivanti dalla tua decisione.

- Configurazione richiesta dal cliente: qualsiasi software, servizio o altra configurazione non identificata in:
  - Accelerazione: configurazioni supportate o AMS Accelerate; descrizione del servizio.
  - AMS Advanced: configurazioni supportate o AMS Advanced; descrizione del servizio.
- Comunicazione di un incidente: AMS comunica un Incidente all'utente o l'utente richiede un Incidente ad AMS tramite un Incidente creato nel Support Center for AMS Accelerate e nella console AMS per AMS. La console AMS Accelerate fornisce un riepilogo degli incidenti e delle richieste di assistenza sulla dashboard e collegamenti al Support Center per i dettagli.
- Ambiente gestito: gli account AMS Advanced e/o gli account AMS Accelerate gestiti da AMS.

  Per AMS Advanced, questi includono account multi-account landing zone (MALZ) e account single-account landing zone (SALZ).
- Data di inizio della fatturazione: il giorno lavorativo successivo alla AWS ricezione delle informazioni richieste nell'e-mail di onboarding di AWS Managed Services. L'e-mail di onboarding di AWS Managed Services si riferisce AWS all'e-mail inviata dall'utente per raccogliere le informazioni necessarie per attivare AWS Managed Services sui propri account.

  Per gli account registrati successivamente da te, la data di inizio della fatturazione è il giorno successivo all'invio da parte di AWS Managed Services di una notifica di attivazione di AWS Managed Services per l'account registrato. Una notifica di attivazione di AWS Managed Services si verifica quando:

  1. Concedi l'accesso a un AWS account compatibile e lo consegni a AWS Managed Services.
  2. AWS Managed Services progetta e crea l'account AWS Managed Services.
- Interruzione del servizio: puoi chiudere AWS Managed Services per tutti gli account AWS Managed Services o per uno specifico account AWS Managed Services per qualsiasi motivo fornendo un preavviso di AWS almeno 30 giorni tramite una richiesta di servizio. Alla data di cessazione del servizio, puoi:

  1. AWS ti cede i controlli di tutti gli account AWS Managed Services o degli account AWS Managed Services specificati, a seconda dei casi, oppure
  2. Le parti rimuovono i AWS Identity and Access Management ruoli che consentono AWS l'accesso da tutti gli account AWS Managed Services o dagli account AWS Managed Services specificati, a seconda dei casi.
- Data di cessazione del servizio: la data di cessazione del servizio è l'ultimo giorno del mese di calendario successivo alla fine del periodo di preavviso di cessazione richiesto di 30 giorni. Se la fine del periodo di disdetta richiesto cade dopo il ventesimo giorno del mese solare, la data

di cessazione del servizio è l'ultimo giorno del mese di calendario successivo. Di seguito sono riportati alcuni esempi di scenari relativi alle date di cessazione.

  - Se l'avviso di risoluzione viene fornito il 12 aprile, il preavviso di 30 giorni termina il 12 maggio. La data di cessazione del servizio è il 31 maggio.
  - Se viene fornito un avviso di risoluzione il 29 aprile, il preavviso di 30 giorni termina il 29 maggio. La data di cessazione del servizio è il 30 giugno.
- Fornitura di AWS Managed Services: ti AWS mette a disposizione e puoi accedere e utilizzare AWS Managed Services per ogni account AWS Managed Services a partire dalla data di inizio del servizio.
- Chiusura per determinati account AWS Managed Services: puoi chiudere AWS Managed Services per uno specifico account AWS Managed Services per qualsiasi motivo fornendo un AWS preavviso tramite una richiesta di servizio («Richiesta di terminazione dell'account AMS»).

Termini di gestione degli incidenti:

- Evento: un cambiamento nell'ambiente AMS.
- Avviso: ogni volta che un evento di un Servizio AWS operatore supportato supera una soglia e attiva un allarme, viene creato un avviso e viene inviato un avviso all'elenco dei contatti. Inoltre, viene creato un incidente nell'elenco degli incidenti.
- Incidente: un'interruzione o un peggioramento non pianificato delle prestazioni dell'ambiente AMS o di AWS Managed Services che provoca un impatto come riportato da AWS Managed Services o da te.
- Problema: causa principale condivisa di uno o più incidenti.
- Risoluzione di un incidente o risoluzione di un incidente:
  - AMS ha ripristinato tutti i servizi o le risorse AMS non disponibili relativi all'incidente riportandoli allo stato disponibile, oppure
  - AMS ha stabilito che gli stack o le risorse non disponibili non possono essere ripristinati allo stato disponibile, oppure
  - AMS ha avviato un ripristino dell'infrastruttura autorizzato dall'utente.
- Tempo di risposta agli incidenti: la differenza di tempo tra il momento in cui si crea un incidente e il momento in cui AMS fornisce una risposta iniziale tramite console, e-mail, centro di assistenza o telefono.
- Tempo di risoluzione dell'incidente: la differenza di tempo tra il momento in cui AMS o l'utente creano un incidente e il momento in cui l'incidente viene risolto.

- Priorità dell'incidente: in che modo AMS o l'utente assegna la priorità agli incidenti, definendoli come bassa, media o alta.
  - Bassa: un problema non critico del servizio AMS.
  - Medio: un servizio AWS all'interno dell'ambiente gestito è disponibile ma non funziona come previsto (secondo la descrizione del servizio applicabile).
  - Alto: (1) la console AMS o uno o più AMS APIs nell'ambiente gestito non sono disponibili; oppure (2) uno o più stack o risorse AMS all'interno dell'ambiente gestito non sono disponibili e l'indisponibilità impedisce all'applicazione di svolgere la propria funzione.

  AMS può riclassificare gli incidenti in base alle linee guida di cui sopra.
- Ripristino dell'infrastruttura: ridistribuzione degli stack esistenti, sulla base di modelli degli stack interessati, e avvio di un ripristino dei dati basato sull'ultimo punto di ripristino noto, se non diversamente specificato dall'utente, quando la risoluzione degli incidenti non è possibile.

Termini relativi all'infrastruttura:

- Ambiente di produzione gestito: un account cliente in cui risiedono le applicazioni di produzione del cliente.
- Ambiente non di produzione gestito: un account cliente che contiene solo applicazioni non di produzione, come applicazioni per lo sviluppo e il test.
- Stack AMS: un gruppo di una o più AWS risorse gestite da AMS come singola unità.
- Infrastruttura immutabile: un modello di manutenzione dell'infrastruttura tipico EC2 dei gruppi Amazon Auto Scaling ASGs () in cui i componenti dell'infrastruttura aggiornati (ad AWS esempio l'AMI) vengono sostituiti per ogni implementazione, anziché essere aggiornati sul posto. Il vantaggio dell'infrastruttura immutabile è che tutti i componenti rimangono in uno stato sincrono poiché vengono sempre generati dalla stessa base. L'immutabilità è indipendente da qualsiasi strumento o flusso di lavoro per la creazione dell'AMI.
- Infrastruttura mutabile: un modello di manutenzione dell'infrastruttura tipico per gli stack che non sono gruppi di Amazon EC2 Auto Scaling e contengono una singola istanza o solo poche istanze. Questo modello rappresenta più da vicino l'implementazione di sistema tradizionale, basata su hardware, in cui un sistema viene distribuito all'inizio del suo ciclo di vita e poi gli aggiornamenti vengono distribuiti su quel sistema nel tempo. Tutti gli aggiornamenti del sistema vengono applicati alle istanze singolarmente e possono comportare tempi di inattività del sistema (a seconda della configurazione dello stack) a causa del riavvio dell'applicazione o del sistema.

- Gruppi di sicurezza: firewall virtuali per l'istanza per controllare il traffico in entrata e in uscita. I gruppi di sicurezza operano a livello di istanza, non di sottorete. Pertanto, a ciascuna istanza di una sottorete del VPC potrebbe essere assegnato un set diverso di gruppi di sicurezza.
- Accordi sul livello di servizio (SLAs): parte dei contratti AMS con voi che definiscono il livello di servizio previsto.
- SLA non disponibile e indisponibilità:
  - Una richiesta API da te inviata che genera un errore.
  - Una richiesta di console inviata da te che genera una risposta HTTP 5xx (il server non è in grado di eseguire la richiesta).
  - Tutte Servizio AWS le offerte che costituiscono stack o risorse nell'infrastruttura gestita da AMS si trovano in uno stato di «interruzione del servizio», come indicato nella Service Health Dashboard.
  - L'indisponibilità derivante direttamente o indirettamente da un'esclusione di AMS non viene considerata nel determinare l'idoneità ai crediti di servizio. I servizi sono considerati disponibili a meno che non soddisfino i criteri per l'indisponibilità.
- Obiettivi del livello di servizio (SLOs): parte dei contratti AMS con l'utente che definiscono obiettivi di servizio specifici per i servizi AMS.

Termini di applicazione delle patch:

- Patch obbligatorie: aggiornamenti di sicurezza critici per risolvere problemi che potrebbero compromettere lo stato di sicurezza dell'ambiente o dell'account. Un «aggiornamento critico di sicurezza» è un aggiornamento di sicurezza classificato come «Critico» dal fornitore di un sistema operativo supportato da AMS.
- Patch annunciate o rilasciate: le patch vengono generalmente annunciate e rilasciate in base a una pianificazione. Le patch emergenti vengono annunciate quando viene scoperta la necessità della patch e, di solito, subito dopo, la patch viene rilasciata.
- Patch add-on: applicazione di patch basata su tag per le istanze AMS che sfrutta la funzionalità AWS Systems Manager (SSM) in modo da poter etichettare le istanze e applicare le patch a tali istanze utilizzando una linea di base e una finestra configurate dall'utente.
- Metodi di patch:
  - Patch sul posto: applicazione di patch che viene eseguita modificando le istanze esistenti.
  - Patch sostitutiva dell'AMI: patch che viene eseguita modificando il parametro di riferimento AMI di una configurazione di avvio del gruppo Auto EC2 Scaling esistente.

- Fornitore di patch (fornitori di sistemi operativi, terze parti): le patch vengono fornite dal fornitore o dall'organo direttivo dell'applicazione.
- Tipi di patch:
  - Aggiornamento critico di sicurezza (CSU): aggiornamento di sicurezza classificato come «critico» dal fornitore di un sistema operativo supportato.
  - Aggiornamento importante (UI): un aggiornamento di sicurezza classificato come «Importante» o un aggiornamento non relativo alla sicurezza classificato come «Critico» dal fornitore di un sistema operativo supportato.
  - Altro aggiornamento (OU): un aggiornamento del fornitore di un sistema operativo supportato che non è una CSU o un'interfaccia utente.
- Patch supportate: AMS supporta le patch a livello di sistema operativo. Gli aggiornamenti vengono rilasciati dal fornitore per correggere vulnerabilità di sicurezza o altri bug o per migliorare le prestazioni. Per un elenco delle configurazioni attualmente supportate OSs, consulta Support Configurations.

Termini di sicurezza:

- Detective Controls: una libreria di monitor creati o abilitati da AMS che forniscono una supervisione continua degli ambienti e dei carichi di lavoro gestiti dai clienti per configurazioni che non sono in linea con i controlli di sicurezza, operativi o dei clienti e intervengono informando i proprietari, modificando in modo proattivo o interrompendo le risorse.

Termini della richiesta di assistenza:

- Richiesta di assistenza: una richiesta da parte tua relativa a un'azione che desideri che AMS intraprenda per tuo conto.
- Notifica di avviso: avviso pubblicato da AMS nella pagina di elenco delle richieste di assistenza quando viene attivato un avviso AMS. Il contatto configurato per il tuo account viene inoltre avvisato tramite il metodo configurato (ad esempio, e-mail). Se hai dei tag di contatto sulle tue istanze/risorse e hai fornito il consenso al tuo cloud service delivery manager (CSDM) per le notifiche basate su tag, le informazioni di contatto (valore chiave) contenute nel tag vengono notificate anche per gli avvisi AMS automatici.
- Notifica di servizio: un avviso di AMS che viene pubblicato nella pagina dell'elenco delle richieste di assistenza.

Termini vari:

- Interfaccia AWS Managed Services: per AMS: la console AWS Managed Services Advanced, l'API AMS CM e Supporto l'API. Per AMS Accelerate: la Supporto console e Supporto l'API.
- Soddisfazione del cliente (CSAT): AMS CSAT viene informata con analisi approfondite, tra cui le valutazioni della corrispondenza dei casi su ogni caso o corrispondenza, sondaggi trimestrali e così via.
- DevOps: DevOps è una metodologia di sviluppo che promuove fortemente l'automazione e il monitoraggio in tutte le fasi. DevOps mira a cicli di sviluppo più brevi, a una maggiore frequenza di implementazione e a rilasci più affidabili, riunendo le funzioni di sviluppo e operazioni, tradizionalmente separate, su una base di automazione. Quando gli sviluppatori possono gestire le operazioni e le operazioni informano lo sviluppo, problemi e problemi vengono scoperti e risolti più rapidamente e gli obiettivi aziendali vengono raggiunti più rapidamente.
- ITIL: Information Technology Infrastructure Library (denominata ITIL) è un framework ITSM progettato per standardizzare il ciclo di vita dei servizi IT. ITIL è organizzato in cinque fasi che coprono il ciclo di vita dei servizi IT: strategia del servizio, progettazione del servizio, transizione del servizio, funzionamento del servizio e miglioramento del servizio.
- Gestione dei servizi IT (ITSM): un insieme di pratiche che allineano i servizi IT alle esigenze dell'azienda.
- Managed Monitoring Services (MMS): AMS gestisce il proprio sistema di monitoraggio, Managed Monitoring Service (MMS), che utilizza gli eventi AWS Health e aggrega i dati di CloudWatch Amazon e i dati di Servizi AWS altri, notificando agli operatori AMS (online 24 ore su 24, 7 giorni su 7) qualsiasi allarme creato tramite un argomento di Amazon Simple Notification Service (Amazon SNS).
- Namespace: quando crei policy IAM o lavori con Amazon Resource Names (ARNs), identifichi un utente Servizio AWS utilizzando uno spazio dei nomi. È possibile utilizzare gli spazi dei nomi quando si identificano azioni e risorse.

Modalità AMS

Utilizzalo per aiutarti a selezionare la modalità AWS Managed Services (AMS) appropriata per ospitare le tue applicazioni, in base alla combinazione desiderata di flessibilità e governance prescrittiva per raggiungere i tuoi risultati di business.

Il pubblico a cui sono destinate queste informazioni è:

- Team clienti responsabili della strategia e della governance delle rispettive landing zone. Queste informazioni aiuteranno il team a gettare le basi di una landing zone gestita da AMS, con le modalità AMS che vorrebbe offrire ai propri clienti interni ed esterni.
- Proprietari di aziende e applicazioni incaricati di migrare la propria applicazione su AMS. Queste informazioni aiuteranno a pianificare la migrazione delle applicazioni, con la modalità AMS appropriata alla migrate/host loro applicazione. Nota, la stessa applicazione può essere ospitata in più di una modalità AMS durante diverse fasi del ciclo di vita del Software Development Life Cycle (SDLC).
- I partner AMS hanno il compito di guidare i clienti sulle diverse opzioni di creazione e migrazione ad AMS.

Queste informazioni presuppongono che tu abbia già deciso di sfruttare AMS per accelerare il tuo percorso verso il cloud. Fai riferimento a questo paper in due momenti del tuo percorso di migrazione al cloud: in primo luogo, durante la fase di base della configurazione della piattaforma gestita da AMS. In secondo luogo, quando state passando dalla fase di base a quella di migrazione del vostro percorso di adozione del cloud, subito dopo il completamento dell'onboarding verso AMS vi state concentrando sulla governance e sulle operazioni delle applicazioni.

Modalità e applicazioni o carichi di lavoro AMS

Considerate i requisiti operativi e di governance per le vostre applicazioni quando scegliete la modalità giusta, richiedendo un nuovo account applicativo o ospitando l'applicazione in un account applicativo esistente. La scelta della modalità AMS appropriata per ogni applicazione o carico di lavoro dipende dai seguenti fattori:

- Il tipo di funzione del ciclo di vita SDLC che l'ambiente fornirà (ad esempio, sandbox con modifiche non moderate, UAT con alcune modifiche frequenti, produzione con modifiche minime e altamente regolamentata)
- Le politiche di governance necessarie (applicate a livello di unità organizzativa) SCPs
- Modello operativo (se desideri assumere la responsabilità operativa o desideri esternalizzarla ad AMS)
- I risultati aziendali desiderati, come il tempo impiegato per operare nel cloud e il costo delle operazioni.

> **Note**
>
> Per una descrizione dei tipi di modalità per servizio AMS, consulta Tipi di modalità e account in AMS.
> Per i casi d'uso reali delle diverse modalità, consulta Casi d'uso nel mondo reale per le modalità AMS

La tabella seguente riporta le considerazioni chiave per i proprietari delle applicazioni per aiutarli a decidere la modalità AMS più adatta. I proprietari delle applicazioni dovrebbero includere una fase di valutazione prima della migrazione delle applicazioni per comprendere appieno quale modalità si applica alla loro applicazione specifica. Esempio: per le applicazioni basate su servizi nativi del cloud o su un'architettura serverless, l'opzione migliore potrebbe essere iniziare a creare e iterare in modalità sviluppatore e implementare l'infrastruttura come codice finale utilizzando la modalità AMS Managed — SSP. In questo caso può essere necessario un leggero rifattorizzazione per garantire che tutti i CloudFormation modelli creati per l'implementazione automatizzata soddisfino le linee guida di acquisizione stabilite da AMS. Inoltre, tutte le autorizzazioni IAM devono essere approvate da AMS Security per garantire che seguano il modello con privilegi minimi.

La modalità AMS selezionata per ospitare l'applicazione può aiutarvi a sviluppare il modello operativo cloud desiderato.

> **Note**
>
> In una singola AMS Managed Landing Zone possono esistere più modelli operativi cloud in base alle diverse modalità AMS selezionate per ospitare le applicazioni.

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
Prontezza operativa						
Registrazione, monitorag	AMS è responsabile di tutte le infrastrutture gestite			Cliente responsabile dei Self-	Cliente responsabile del	Responsabile del cliente

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
gio e gestione degli eventi				Service Provision ed Services (SSP)	provisioning delle risorse utilizzando il ruolo di sviluppatore IAM esterno al sistema AMS CM	
Gestione della continuità	Responsabilità di AMS di eseguire il piano di backup selezionato dal cliente			Cliente responsab ile dei Self-Service Provision ed Services (SSP)	Cliente responsab ile del provisioning delle risorse utilizzando il ruolo di sviluppatore IAM esterno al sistema AMS CM	
Gestione degli accessi a livello di istanza	Gestione AMS tramite AD trust unidirezionale con dominio locale. Richiede un'infrastruttura gestita per entrare a far parte del dominio AMS			Non applicabile	Cliente responsab ile del provisioning delle risorse utilizzando il ruolo di sviluppatore IAM esterno al sistema AMS CM	

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
Gestione della sicurezza e gestione degli accessi a livello di account	Responsabilità di AMS per tutti gli account gestiti			AMS è responsabile di tutti gli account gestiti	Cliente responsabile delle risorse fornite utilizzando il ruolo di sviluppatore IAM esterno al sistema AMS CM	
Gestione delle patch	Responsabilità di AMS per tutti gli account gestiti			Cliente responsabile dei Self-Service Provisioned Services (SSP)	Cliente responsabile del provisioning delle risorse utilizzando il ruolo di sviluppatore IAM esterno al sistema AMS CM	

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
Gestione delle modifiche	Responsabilità di AMS per tutti gli account gestiti			Cliente responsabile dei Self-Service Provisioned Services (SSP)	Cliente responsabile del provisioning delle risorse utilizzando il ruolo di sviluppatore IAM esterno al sistema AMS CM	
Gestione del provisioning	Prescrittiva e standardizzata per le opzioni di approvvigionamento offerte in AMS	Flessibilità di utilizzare direttamente l'API di servizio AWS per AWS Service Catalog secondo gli standard prescrittivi AMS	Flessibilità per utilizzare direttamente l'API dei servizi AWS secondo gli standard prescrittivi AMS	Flessibilità di utilizzare direttamente il servizio AWS APIs per i servizi SSP	Flessibilità di utilizzare direttamente l'API dei servizi AWS per il provisioning	

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
Gestione e audit degli incidenti	AMS è responsabile di tutti gli account gestiti				Cliente responsabile delle risorse fornite utilizzando il ruolo di sviluppatore IAM esterno ad AMS Change Management System	
GuardRails e infrastruttura condivisa (rete) e framework di sicurezza	Prescrittivo e standardizzato che sfrutta gli account AMS Core					Flessibile e personalizzato che sfrutta gli account AMS Core
Prontezza delle applicazioni						

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
Rifattorizzazione delle applicazioni	È necessaria una leggera rifattorizzazione				È necessaria a una leggera rifattorizzazione (se fornita utilizzando AMS Standard CM)	Non è necessario il refactoring
Support per i servizi AWS	Limitato a quanto supportato da AMS					Non limitato
Considerazioni aziendali						
È ora di essere pronti all'operatività	Da tre a sei mesi			Oltre 6 mesi a seconda delle competenze operative delle applicazioni del cliente		6-18 mesi a seconda dell'infrastruttura del cliente e delle competenze operative delle applicazioni
Costi	$$$$			$$$	$$	$

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
Esempi di applicazione	Server Web con stack a 3 livelli, app con requisiti di conformità e normativi			Server Web che utilizza API Gateway, applicazione containerizzata che sfrutta ECS/ EKS	Iterazione/ottimizzazione su un'applicazione Data Lake che utilizza Lambda, Glue, Athena, ecc.	Applicazioni decentralizzate accounts/ applications come sandbox, gestite da terze parti

* Operations On Demand (OOD) offre un'offerta ai clienti che utilizzano la modalità CM Standard per gestire le modifiche tramite risorse dedicate. Per ulteriori dettagli, consultate il catalogo di offerte di Operations on Demand e contattate il vostro cloud service delivery manager (CSDM).

> **Note**
>
> Il confronto dei prezzi tra la modalità SSP e la modalità Developer presuppone che vengano forniti gli stessi servizi AWS.

Confronto delle modalità AMS con gli obiettivi aziendali e IT

Come mostrato, se stai cercando un modello di governance altamente controllato e standardizzato per le tue applicazioni, le modalità Standard Change gestite da AMS, AWS Service Catalog o Direct Change sono la soluzione migliore. Se hai bisogno di un modello di governance personalizzato incentrato sull'innovazione delle applicazioni senza la necessità di una prontezza operativa, seleziona la modalità Customer Managed. Con la modalità Customer Managed, potrebbe essere necessario più tempo per rendere operative le applicazioni, in quanto spetta a te definire persone, processi e

strumenti per supportare funzionalità operative come la gestione degli incidenti, la gestione della configurazione, la gestione del provisioning, la gestione della sicurezza, la gestione delle patch, ecc.

Guida prescrittiva AMS post-account

Poiché le organizzazioni adottano operazioni e DevOps pratiche distribuite, esistono una serie di funzionalità operative di base che devono essere applicate a ogni account prima dell'implementazione dei carichi di lavoro per soddisfare i pilastri di Well Architected.

Questo collegamento consente di scaricare un file ZIP contenente un documento Word e un file ZIP con script ed esempi. La configurazione automatica dell'account è un insieme di script per automatizzare, o avviare, la configurazione di un nuovo account dell'applicazione.

Una volta venduto un nuovo account e prima dell'implementazione dei carichi di lavoro, per rendere l'account pronto dal punto di vista operativo, di sicurezza e di gestione, si configurano piani di backup predefiniti, finestre di patch e crittografia (e altro ancora). Per contribuire a migliorare l'agilità, la coerenza e la reattività della configurazione degli account applicativi, viene fornito il seguente esempio di «How To» come riferimento.

Configurazione automatica dell'account.

Cosa facciamo, cosa non facciamo

AMS offre un approccio standardizzato all'implementazione dell'infrastruttura AWS e fornisce la necessaria gestione operativa continua. Per una descrizione completa dei ruoli, delle responsabilità e dei servizi supportati, consulta Descrizione del servizio.

> **Note**
>
> Per richiedere che AMS fornisca un servizio AWS aggiuntivo, invia una richiesta di servizio. Per ulteriori informazioni, consulta Making Service Requests.

- Cosa facciamo:

  Dopo aver completato l'onboarding, l'ambiente AMS è disponibile per ricevere richieste di modifica (RFCs), incidenti e richieste di assistenza. L'interazione con il servizio AMS ruota attorno al ciclo di vita di uno stack di applicazioni. I nuovi stack vengono ordinati da un elenco preconfigurato di modelli, lanciati in specifiche sottoreti di cloud privato virtuale (VPC), modificati durante la loro vita

operativa tramite request for change (RFCs) e monitorati per eventi e incidenti 24 ore su 24, 7 giorni su 7.

Gli stack di applicazioni attivi sono monitorati e mantenuti da AMS, comprese le patch, e non richiedono ulteriori azioni per tutta la durata dello stack, a meno che non sia necessaria una modifica o lo stack non venga smantellato. Gli incidenti rilevati da AMS che influiscono sullo stato e sul funzionamento dello stack generano una notifica e possono richiedere o meno l'intervento dell'utente per risolverli o verificarli. È possibile porre domande pratiche e altre richieste inviando una richiesta di assistenza.

Inoltre, AMS consente di abilitare servizi AWS compatibili che non sono gestiti da AMS. Per informazioni sui servizi compatibili con AWS-AMS, consulta Modalità di provisioning self-service.

- Cosa NON facciamo:

  Sebbene AMS semplifica l'implementazione delle applicazioni fornendo una serie di opzioni manuali e automatizzate, sei responsabile dello sviluppo, del test, dell'aggiornamento e della gestione della tua applicazione. AMS fornisce assistenza per la risoluzione dei problemi di infrastruttura che influiscono sulle applicazioni, ma AMS non può accedere o convalidare le configurazioni delle applicazioni.

Gestione del traffico in uscita AMS

Per impostazione predefinita, la route con un CIDR di destinazione di 0.0.0.0/0 per le sottoreti AMS private e per le applicazioni personalizzate ha come destinazione un gateway NAT (Network Address Translation). I servizi AMS TrendMicro e l'applicazione delle patch sono componenti che devono disporre dell'accesso in uscita a Internet in modo che AMS sia in grado di fornire il proprio servizio e che i sistemi operativi possano ottenere aggiornamenti. TrendMicro

AMS supporta la deviazione del traffico in uscita verso Internet tramite un dispositivo di uscita gestito dal cliente a condizione che:

- Funziona come un proxy implicito (ad esempio trasparente).

  e

- Consente le dipendenze HTTP e HTTPS di AMS (elencate in questa sezione) per consentire l'applicazione di patch e la manutenzione continui dell'infrastruttura gestita da AMS.

Alcuni esempi sono:

- Il gateway di transito (TGW) ha una route predefinita che punta al firewall locale gestito dal cliente tramite la connessione AWS Direct Connect nell'account Multi-Account Landing Zone Networking.
- Il TGW ha una route predefinita che punta a un endpoint AWS nel Multi-Account Landing Zone egress VPC che sfrutta AWS PrivateLink, puntando a un proxy gestito dal cliente in un altro account AWS.
- Il TGW ha un percorso predefinito che punta a un firewall gestito dal cliente in un altro account AWS, con una connessione site-to-site VPN come allegato alla Multi-Account Landing Zone TGW.

AMS ha identificato le dipendenze AMS HTTP e HTTPS corrispondenti e sviluppa e perfeziona queste dipendenze su base continuativa. Vedi egressMgmt.zip. Oltre al file JSON, lo ZIP contiene un file README.

> **Note**
>
> - Queste informazioni non sono complete: alcuni siti esterni obbligatori non sono elencati qui.
> - Non utilizzare questo elenco nell'ambito di una lista negata o di una strategia di blocco.
> - Questo elenco è inteso come punto di partenza per un set di regole di filtraggio delle uscite, con l'aspettativa che vengano utilizzati strumenti di reporting per determinare con precisione dove il traffico effettivo diverge dall'elenco.

Per richiedere informazioni sul filtraggio del traffico in uscita, inviate un'e-mail al vostro CSDM: ams-csdm@amazon.com.

Ruolo utente IAM in AMS

Un ruolo IAM è simile a quello di un utente IAM, in quanto è un' AWS identità con politiche di autorizzazione che determinano ciò che l'identità può e non può fare AWS. Tuttavia, invece di essere associato in modo univoco a una persona, un ruolo è destinato a essere assunto da chiunque.

Attualmente esiste un ruolo utente AMS predefinito`Customer_ReadOnly_Role`, per gli account AMS standard e un ruolo aggiuntivo, `customer_managed_ad_user_role` per gli account AMS con Managed Active Directory.

Le politiche di ruolo stabiliscono le autorizzazioni CloudWatch e le azioni di registro di Amazon S3, l'accesso alla console AMS, le restrizioni di sola lettura per la Servizi AWS maggior parte, l'accesso limitato alla console S3 dell'account e l'accesso al tipo di modifica AMS.

Inoltre, `Customer_ReadOnly_Role` dispone di autorizzazioni mutative per le istanze riservate che consentono di prenotare le istanze. Ha alcuni vantaggi in termini di risparmio, quindi, se sai che avrai bisogno di un certo numero di istanze Amazon EC2 per un lungo periodo di tempo, puoi chiamarle. APIs Per ulteriori informazioni, consulta la pagina Istanze riservate di Amazon EC2.

> **Note**
>
> L'obiettivo del livello di servizio (SLO) di AMS per la creazione di policy IAM personalizzate per gli utenti IAM è di quattro giorni lavorativi, a meno che non si voglia riutilizzare una policy esistente. Se desideri modificare il ruolo utente IAM esistente o aggiungerne uno nuovo, invia rispettivamente una RFC IAM: Update Entity o IAM: Create Entity.

Se non conosci i ruoli Amazon IAM, consulta Ruoli IAM per informazioni importanti.

Multi-Account Landing Zone (MALZ): per visualizzare le politiche relative ai ruoli utente predefinite e non personalizzate di AMS per i ruoli utente, vedere, successivo. MALZ: ruoli utente IAM predefiniti

MALZ: ruoli utente IAM predefiniti

Dichiarazioni sulle policy JSON per i ruoli utente predefiniti multi-account AMS multi-account landing zone.

> **Note**
>
> I ruoli utente sono personalizzabili e possono differire in base all'account. Vengono fornite istruzioni su come trovare il proprio ruolo.

Questi sono esempi dei ruoli utente MALZ predefiniti. Per assicurarti di avere le policy impostate di cui hai bisogno, esegui il comando AWS `get-role`o accedi alla console AWS Management -> IAM e scegli Ruoli nel riquadro di navigazione.

Ruoli principali dell'account OU

Un account principale è un account di infrastruttura gestito da Malz. Gli account AMS multi-account landing zone Gli account Core includono un account di gestione e un account di rete.

Account Core OU: ruoli e politiche comuni

Ruolo	Politica o politiche
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Politica gestita AWS pubblica).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccesso (AWS Managed Policy pubblica).
AWSManagedServicesChangeManagementRole (versione dell'account principale)	ReadOnlyAccess
	AWSSupportAccesso
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

Account Core OU: ruoli e politiche dell'account di gestione

Ruolo	Politica o politiche
AWSManagedServicesBillingRole	AMSBillingPolitica (AMSBillingPolitica).
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Politica gestita AWS pubblica).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccesso (AWS Managed Policy pubblica).
AWSManagedServicesChangeManagementRole (versione dell'account di gestione)	ReadOnlyAccess

Ruolo	Politica o politiche
	AWSSupportAccesso
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

Account Core OU: ruoli e politiche degli account di rete

Ruolo	Politica o politiche
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Politica gestita AWS pubblica).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccesso (AWS Managed Policy pubblica).
AWSManagedServicesChangeManagementRole (versione dell'account di rete)	ReadOnlyAccess
	AWSSupportAccesso
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy
	AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

Ruoli dell'account dell'applicazione

I ruoli degli account dell'applicazione vengono applicati agli account specifici dell'applicazione.

Account dell'applicazione: ruoli e politiche

Ruolo	Politica o politiche
AWSManagedServicesReadOnlyRole	ReadOnlyAccess(Politica gestita AWS pubblica).
AWSManagedServicesCaseRole	ReadOnlyAccess
	AWSSupportAccesso (AWS Managed Policy pubblica). Questa policy fornisce l'accesso a tutte le operazioni e le risorse di supporto. Per informazioni, consulta Getting Started with AWS Support.
AWSManagedServicesSecurityOpsRole	ReadOnlyAccess
	AWSSupportEsempio di accesso Questa politica fornisce l'accesso a tutte le operazioni e le risorse di supporto.
	AWSCertificateManagerFullAccess informazioni, (AWS Managed Policy pubblica)
	AWSWAFFullAccess informazioni, (policy AWS Managed pubblica). Questa policy garantisce l'accesso completo alle risorse AWS WAF.
	AMSSecretsManagerSharedPolicy
AWSManagedServicesChangeManagementRole (versione dell'account dell'applicazione)	ReadOnlyAccess
	AWSSupportAccesso (AWS Managed Policy pubblica).

Ruolo	Politica o politiche
	Questa policy fornisce l'accesso a tutte le operazioni e le risorse di supporto. Per informazioni, consulta Getting Started with AWS Support.
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AMSReservedInstancesPolicy
	AMSS3Policy
AWSManagedServicesAdminRole	ReadOnlyAccess
	AWSSupportAccesso
	AMSChangeManagementInfrastructurePolicy
	AWSMarketplaceManageSubscriptions
	AMSSecretsManagerSharedPolicy
	AMSChangeManagementPolicy
	AWSCertificateManagerFullAccess
	AWSWAFFullAccesso
	AMSS3Policy
	AMSReservedInstancesPolicy

Esempi di policy

Vengono forniti esempi per la maggior parte delle politiche utilizzate. Per visualizzare la ReadOnlyAccess policy (lunga pagine in quanto fornisce l'accesso in sola lettura a tutti i AWS servizi), puoi utilizzare questo link, se disponi di un account AWS attivo:. ReadOnlyAccess Inoltre, qui è inclusa una versione ridotta.

AMSBillingPolitica

`AMSBillingPolicy`

Il nuovo ruolo Fatturazione può essere utilizzato dal reparto contabilità per visualizzare e modificare le informazioni di fatturazione o le impostazioni dell'account nell'account di gestione. Per accedere a informazioni come Contatti alternativi, visualizzare l'utilizzo delle risorse dell'account o tenere sotto controllo la fatturazione o persino modificare i metodi di pagamento, utilizzi questo ruolo. Questo nuovo ruolo comprende tutte le autorizzazioni elencate nella pagina Web delle azioni IAM di AWS Billing.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Action": [
                "aws-portal:ViewBilling",
                "aws-portal:ModifyBilling"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToBilling"
        },
        {
            "Action": [
                "aws-portal:ViewAccount",
                "aws-portal:ModifyAccount"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountSettings"
        },
        {
            "Action": [
                "budgets:ViewBudget",
                "budgets:ModifyBudget"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToAccountBudget"
```

```
        },
        {
            "Action": [
                "aws-portal:ViewPaymentMethods",
                "aws-portal:ModifyPaymentMethods"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPaymentMethods"
        },
        {
            "Action": [
                "aws-portal:ViewUsage"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToUsage"
        },
        {
            "Action": [
                "cur:DescribeReportDefinitions",
                "cur:PutReportDefinition",
                "cur:DeleteReportDefinition",
                "cur:ModifyReportDefinition"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostAndUsageReport"
        },
        {
            "Action": [
                "pricing:DescribeServices",
                "pricing:GetAttributeValues",
                "pricing:GetProducts"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPricing"
        },
        {
            "Action": [
                "ce:*",
                "compute-optimizer:*"
            ],
```

```
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToCostExplorerComputeOptimizer"
        },
        {
            "Action": [
                "purchase-orders:ViewPurchaseOrders",
                "purchase-orders:ModifyPurchaseOrders"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToPurchaseOrders"
        },
        {
            "Action": [
                "redshift:AcceptReservedNodeExchange",
                "redshift:PurchaseReservedNodeOffering"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AllowAccessToRedshiftAction"
        },
        {
            "Action": "savingsplans:*",
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "AWSSavingsPlansFullAccess"
        }
    ]
}
```

AMSChangeManagementReadOnlyPolicy

`AMSChangeManagementReadOnlyPolicy`

Autorizzazioni per visualizzare tutti i tipi di modifica AMS e la cronologia dei tipi di modifica richiesti.

AMSMasterAccountSpecificChangeManagementInfrastructurePolicy

`AMSMasterAccountSpecificChangeManagementInfrastructurePolicy`

Autorizzazioni per richiedere il tipo di modifica Deployment | Managed landing zone | Management account | Create application account (con VPC).

AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy

`AMSNetworkingAccountSpecificChangeManagementInfrastructurePolicy`

Autorizzazioni per richiedere l'account Deployment | Managed landing zone | Networking | Create application route table.

AMSChangeManagementInfrastructurePolicy

`AMSChangeManagementInfrastructurePolicy`(per gestione | Altro | Altro CTs)

Autorizzazioni per richiedere i tipi di modifica Gestione | Altro | Altro | Creazione e gestione | Altro | Altro | Aggiornamento dei tipi di modifica.

AMSSecretsManagerSharedPolicy

`AMSSecretsManagerSharedPolicy`

Autorizzazioni per la visualizzazione di dati segreti passwords/hashes condivisi da AMS Gestione dei segreti AWS (ad esempio password di accesso all'infrastruttura per il controllo).

Autorizzazioni per creare dati segreti da condividere con AMS password/hashes . (ad esempio, chiavi di licenza per prodotti che devono essere distribuiti).

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
   "Sid": "AllowAccessToSharedNameSpaces",
   "Effect": "Allow",
   "Action": "secretsmanager:*",
   "Resource": [
    "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
    "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
   ]
  },
  {
   "Sid": "DenyGetSecretOnCustomerNamespace",
   "Effect": "Deny",
   "Action": "secretsmanager:GetSecretValue",
   "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
```

```
  },
  {
   "Sid": "AllowReadAccessToAMSNameSpace",
   "Effect": "Deny",
   "NotAction": [
    "secretsmanager:Describe*",
    "secretsmanager:Get*",
    "secretsmanager:List*"
   ],
   "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
  }
 ]
}
```

AMSChangeManagementPolicy

`AMSChangeManagementPolicy`

Autorizzazioni per richiedere e visualizzare tutti i tipi di modifica AMS e la cronologia dei tipi di modifica richiesti.

AMSReservedInstancesPolicy

`AMSReservedInstancesPolicy`

Autorizzazioni per gestire le istanze riservate di Amazon EC2; per informazioni sui prezzi, consulta le istanze riservate di Amazon EC2.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Sid": "AllowReservedInstancesManagement",
  "Effect": "Allow",
  "Action": [
   "ec2:ModifyReservedInstances",
   "ec2:PurchaseReservedInstancesOffering"
  ],
  "Resource": [
   "*"
```

```
  ]
 }]
}
```

AMSS3Policy

`AMSS3Policy`

Autorizzazioni per creare ed eliminare file da bucket Amazon S3 esistenti.

> **Note**
>
> Queste autorizzazioni non garantiscono la possibilità di creare bucket S3; ciò deve essere fatto con il tipo Deployment | Advanced stack components | S3 storage | Create change.

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:AbortMultipartUpload",
                "s3:DeleteObject",
                "s3:PutObject"
            ],
            "Resource": "*"
        }
    ]
}
```

AWSSupportAccesso

`AWSSupportAccess`

Accesso completo a Supporto. Per informazioni, consulta Guida introduttiva a Supporto. Per informazioni su Premium Support, vedere Supporto.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "support:*"
  ],
  "Resource": "*"
 }]
}
```

AWSMarketplaceManageSubscriptions

`AWSMarketplaceManageSubscriptions`(Politica AWS gestita dal pubblico)

Autorizzazioni per sottoscrivere, annullare l'iscrizione e visualizzare Marketplace AWS gli abbonamenti.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "aws-marketplace:ViewSubscriptions",
   "aws-marketplace:Subscribe",
   "aws-marketplace:Unsubscribe"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
}
```

AWSCertificateManagerFullAccess

`AWSCertificateManagerFullAccess`

Accesso completo a. AWS Certificate Manager Per ulteriori informazioni, consulta AWS Certificate Manager.

AWSCertificateManagerFullAccessinformazioni, (Public AWS Managed Policy).

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Effect": "Allow",
  "Action": [
   "acm:*"
  ],
  "Resource": "*"
 }]
}
```

AWSWAFFullAccesso

AWSWAFFullAccess

Accesso completo a AWS WAF. Per ulteriori informazioni, vedere AWS WAF - Web Application Firewall.

AWSWAFFullAccessinformazioni, (politica AWS gestita dal pubblico). Questa politica garantisce l'accesso completo alle AWS WAF risorse.

JSON

```
{
 "Version":"2012-10-17",
 "Statement": [{
  "Action": [
   "waf:*",
   "waf-regional:*",
   "elasticloadbalancing:SetWebACL"
  ],
  "Effect": "Allow",
  "Resource": "*"
 }]
```

```
}
```

ReadOnlyAccess

`ReadOnlyAccess`

Accesso in sola lettura a tutti i AWS servizi e le risorse sulla console. AWS Quando AWS lancia un nuovo servizio, AMS aggiorna la ReadOnlyAccess policy per aggiungere autorizzazioni di sola lettura per il nuovo servizio. Le autorizzazioni aggiornate vengono applicate a tutte le entità principali a cui la policy è collegata.

Ciò non garantisce la possibilità di accedere agli host EC2 o agli host di database.

Se ne hai una attiva Account AWS, puoi utilizzare questo link ReadOnlyAccessper visualizzare l'intera ReadOnlyAccess policy. L'intera ReadOnlyAccess politica è molto lunga in quanto fornisce l'accesso in sola lettura a tutti. Servizi AWS Di seguito è riportato un estratto parziale della politica. ReadOnlyAccess

Single-Account Landing Zone (SALZ): per visualizzare le politiche relative ai ruoli utente predefinite e non personalizzate di AMS relative ai ruoli utente, vedere, successivo. SALZ: ruolo utente IAM predefinito

SALZ: ruolo utente IAM predefinito

Dichiarazioni di policy JSON per il ruolo utente predefinito di AMS single-account landing zone.

> **Note**
>
> Il ruolo utente predefinito di SALZ è personalizzabile e potrebbe differire in base all'account. Vengono fornite istruzioni su come trovare il proprio ruolo.

Di seguito è riportato un esempio del ruolo utente SALZ predefinito. Per assicurarti di avere le politiche impostate per te, esegui il `get-role`comando. In alternativa, accedi alla AWS Identity and Access Management console all'indirizzo https://console.aws.amazon.com/iam/, quindi scegli Ruoli.

Il ruolo di sola lettura del cliente è una combinazione di più politiche. Segue una suddivisione del ruolo (JSON).

Politica di audit di Managed Services:

ReadOnly Politica IAM di Managed Services

Politica per gli utenti di Managed Services

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
     "Sid": "AllowCustomerToListTheLogBucketLogs",
     "Effect": "Allow",
     "Action": [
       "s3:ListBucket"
     ],
     "Resource": [
       "arn:aws:s3:::mc-a*-logs-*"
     ],
     "Condition": {
       "StringLike": {
         "s3:prefix": [
           "aws/*",
           "app/*",
           "encrypted",
           "encrypted/",
           "encrypted/app/*"
         ]
       }
     }
   },
   {
     "Sid": "BasicAccessRequiredByS3Console",
     "Effect": "Allow",
     "Action": [
       "s3:ListAllMyBuckets",
       "s3:GetBucketLocation"
     ],
     "Resource": [
       "arn:aws:s3:::*"
     ]
   },
   {
     "Sid": "AllowCustomerToGetLogs",
     "Effect": "Allow",
     "Action": [
```

```
        "s3:GetObject*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/aws/*",
        "arn:aws:s3:::mc-a*-logs-*/encrypted/app/*"
      ]
    },
    {
      "Sid": "AllowAccessToOtherObjects",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteObject*",
        "s3:Get*",
        "s3:List*",
        "s3:PutObject*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCustomerToListTheLogBucketRoot",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringEquals": {
          "s3:prefix": [
            "",
            "/"
          ]
        }
      }
    },
    {
      "Sid": "AllowCustomerCWLConsole",
      "Effect": "Allow",
      "Action": [
        "logs:DescribeLogStreams",
        "logs:DescribeLogGroups"
```

```
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "AllowCustomerCWLAccessLogs",
      "Effect": "Allow",
      "Action": [
        "logs:FilterLogEvents",
        "logs:GetLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/aws/*",
        "arn:aws:logs:*:*:log-group:/infra/*",
        "arn:aws:logs:*:*:log-group:/app/*",
        "arn:aws:logs:*:*:log-group:RDSOSMetrics:*:*"
      ]
    },
    {
      "Sid": "AWSManagedServicesFullAccess",
      "Effect": "Allow",
      "Action": [
        "amscm:*",
        "amsskms:*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "ModifyAWSBillingPortal",
      "Effect": "Allow",
      "Action": [
        "aws-portal:Modify*"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "DenyDeleteCWL",
      "Effect": "Deny",
      "Action": [
```

```
        "logs:DeleteLogGroup",
        "logs:DeleteLogStream"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:*"
      ]
    },
    {
      "Sid": "DenyMCCWL",
      "Effect": "Deny",
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogStreams",
        "logs:FilterLogEvents",
        "logs:GetLogEvents",
        "logs:PutLogEvents"
      ],
      "Resource": [
        "arn:aws:logs:*:*:log-group:/mc/*"
      ]
    },
    {
      "Sid": "DenyS3MCNamespace",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/encrypted/mc/*",
        "arn:aws:s3:::mc-a*-logs-*/mc/*",
        "arn:aws:s3:::mc-a*-logs-*-audit/*",
        "arn:aws:s3:::mc-a*-internal-*/*",
        "arn:aws:s3:::mc-a*-internal-*"
      ]
    },
    {
      "Sid": "ExplicitDenyS3CfnBucket",
      "Effect": "Deny",
      "Action": [
        "s3:*"
      ],
      "Resource": [
        "arn:aws:s3:::cf-templates-*"
```

```
      ]
    },
    {
      "Sid": "DenyListBucketS3LogsMC",
      "Action": [
        "s3:ListBucket"
      ],
      "Effect": "Deny",
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*"
      ],
      "Condition": {
        "StringLike": {
          "s3:prefix": [
            "auditlog/*",
            "encrypted/mc/*",
            "mc/*"
          ]
        }
      }
    },
    {
      "Sid": "DenyS3LogsDelete",
      "Effect": "Deny",
      "Action": [
        "s3:Delete*",
        "s3:Put*"
      ],
      "Resource": [
        "arn:aws:s3:::mc-a*-logs-*/*"
      ]
    },
    {
      "Sid": "DenyAccessToKmsKeysStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "kms:*"
      ],
      "Resource": [
        "arn:aws:kms::*:key/mc-*",
        "arn:aws:kms::*:alias/mc-*"
      ]
    },
    {
```

```
      "Sid": "DenyListingOfStacksStartingWithMC",
      "Effect": "Deny",
      "Action": [
        "cloudformation:*"
      ],
      "Resource": [
        "arn:aws:cloudformation:*:*:stack/mc-*"
      ]
    },
    {
      "Sid": "AllowCreateCWMetricsAndManageDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:PutMetricData"
      ],
      "Resource": [
        "*"
      ]
    },
    {
      "Sid": "AllowCreateandDeleteCWDashboards",
      "Effect": "Allow",
      "Action": [
        "cloudwatch:DeleteDashboards",
        "cloudwatch:PutDashboard"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Politica condivisa di Customer Secrets Manager

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowSecretsManagerListSecrets",
      "Effect": "Allow",
```

```
      "Action": "secretsmanager:listSecrets",
      "Resource": "*"
    },
    {
      "Sid": "AllowCustomerAdminAccessToSharedNameSpaces",
      "Effect": "Allow",
      "Action": "secretsmanager:*",
      "Resource": [
        "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
        "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
      ]
    },
   {
      "Sid": "DenyCustomerGetSecretCustomerNamespace",
      "Effect": "Deny",
      "Action": "secretsmanager:GetSecretValue",
      "Resource": "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
    },
    {
      "Sid": "AllowCustomerReadOnlyAccessToAMSNameSpace",
      "Effect": "Deny",
      "NotAction": [
        "secretsmanager:Describe*",
        "secretsmanager:Get*",
        "secretsmanager:List*"
      ],
      "Resource": "arn:aws:secretsmanager:*:*:secret:ams-shared/*"
    }
  ]
}
```

Politica di iscrizione al Customer Marketplace

JSON

```
{
  "Version":"2012-10-17",
  "Statement": [
    {
      "Sid": "AllowMarketPlaceSubscriptions",
      "Effect": "Allow",
      "Action": [
```

```
        "aws-marketplace:ViewSubscriptions",
        "aws-marketplace:Subscribe"
      ],
      "Resource": [
        "*"
      ]
    }
  ]
}
```

Regole firewall di accesso predefinite

Queste sono le regole firewall predefinite necessarie per accedere alle istanze.

> **Note**
>
> Per informazioni sulle regole e le porte del firewall necessarie per stabilire un trust unidirezionale AD, consulta la AMS Security Guide accedendo alla console AWS Artifact -> scheda Report e cerca AWS Managed Services.

Porte di istanze Linux Stack

Queste regole sono necessarie per l'autenticazione negli stack AMS Linux.

Regole per le porte delle istanze Linux DA: Istanza Linux Stack A: CORP Domain Controller

Porta	Protocollo	Servizio	Direzione
389	TCP	LDAP	Ingresso
389	UDP	LDAP	Ingresso
88	TCP	Kerberos	Ingresso
88	UDP	Kerberos	Ingresso

Porte per istanze Windows Stack

Queste regole sono necessarie per l'autenticazione negli stack AMS Windows.

DA: Windows Stack Instance A: CORP Domain Controller

Porta	Protocollo	Servizio	Direzione
88	TCP | UDP	Kerberos	Ingresso e uscita
135	TCP | UDP	servizio DCE/RPC Locator	Ingresso e uscita
389	TCP | UDP	LDAP	Ingresso e uscita
3268	TCP | UDP	msft-gc, Microsoft Global Catalog (servizio LDAP che contiene dati provenienti da foreste di Active Directory)	Ingresso e uscita
445	TCP	Microsoft-DS Active Directory, condivisioni Windows	Ingresso e uscita
49152 - 65535	TCP	Porte dinamiche o private che non possono essere registrate con IANA. Questo intervallo viene utilizzato per servizi privati o personalizzati o per scopi temporanei e per l'allocazione automatica di porte effimere.	Ingresso e uscita

Gestione dei servizi in AWS Managed Services

Argomenti

- Governance degli account in AWS Managed Services
- Inizio del servizio in AWS Managed Services
- Gestione delle relazioni con i clienti (CRM)
- Ottimizzazione dei costi in AWS Managed Services
- Orari di servizio in AWS Managed Services
- Ottenere assistenza in AWS Managed Services

Come funziona il servizio AMS per te.

Governance degli account in AWS Managed Services

Questa sezione riguarda la governance degli account AMS.

Sei designato come cloud service delivery manager (CSDM) che fornisce assistenza consultiva in AMS e ha una conoscenza dettagliata del tuo caso d'uso e dell'architettura tecnologica per l'ambiente gestito. CSDMs collabora con account manager, account manager tecnici, architetti cloud AWS Managed Services (CAs) e architetti di soluzioni AWS (SAs), a seconda dei casi, per contribuire al lancio di nuovi progetti e fornire consigli sulle migliori pratiche durante lo sviluppo del software e i processi operativi. Il CSDM è il punto di contatto principale per AMS. Le principali responsabilità del vostro CSDM sono:

- Organizza e conduci riunioni mensili di revisione del servizio con i clienti.
- Fornisci dettagli sulla sicurezza, sugli aggiornamenti software per l'ambiente e sulle opportunità di ottimizzazione.
- Rispetta i tuoi requisiti, comprese le richieste di funzionalità per AMS.
- Rispondi e risolvi le richieste di fatturazione e segnalazione dei servizi.
- Fornisci informazioni dettagliate per consigli finanziari e di ottimizzazione della capacità.

Inizio del servizio in AWS Managed Services

Inizio del servizio: la data di inizio del servizio per un account AWS Managed Services è il primo giorno del primo mese di calendario dopo il quale AWS ti notifica che le attività stabilite nei requisiti di onboarding per quell'account AWS Managed Services sono state completate; a condizione che se AWS invia tale notifica dopo il ventesimo giorno di un mese solare, la data di inizio del servizio è il primo giorno del secondo mese di calendario successivo alla data di tale notifica.

Inizio del servizio

- R sta per parte responsabile che fa il lavoro per raggiungere l'obiettivo.
- I sta per informato; una parte che viene informata sui progressi, spesso solo al completamento del compito o del risultato.

Inizio del servizio

Fase #	Titolo della fase	Descrizione	Custome	AMBITI
1.	Consegna dell'account AWS al cliente	Il cliente crea un nuovo account AWS e lo consegna ad AWS Managed Services	R	I
2.	Account AWS Managed Services - progettazione	Completa la progettazione dell'account AWS Managed Services	I	R
3.	Account AWS Managed Services: crea	Un account AWS Managed Services viene creato in base alla progettazione nella fase 2.	I	R

Gestione delle relazioni con i clienti (CRM)

AWS Managed Services (AMS) fornisce un processo di gestione delle relazioni con i clienti (CRM) per garantire che venga stabilita e mantenuta una relazione ben definita con te. La base di questa relazione si basa sulla conoscenza approfondita di AMS delle tue esigenze aziendali. Il processo CRM facilita la comprensione accurata e completa di:

- Le esigenze della tua azienda e come soddisfarle
- Le tue capacità e i tuoi vincoli
- AMS e le tue diverse responsabilità e obblighi

Il processo CRM consente ad AMS di utilizzare metodi coerenti per fornirti servizi e garantire la governance del tuo rapporto con AMS. Il processo CRM include:

- Identificazione dei principali stakeholder
- Istituire un team di governance
- Conduzione e documentazione delle riunioni di revisione del servizio con voi
- Fornitura di una procedura formale per i reclami relativi al servizio con una procedura di intensificazione
- Implementazione e monitoraggio del processo di soddisfazione e feedback
- Gestione del contratto

Processo CRM

Il processo CRM include le seguenti attività:

- Identificazione e comprensione dei processi e delle esigenze aziendali. Il vostro accordo con AMS identifica i vostri stakeholder.
- Definizione dei servizi da fornire per soddisfare le vostre esigenze e requisiti.
- Vi incontreremo durante le riunioni di revisione del servizio per discutere di eventuali modifiche all'ambito del servizio AMS, allo SLA, al contratto e alle vostre esigenze aziendali. È possibile tenere riunioni intermedie con voi per discutere di prestazioni, risultati, problemi e piani d'azione.
- Monitoraggio della vostra soddisfazione utilizzando il nostro sondaggio sulla soddisfazione dei clienti e il feedback fornito durante le riunioni.
- Segnalazione delle prestazioni su report mensili sulle prestazioni misurati internamente.
- Esaminate insieme a voi il servizio per determinare le opportunità di miglioramento. Ciò include comunicazioni frequenti con l'utente in merito al livello e alla qualità del servizio AMS fornito.

Riunioni CRM

I responsabili della fornitura di servizi cloud AMS (CSDMs) organizzano riunioni con voi regolarmente per discutere dei percorsi di servizio (operazioni, sicurezza e innovazioni dei prodotti) e dei percorsi esecutivi (rapporti SLA, misure di soddisfazione e cambiamenti nelle esigenze aziendali).

Riunione	Scopo	Modalità	Partecipanti
Revisione settimanale dello stato (opzionale)	Problemi o incidenti in sospeso, patch, eventi di sicurezza, record dei problemi Tendenza operativa a 12 settimane (+/- 6) Preoccupazioni degli operatori dell'applicazione Programma del fine settimana	Cliente in loco location/ Telecom/Chime	AMS: CSDM e architetto cloud (CA) Membri del team assegnati dal cliente (ad es.: Cloud/Infrastructure, Application Support, team di architettura, ecc.)
Revisione aziendale mensile	Esamina le prestazioni dei livelli di servizio (report, analisi e tendenze) Analisi finanziaria Roadmap del prodotto GATTO	Cliente in loco location/ Telecom/Chime	AMS: CSDM, cloud architect (CA), account team AMS, responsabile tecnico del prodotto AMS (TPM) (opzionale), AMS OPS manager (opzionale) Tu: rappresentante dell'Application Operator

Riunione	Scopo	Modalità	Partecipanti
Revisione aziendale trimestrale	Prestazioni e tendenze di Scorecard e Service Level Agreement (SLA) (6 mesi) Prossimi piani/migrazioni per 3/6/9/12 mesi Rischio e mitigazione del rischio Principali iniziative di miglioramento Elementi della roadmap del prodotto Opportunità orientate al futuro Finanziari Iniziative di riduzione dei costi Ottimizzazione aziendale	Ubicazione del cliente in sede	AMS: CSDM, architetto cloud, account team AMS, direttore del servizio AMS, responsabile operativo AMS Tu: rappresentante dell'operatore dell'applicazione, rappresentante del servizio, direttore del servizio

Organizzazione delle riunioni CRM

L'AMS CSDM è responsabile della documentazione della riunione, tra cui:

- Creazione dell'agenda, che include le azioni da intraprendere, i problemi e l'elenco dei partecipanti.
- Creazione dell'elenco delle azioni esaminate in ogni riunione per garantire che le questioni vengano completate e risolte nei tempi previsti.
- Distribuzione dei verbali delle riunioni e dell'elenco delle azioni da intraprendere ai partecipanti alla riunione tramite e-mail entro un giorno lavorativo dalla riunione.
- Archiviazione dei verbali delle riunioni nell'apposito archivio di documenti.

In assenza del CSDM, il rappresentante AMS che dirige la riunione crea e distribuisce i verbali.

> **Note**
>
> Il CSDM collabora con voi per stabilire la governance degli account.

Rapporti mensili CRM

Il CSDM AMS prepara e invia presentazioni mensili sulle prestazioni del servizio. Le presentazioni includono informazioni su quanto segue:

- Data del rapporto
- Riepilogo e approfondimenti:
  - Richieste principali: numero di stack totali e attivi, stato dell'applicazione delle patch allo stack, stato di attivazione dell'account (solo durante l'onboarding), riepiloghi dei problemi specifici del cliente
  - Prestazioni: statistiche sulla risoluzione degli incidenti, avvisi, patch, richieste di modifica (), richieste di servizio e disponibilità di console e API RFCs
  - Problemi, sfide, preoccupazioni e rischi: stato dei problemi specifici del cliente
  - Prossimi articoli: piani di onboarding o risoluzione degli incidenti specifici per il cliente
- Risorse gestite: grafici e diagrammi a torta degli stack
- Metriche AMS: metriche di monitoraggio ed eventi, metriche degli incidenti, metriche di aderenza agli SLA di AMS, metriche delle richieste di assistenza, metriche di gestione delle modifiche, metriche di storage, metriche di continuità, metriche Trusted Advisor e riepiloghi dei costi (presentati in diversi modi). Richieste di funzionalità. Informazioni di contatto

> **Note**
>
> Oltre alle informazioni descritte, il CSDM vi informa anche di qualsiasi modifica sostanziale dell'ambito o dei termini, incluso il ricorso a subappaltatori da parte di AMS per attività operative.
> AMS genera report sull'applicazione di patch e backup che il CSDM include nel rapporto mensile. Come parte del sistema di generazione dei report, AMS aggiunge al tuo account un'infrastruttura che non è accessibile a te:
>
> - Un S3 Bucket, con i dati grezzi riportati
> - Un'istanza Athena, con definizioni di query per interrogare i dati

- Un Glue Crawler per leggere i dati grezzi dal bucket S3

Ottimizzazione dei costi in AWS Managed Services

AWS Managed Services fornisce ogni mese report dettagliati sull'utilizzo dei costi e sui risparmi durante le revisioni aziendali mensili (MBRs).

AMS segue una serie standard di processi e meccanismi per identificare le possibilità di riduzione dei costi nei tuoi account gestiti e aiutarti a pianificare e implementare le modifiche per ottimizzare la spesa in AWS.

> **Note**
>
> AMS sta sviluppando un video per contribuire all'ottimizzazione dei costi. Il primo passo consiste nel fornirti un PDF e un foglio di calcolo Excel con le migliori pratiche di ottimizzazione dei costi. Per accedere a queste risorse, aprite il file ZIP della guida rapida all'ottimizzazione dei costi.

Framework di ottimizzazione dei costi

AMS segue un approccio in tre fasi per ottimizzare i costi di AWS:

1. Identifica le modalità di ottimizzazione dei costi nel tuo ambiente gestito
2. Presentate un piano di ottimizzazione dei costi
3. Contribuisci a raggiungere l'ottimizzazione dei costi in modo misurabile

Identifica le vie di ottimizzazione dei costi nell'ambiente gestito

AMS utilizza strumenti AWS nativi come Cost explorer e Trusted Advisor, sfruttando al contempo oltre 20 modelli di risparmio sui costi tra ottimizzazione dell'architettura, ottimizzazioni delle EC2 istanze e ottimizzazioni AWS incentrate sull'account per creare consigli di risparmio su misura per te.

Alcuni dei consigli di ottimizzazione includono quanto segue.

Consigli per l'ottimizzazione dell'architettura:

- Utilizzo ottimale della classe di storage S3: Amazon S3 offre una gamma di classi di storage per soddisfare diversi requisiti di carico di lavoro in base all'accesso ai dati, alla resilienza e ai costi. L'analisi delle classi di storage S3 Intelligent-Tiering e S3 basata sulle esigenze del carico di lavoro consente di gestire i costi di S3 in modo efficiente.
- Utilizzo di architetture di caching: l'utilizzo delle istanze di cache, ove applicabile, può aiutarti a sostituire alcune istanze di database, soddisfacendo contemporaneamente i requisiti IOPS.
- Risparmi sugli upgrade EBS: la migrazione dei volumi EBS da gp2 a gp3 offre un risparmio sui costi fino al 20% e puoi sfruttare le prestazioni di base prevedibili di 3.000 IOPS e 125 MiB/s, indipendentemente dalle dimensioni del volume.
- Utilizzo dell'elasticità: le funzionalità di auto-scaling offerte AWS consentono un utilizzo efficace delle risorse e consentono l'ottimizzazione dei costi. La revisione e l'aggiornamento regolari delle politiche di scalabilità delle istanze in base alle necessità consentono ulteriori risparmi sui costi.

EC2 consigli incentrati sulle istanze

- Ridimensionamento corretto delle istanze: raccomandazioni incentrate sul dimensionamento delle istanze e sulle configurazioni ottimali in base all'utilizzo. I consigli includono anche l'utilizzo della funzionalità Amazon EC2 Auto Scaling e la EC2 sostituzione delle istanze, ove applicabile, AWS Lambda con contenuti Web statici su Amazon S3, ecc.
- Pianificazione delle istanze: l'utilizzo di AMS Resource Scheduler per avviare e arrestare automaticamente le istanze in base a una pianificazione temporale aiuta a contenere i costi, in particolare per le istanze non di produzione che non vengono utilizzate durante le ore non lavorative.
- Abbonamento ai piani di risparmio: il piano di risparmio è il modo più semplice per risparmiare sull'utilizzo. AWS Gli EC2 Instance Savings Plans offrono risparmi fino al 72% rispetto ai prezzi On-Demand sull'utilizzo delle EC2 istanze Amazon. Gli Amazon SageMaker AI Savings Plans offrono fino al 64% di risparmio sull'utilizzo dei servizi Amazon SageMaker AI. AMS fornisce raccomandazioni appropriate sui piani di risparmio in base all'utilizzo AWS delle risorse.
- Guida all'utilizzo e al consumo delle istanze EC2 riservate (RI): Amazon Reserved Instances (RI) offre uno sconto significativo (fino al 75%) rispetto ai prezzi On-Demand e fornisce una riserva di capacità se utilizzate in una zona di disponibilità specifica.
- Utilizzo delle istanze Spot: i carichi di lavoro con tolleranza ai guasti possono utilizzare le istanze Spot e ridurre i prezzi fino al 90%.
- Chiusura delle istanze inattive: identificazione e segnalazione delle istanze inattive o con un utilizzo limitato che possono essere interrotte.

Consigli incentrati sull'account

- Pulizia dell'account: a livello di account, AMS identifica anche i volumi EBS non utilizzati, i CloudTrail percorsi duplicati, gli account vuoti con risorse inutilizzate e così via, e fornisce consigli per la pulizia.
- Raccomandazioni sugli SLA: inoltre, AMS esamina regolarmente gli account Plus e Premium e consiglia di scegliere il livello SLA giusto per gli account.
- Ottimizzazione dell'automazione AMS: AMS ottimizza continuamente l'automazione AMS e l'infrastruttura utilizzata per fornire i servizi AMS.

Presentazione ai clienti e assistenza nella pianificazione

AMS effettua revisioni aziendali mensili (MBRs) con le principali parti interessate dei clienti e presenta le possibilità, i meccanismi e le raccomandazioni di riduzione dei costi identificati, oltre ai potenziali risparmi sui costi. Collaboriamo inoltre con voi per pianificare le modifiche necessarie.

Assisti nell'implementazione delle raccomandazioni e misura l'impatto sui costi

AMS aiuta a raggiungere e misurare gli impatti sui costi e le modifiche all'ottimizzazione.

Valuti l'impatto applicativo, il rischio e i criteri di successo delle modifiche consigliate e invii le richieste di modifica appropriate (RFCs) tramite la console AMS. AMS collabora con te e implementa le modifiche relative all'ottimizzazione dei costi nei tuoi account gestiti. AMS misura l'impatto sui costi e include i risparmi realizzati nelle revisioni aziendali mensili (). MBRs

Matrice di responsabilità per l'ottimizzazione dei costi

Responsabilità nell'ottimizzazione dei costi di AMS.

Ottimizzazione dei costi RACI

Attività	Customer	AMS
Compilazione di raccomandazioni per la riduzione	I	R

Attività	Customer	AMS
dei costi e preparazione del rapporto		
Presentazione del rapporto sui risparmi	C	R
Pianificazione delle modifiche associate ai risparmi sui costi	R	C
Valutazione dell'impatto e del rischio del cambiamento	R	C
Raccolta fondi RFCs per l'attuazione delle modifiche	R	C

Attività	Customer	AMS
Revisione RFCs e implementazione delle modifiche	C	R
Test dell'applicazione e convalida dell'implementazione delle modifiche	R	C
Misurazione dell'impatto sui costi dopo la modifica e presentazione al cliente	I	R

Orari di servizio in AWS Managed Services

Funzionalità	AMS Advanced
	Livello Premium
Richiesta di assistenza	24/7
Gestione degli incidenti (P2-P3)	24/7
Backup e ripristino	24/7
Gestione delle patch	24/7
Monitoraggio e avvisi	24/7
Richiesta di modifica automatica (RFC)	24/7
Richiesta di modifica non automatizzata (RFC)	24/7
Responsabile della fornitura di servizi cloud (CSDM)	Dal lunedì al venerdì: dalle 08:00 alle 17:00, orario lavorativo locale

Ottenere assistenza in AWS Managed Services

AMS ti supporta con la gestione degli incidenti, la gestione delle richieste di servizio e la gestione delle modifiche 24 ore al giorno, 7 giorni alla settimana, 365 giorni all'anno (in conformità con l'accordo sul livello di servizio AMS applicato all'account).

Per segnalare un problema di prestazioni del servizio AWS o AMS che ha un impatto sull'ambiente gestito, utilizza la console AMS e invia un rapporto sull'incidente. Per i dettagli, consulta Segnalazione di un incidente. Per informazioni generali sulla gestione degli incidenti con AMS, consulta Risposta agli incidenti.

Per richiedere informazioni o consigli o per richiedere servizi aggiuntivi ad AMS, utilizza la console AMS e invia una richiesta di servizio. Per i dettagli, vedi Creazione di una richiesta di assistenza. Per informazioni generali sulle richieste di assistenza AMS, vedere Gestione delle richieste di assistenza.

Modifiche alle modalità di gestione

AWS Managed Services (AMS) utilizza la modalità di gestione delle modifiche per bloccare le modifiche in AMS Advanced. Le modalità di gestione delle modifiche aiutano a mantenere elevati standard operativi per l'ambiente, a controllare i rischi e prevenire impatti negativi. AMS Advanced dispone di diverse modalità che offrono diversi livelli di controllo e rischio. Tutte le modalità, ad eccezione della modalità Customer-Managed, sono gestite da AMS. Le seguenti sono le modalità di gestione delle modifiche disponibili:

- Modalità RFC (in precedenza modalità CM standard): fornisce un sistema di «richiesta di modifica» (RFC) e tipi di modifica personalizzati AMS () CTs
- Modalità Direct Change: uguale alla modalità RFC più utilizzo di AWS APIs e console per creare risorse gestite da AMS
- AWS Service Catalog su AMS: simile alla modalità Direct Change, ma invece di utilizzare il sistema di gestione delle modifiche AMS (RFCs), utilizzi AWS Service Catalog per creare risorse che poi AMS gestisce.
- Modalità sviluppatore: come nella modalità Direct Change, solo le risorse create con AWS APIs e le console non sono gestite da AMS: sei responsabile della loro gestione
- Modalità Self Service Provisioning (SSP): uguale alla modalità Developer, tranne per il fatto che non è possibile accedere al sistema di gestione delle modifiche AMS (no) RFCs
- Modalità gestita dal cliente: AMS ti offre una landing zone multi-account, ma la gestione di tutte le risorse è a tuo carico

Il sistema di gestione delle modifiche AWS Managed Services (AMS), che utilizza l'API di gestione delle modifiche (CM), fornisce operazioni per creare e gestire le richieste di modifica (RFCs) per gli account multi-account landing zone (MALZ) e single-account landing zone (SALZ).

Una richiesta di modifica (RFC) è una richiesta creata dall'utente o da AMS tramite l'interfaccia AMS per apportare una modifica all'ambiente gestito e include un ID del tipo di modifica (CT) per una particolare operazione.

L'API AMS change management (CM) fornisce operazioni per creare e gestire le richieste di modifica (RFCs). Puoi creare, aggiornare, inviare, approvare, rifiutare e annullare. RFCs Gli operatori AMS possono creare, aggiornare, inviare, approvare, rifiutare, annullare e contrassegnare come chiuso. RFCs

Per un elenco dei prefissi riservati AMS da non utilizzare nei tag o in altri nomi, consulta Prefissi riservati.

Per informazioni su ogni tipo di modifica, inclusi schemi ed esempi, consulta l'AMS Change Type Reference.

> **Note**
>
> Tutte le chiamate API di gestione delle modifiche vengono registrate in AWS CloudTrail. Per ulteriori informazioni, consulta Accesso ai log.

Panoramica delle modalità

Usa queste informazioni per aiutarti a selezionare la modalità AWS Managed Services (AMS) appropriata per ospitare le tue applicazioni, in base alla combinazione desiderata di flessibilità e governance prescrittiva per raggiungere i tuoi risultati di business.

Il pubblico a cui sono destinate queste informazioni è:

- Team clienti responsabili della strategia e della governance delle rispettive landing zone. Queste informazioni aiuteranno il team a gettare le basi di una landing zone gestita da AMS, con le modalità AMS che vorrebbe offrire ai propri clienti interni ed esterni.
- Proprietari di aziende e applicazioni incaricati di migrare la propria applicazione su AMS. Queste informazioni aiuteranno a pianificare la migrazione delle applicazioni, con la modalità AMS appropriata alla migrate/host loro applicazione. Nota, la stessa applicazione può essere ospitata in più di una modalità AMS durante diverse fasi del ciclo di vita del Software Development Life Cycle (SDLC).
- I partner AMS hanno il compito di guidare i clienti sulle diverse opzioni di creazione e migrazione ad AMS.

Queste informazioni sono particolarmente utili durante la fase di base della configurazione della piattaforma gestita da AMS e durante la transizione dalla fase di base a quella di migrazione del percorso di adozione del cloud, subito dopo il completamento dell'onboarding verso AMS e ti concentri sulla governance e sulle operazioni delle applicazioni.

Tipi di modalità e account in AMS

Le modalità AWS Managed Services (AMS) possono essere definite come modalità di interazione con il servizio AMS nell'ambito del framework di governance specifico per ciascuna modalità. Sono riportate le differenze tra le zone di atterraggio, la multi-account landing zone o MALZ e la single-account landing zone o SALZ.

> **Note**
>
> Per dettagli sull'implementazione delle applicazioni e sulla scelta della modalità AMS corretta, consulta Modi e applicazioni o carichi di lavoro AMS.
> Per i casi d'uso reali delle diverse modalità, consulta Casi d'uso nel mondo reale per le modalità AMS

La tabella seguente fornisce le descrizioni delle modalità per servizio AMS.

Funzionalità AMS	modalità RFC (precedentemente modalità CM standard) / OOD*	modalità Direct Change	AWS Service Catalog	Provisioning self-service /modalità sviluppatore	Gestito dal cliente
Configurazione della zona di atterraggio	MALZ e SALZ	MALZ e SALZ	MALZ e SALZ		
Gestione delle modifiche	Pianificazione delle modifiche, revisione delle modifiche manuali e registraz	Uguale alla modalità RFC per modifiche ad alto rischio come IAM o gruppi di sicurezza	Nessuno		

Funzionalità AMS	modalità RFC (precedentemente modalità CM standard) / OOD*	modalità Direct Change	AWS Service Catalog	Provisioning self-service /modalità sviluppatore	Gestito dal cliente
	ione delle modifiche				
Registrazione, monitoraggio, guardrail e gestione degli eventi	Sì (risorse supportate)			No	
Gestione della continuità	Sì (risorse supportate)			Non applicabile/ No	No
Gestione della sicurezza	Controlli di sicurezza a livello di istanza e controlli a livello di account			Controlli a livello di account	Controlli a livello di AWS Org
Gestione delle patch	Sì			Non applicabile/ No	No
Gestione degli incidenti e dei problemi	SLA di risposta e risoluzione per le risorse supportate da AMS			SLA di risposta per le risorse risultanti	No
Creazione di report	Sì			No	

Funzionalità AMS	modalità RFC (precedentemente modalità CM standard) / OOD*	modalità Direct Change	AWS Service Catalog	Provisioning self-service /modalità sviluppatore	Gestito dal cliente
Gestione delle richieste di assistenza	Sì			Solo richieste di supporto	No

* Operations On Demand (OOD) offre un'offerta ai clienti che utilizzano la modalità RFC per gestire le modifiche tramite risorse dedicate. Per ulteriori dettagli, consultate il catalogo di offerte di Operations on Demand e contattate il vostro responsabile della fornitura di servizi cloud (CSDM).

> **Note**
>
> Modalità Self-Service Provisioning in AMSe Modalità AMS Advanced Developer possono entrambi sembrare adatti per un'applicazione con un'architettura complessa radicata nei servizi AWS nativi. Quando si progettano carichi di lavoro, si fanno compromessi tra eccellenza operativa e agilità, in base al contesto aziendale. Questo è un buon modo di pensare alla selezione della modalità SSP o della modalità Sviluppatore per l'applicazione. La selezione può cambiare anche in base alla fase SDLC dell'applicazione. Ad esempio: quando l'applicazione è pronta per la produzione, la modalità SSP potrebbe essere l'opzione più appropriata a causa dei guardrail AMS più rigidi in questa modalità. I guardrail vengono applicati sotto forma di controlli preventivi come il controllo delle modifiche basato su RFC per gli aggiornamenti IAM e a livello di unità organizzativa dell'applicazione. SCPs Le decisioni aziendali possono stabilire le priorità di progettazione. È possibile ottimizzare per aumentare la flessibilità per i proprietari delle applicazioni nella fase di «pre-produzione», a scapito della governance e del supporto operativo.

Architettura MALZ e modalità AMS associate

AMS multi-account landing zone (MALZ) offre la possibilità di effettuare automaticamente il provisioning degli account delle applicazioni (o account delle risorse) nelle unità organizzative (OU) predefinite: Customer Managed OU, Managed OU o Development OU. L'infrastruttura fornita negli account applicativi creati in ciascuna di queste unità organizzative è soggetta alla modalità AMS specifica offerta da tali unità organizzative di base. È comune trovare una combinazione di due o più modalità nello stesso account dell'applicazione. Ad esempio: la modalità RFC e la modalità SSP possono coesistere in un account gestito AMS che ospita un'architettura di pipeline composta da API Gateway e Lambda per le funzioni di attivazione ed EC2, S3 e SQS per l'ingestione e l'orchestrazione. In questo caso, la modalità SSP si applicherebbe a Lambda e API Gateway.

La Figura 1 illustra come vengono offerte diverse modalità tramite la funzionalità di base di AMS. OUs Quando si richiede un nuovo account di applicazione in AMS, è necessario selezionare l'unità organizzativa per l'account.

Architettura MALZ e modalità AMS associate

AMS sfrutta le best practice di OUs base basate su AWS per gestire in modo logico gli account utilizzando Service Control Policies (). SCPs Questo serve come modo per applicare il framework di governance con ogni modalità AMS. Qualsiasi barriera di governance e sicurezza (sotto forma di SCPs) applicata al sistema di base viene applicata OUs anche automaticamente. custom/child OUs SCPs È possibile richiederne di aggiuntivi per il bambino. OUs È importante comprendere che gli account delle applicazioni non sono la stessa cosa delle modalità. Le modalità vengono applicate all'infrastruttura fornita all'interno degli account e definiscono le responsabilità operative tra AMS e i clienti.

Figura 1: Architettura MALZ e modalità AMS associate

> **Note**
>
> Il termine «restrittivo» implica la possibilità di richiedere politiche personalizzate in merito OUs, che vengono approvate da AMS per garantire che non interferiscano con le capacità di AMS di fornire l'eccellenza operativa. case-by-case Per un elenco dettagliato dei guardrail AMS, consulta AMS Guardrails nella guida per l'utente.

Modalità e applicazioni o carichi di lavoro AMS

Considerate i requisiti operativi e di governance per le vostre applicazioni quando scegliete la modalità giusta, richiedendo un nuovo account applicativo o ospitando l'applicazione in un account applicativo esistente. La scelta della modalità AMS appropriata per ogni applicazione o carico di lavoro dipende dai seguenti fattori:

- Il tipo di funzione del ciclo di vita SDLC che l'ambiente fornirà (ad esempio, sandbox con modifiche non moderate, UAT con alcune modifiche frequenti, produzione con modifiche minime e altamente regolamentata)
- Le politiche di governance necessarie (applicate a livello di unità organizzativa) SCPs
- Modello operativo (se desideri assumere la responsabilità operativa o desideri esternalizzarla ad AMS)
- I risultati aziendali desiderati, come il tempo impiegato per operare nel cloud e il costo delle operazioni.

> **Note**
>
> Per una descrizione dei tipi di modalità per servizio AMS, consulta Tipi di modalità e account in AMS.
> Per i casi d'uso reali delle diverse modalità, consulta Casi d'uso nel mondo reale per le modalità AMS

La tabella seguente riporta le considerazioni chiave per i proprietari delle applicazioni per aiutarli a decidere la modalità AMS più adatta. I proprietari delle applicazioni dovrebbero includere una fase di valutazione prima della migrazione delle applicazioni per comprendere appieno quale modalità si applica alla loro applicazione specifica. Esempio: per le applicazioni basate su servizi nativi del cloud o su un'architettura serverless, l'opzione migliore potrebbe essere iniziare a creare e iterare in modalità sviluppatore e implementare l'infrastruttura come codice finale utilizzando la modalità AMS Managed — SSP. In questo caso può essere necessario un leggero rifattorizzazione per garantire che tutti i CloudFormation modelli creati per l'implementazione automatizzata soddisfino le linee guida di acquisizione stabilite da AMS. Inoltre, tutte le autorizzazioni IAM devono essere approvate da AMS Security per garantire che seguano il modello con privilegi minimi.

La modalità AMS selezionata per ospitare l'applicazione può aiutarvi a sviluppare il modello operativo cloud desiderato.

> **Note**
>
> In una singola AMS Managed Landing Zone possono esistere più modelli operativi cloud in base alle diverse modalità AMS selezionate per ospitare le applicazioni.

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
Prontezza operativa						
Registrazione, monitoraggio e gestione degli eventi	AMS è responsabile di tutte le infrastrutture gestite			Cliente responsabile dei Self-Service Provisioned Services (SSP)	Cliente responsabile del provisioning delle risorse utilizzando il ruolo di sviluppatore IAM esterno al sistema AMS CM	Responsabile del cliente
Gestione della continuità	Responsabilità di AMS di eseguire il piano di backup selezionato dal cliente			Cliente responsabile dei Self-Service Provisioned Services (SSP)	Cliente responsabile del provisioning delle risorse utilizzando il ruolo di sviluppatore IAM esterno al sistema AMS CM	

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
Gestione degli accessi a livello di istanza	Gestione AMS tramite AD trust unidirezionale con dominio locale. Richiede un'infrastruttura gestita per entrare a far parte del dominio AMS			Non applicabile	Cliente responsabile del provisioning delle risorse utilizzando il ruolo di sviluppatore IAM esterno al sistema AMS CM	
Gestione della sicurezza e gestione degli accessi a livello di account	Responsabilità di AMS per tutti gli account gestiti			AMS è responsabile di tutti gli account gestiti	Cliente responsabile delle risorse fornite utilizzando il ruolo di sviluppatore IAM esterno al sistema AMS CM	

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
Gestione delle patch	Responsabilità di AMS per tutti gli account gestiti			Cliente responsabile dei Self-Service Provisioned Services (SSP)	Cliente responsabile del provisioning delle risorse utilizzando il ruolo di sviluppatore IAM esterno al sistema AMS CM	
Gestione delle modifiche	Responsabilità di AMS per tutti gli account gestiti			Cliente responsabile dei Self-Service Provisioned Services (SSP)	Cliente responsabile del provisioning delle risorse utilizzando il ruolo di sviluppatore IAM esterno al sistema AMS CM	

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
Gestione del provisioning	Prescrittiva e standardizzata per le opzioni di approvvigionamento offerte in AMS	Flessibilità di utilizzare direttamente l'API di servizio AWS per AWS Service Catalog secondo gli standard prescrittivi AMS	Flessibilità per utilizzare direttamente l'API dei servizi AWS secondo gli standard prescrittivi AMS	Flessibilità di utilizzare direttamente il servizio AWS APIs per i servizi SSP	Flessibilità di utilizzare direttamente l'API dei servizi AWS per il provisioning	
Gestione e audit degli incidenti	AMS è responsabile di tutti gli account gestiti				Cliente responsabile delle risorse fornite utilizzando il ruolo di sviluppatore IAM esterno ad AMS Change Management System	

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
GuardRails e infrastruttura condivisa (rete) e framework di sicurezza	Prescrittivo e standardizzato che sfrutta gli account AMS Core					Flessibile e personalizzato che sfrutta gli account AMS Core
Prontezza delle applicazioni						
Rifattorizzazione delle applicazioni	È necessaria una leggera rifattorizzazione				È necessaria una leggera rifattorizzazione (se fornita utilizzando AMS Standard CM)	Non è necessario il refactoring
Support per i servizi AWS	Limitato a quanto supportato da AMS					Non limitato
Considerazioni aziendali						

Problemi decisionali	Modalità CM standard/ OOD*	AWS Service Catalog	Modalità Direct Change	Fornitura self-service	Modalità sviluppatore	Gestito dal cliente
È ora di essere pronti all'operatività	Da tre a sei mesi			Oltre 6 mesi a seconda delle competenze operative delle applicazioni del cliente		6-18 mesi a seconda dell'infrastruttura del cliente e delle competenze operative delle applicazioni
Costi	$$$$			$$$	$$	$
Esempi di applicazione	Server Web con stack a 3 livelli, app con requisiti di conformità e normativi			Server Web che utilizza API Gateway, applicazione containerizzata che sfrutta ECS/ EKS	Iterazione/ottimizzazione su un'applicazione Data Lake che utilizza Lambda, Glue, Athena, ecc.	Applicazioni decentralizzate accounts/ applications come sandbox, gestite da terze parti

* Operations On Demand (OOD) offre un'offerta ai clienti che utilizzano la modalità CM Standard per gestire le modifiche tramite risorse dedicate. Per ulteriori dettagli, consultate il catalogo di offerte di Operations on Demand e contattate il vostro cloud service delivery manager (CSDM).

> **Note**
>
> Il confronto dei prezzi tra la modalità SSP e la modalità Developer presuppone che vengano forniti gli stessi servizi AWS.

Confronto delle modalità AMS con gli obiettivi aziendali e IT

Come mostrato, se stai cercando un modello di governance altamente controllato e standardizzato per le tue applicazioni, le modalità Standard Change gestite da AMS, AWS Service Catalog o Direct Change sono la soluzione migliore. Se hai bisogno di un modello di governance personalizzato incentrato sull'innovazione delle applicazioni senza la necessità di una prontezza operativa, seleziona la modalità Customer Managed. Con la modalità Customer Managed, potrebbe essere necessario più tempo per rendere operative le applicazioni, in quanto spetta a te definire persone, processi e strumenti per supportare funzionalità operative come la gestione degli incidenti, la gestione della configurazione, la gestione del provisioning, la gestione della sicurezza, la gestione delle patch, ecc.

Casi d'uso reali per le modalità AMS

Esaminali per determinare come utilizzare le modalità AMS.

- Caso d'uso 1, imperativo aziendale per ridurre i costi con un'uscita dal data center urgente: un'azienda che organizza un evento aziendale importante, come l'uscita dal data center, è interessata a riospitare le proprie applicazioni on-premise sul cloud. La maggior parte dell'inventario locale è costituito da server Windows e Linux con una combinazione di versioni del sistema operativo. In tal modo, il cliente desidera anche sfruttare i risparmi sui costi offerti dal passaggio al cloud e migliorare il livello tecnico e di sicurezza delle proprie applicazioni. Il cliente desidera muoversi rapidamente, ma non ha ancora maturato le competenze interne in materia di operazioni cloud. Il cliente deve trovare un equilibrio tra il refactoring, un eccesso di refactoring può essere rischioso in tempi ristretti. Tuttavia, con alcune operazioni di refactoring, come l'aggiornamento delle versioni del sistema operativo e l'ottimizzazione dei database, le applicazioni possono raggiungere un livello di prestazioni superiore. In questo esempio, il cliente può selezionare la modalità RFC gestita da AMS per riospitare la maggior parte delle proprie applicazioni. AMS fornisce operazioni infrastrutturali, guidando al contempo i team operativi dei clienti sulle migliori pratiche per operare in sicurezza nel cloud.

La modalità AWS Service Catalog gestita da AMS e Direct Change gestita da AMS offre al cliente una maggiore flessibilità e al contempo il raggiungimento degli stessi risultati e obiettivi di business. Inoltre, il cliente può utilizzare l'offerta AMS Operations On Demand (OOD) per disporre di tecnici operativi AMS dedicati a dare priorità all'esecuzione delle richieste di modifica (). RFCs

Oltre a delegare ad AMS le attività operative indifferenziate dell'infrastruttura (patch, backup, gestione degli account, ecc.), il cliente può continuare a concentrarsi sull'ottimizzazione della propria applicazione e potenziare i team interni sulle operazioni cloud. AMS fornisce report mensili al cliente sui risparmi sui costi e fornisce raccomandazioni sull'ottimizzazione delle risorse. In questo caso d'uso, se ci sono end-of-life applicazioni ospitate su versioni di sistemi operativi precedenti come Windows 2003 e 2008, che il cliente ha deciso di non rifattorizzare, anche quelle possono essere migrate su AMS e ospitate in un account che sfrutta la modalità Customer Managed.

- Usa Case 2, creando un data lake con Lambda, Glue, Athena entro i confini sicuri di AMS: un'azienda sta cercando di configurare un Data Lake per soddisfare le esigenze di reporting per più applicazioni in AMS. Il cliente desidera utilizzare i bucket S3 per l'archiviazione di set di dati e AWS Athena per eseguire query sul set di dati per ogni report. S3 e AWS Athena verranno distribuiti in account AMS Managed separati. L'account con S3 dispone anche di altri servizi come Glue, Lambda e Step Functions per creare una pipeline di ingestione dei dati. Glue, Lambda, Athena e Step Functions sono considerati servizi Self-Service Provisioning (SSP) in questo caso. Il cliente ha inoltre distribuito un' EC2 istanza nell'account che funge da server ad hoc. tooling/scripting Il cliente inizia richiedendo ad AMS di abilitare i servizi SSP nel proprio account AMS Managed. AMS assegna un ruolo IAM per ogni servizio che il cliente può assumere, una volta che il ruolo è stato integrato nella soluzione di federazione del cliente. Per facilitare la gestione, il cliente può anche combinare le policy per i ruoli IAM separati in un unico ruolo personalizzato, alleviando la necessità di cambiare ruolo quando si lavora tra i servizi AWS. Una volta abilitato il ruolo nell'account, il cliente può configurare i servizi in base alle proprie esigenze. Tuttavia, il cliente deve utilizzare il sistema di gestione delle modifiche AMS per richiedere autorizzazioni aggiuntive, a seconda del caso d'uso.

  Ad esempio, per accedere a Glue Crawlers, Glue ha bisogno di autorizzazioni aggiuntive. Saranno inoltre necessarie autorizzazioni aggiuntive per creare sorgenti di eventi per Lambda. Il cliente collaborerà con AMS per aggiornare i ruoli IAM per consentire l'accesso da più account ad Athena per interrogare i bucket S3. Saranno inoltre necessari aggiornamenti ai ruoli di servizio o ai ruoli collegati ai servizi tramite AMS change management for Lambda per chiamare il servizio Step Functions e Glue per leggere e scrivere su tutti i bucket S3. AMS collabora con i clienti per

garantire che venga seguito il modello di accesso con privilegi minimi e che le modifiche IAM richieste non siano eccessivamente permissive e non espongano l'ambiente a rischi inutili. Il team del data lake del cliente dedica del tempo alla pianificazione di tutte le autorizzazioni IAM necessarie per i servizi specifici dell'architettura del cliente e richiede ad AMS di abilitarle. Questo perché tutte le modifiche IAM vengono elaborate manualmente e sottoposte a revisione da parte del team di sicurezza AMS. Il tempo necessario per elaborare queste richieste deve essere preso in considerazione nella pianificazione di distribuzione delle applicazioni.

Poiché i servizi SSP sono operativi nell'account, il cliente può richiedere assistenza e segnalare problemi tramite la gestione degli incidenti e le richieste di assistenza AMS. Tuttavia, AMS non monitorerà attivamente le metriche delle prestazioni e della concorrenza per Lambda o le metriche dei lavori per Glue. È responsabilità del cliente garantire che la registrazione e il monitoraggio appropriati siano abilitati per i servizi SSP. L' EC2 istanza e il bucket S3 dell'account sono completamente gestiti da AMS.

- Usa Case 3, configurazione rapida e flessibile di una pipeline di implementazione CICD in AMS: un cliente sta cercando di configurare una pipeline CICD basata su Jenkins per distribuire la pipeline di codice a tutti gli account di applicazione in AMS. Il cliente potrebbe ritenere più adatto ospitare questa pipeline CICD nella modalità Direct Change (DCM) gestita da AMS o nella modalità Developer gestita da AMS, perché offre la flessibilità necessaria per configurare il server Jenkins con la configurazione personalizzata richiesta EC2, con le autorizzazioni IAM desiderate per l'accesso CloudFormation e i bucket S3 che ospitano l'artifact repository. Sebbene ciò possa essere fatto anche in modalità RFC gestita da AMS, il team del cliente dovrebbe creare più manuali RFCs per i ruoli IAM per iterare sul set meno permissivo di autorizzazioni approvate, che vengono riviste manualmente da AMS. DCM consente ai clienti di raggiungere i propri obiettivi operativi su AWS evitando al contempo la necessità di creare più ruoli manuali RFCs per IAM, quando utilizzano la modalità RFC gestita da AMS, per iterare sul set meno permissivo di autorizzazioni approvate, che vengono riviste manualmente da AMS. Ciò richiederebbe tempo e formazione da parte del cliente per potenziare i processi e gli strumenti AMS. Utilizzando la modalità Developer, il cliente può iniziare con un «ruolo di sviluppatore» per il provisioning dell'infrastruttura utilizzando AWS nativo APIs. Il modo più rapido e flessibile per configurare questa pipeline sarebbe utilizzare la modalità AMS Managed-Developer. La modalità sviluppatore offre il modo più rapido e semplice, compromettendo al contempo l'integrazione operativa, mentre DCM è meno flessibile ma fornisce lo stesso livello di supporto operativo della modalità RFC.
- Usa Case 4, modello operativo personalizzato all'interno di AMS Foundation: un cliente sta cercando di uscire dal data center in base alle scadenze e una delle sue applicazioni aziendali è completamente gestita da un MSP di terze parti, comprese le operazioni delle applicazioni e

le operazioni dell'infrastruttura. Supponendo che il cliente non abbia il tempo di programmare per rifattorizzare l'applicazione in modo che possa essere gestita da AMS, la modalità Customer Managed è un'opzione adatta. Il cliente può sfruttare la configurazione automatica e rapida della Landing Zone gestita da AMS. Possono sfruttare la gestione centralizzata degli account che controlla la vendita e la connettività degli account tramite l'account di rete centralizzato. Inoltre, semplifica la loro fatturazione consolidando gli addebiti per tutti gli account gestiti dai clienti tramite l'account AMS Payer. Il cliente ha la flessibilità necessaria per configurare il proprio modello di gestione degli accessi personalizzato con l'MSP, separato dalla gestione degli accessi standard utilizzata per gli account AMS Managed. In questo modo, utilizzando la modalità Customer Managed, può configurare un ambiente gestito AMS soddisfacendo al contempo l'esigenza aziendale di abbandonare l'ambiente locale. In questo caso, se il cliente dispone anche di applicazioni basate su Windows da migrare sul cloud e sceglie di trasferirle su un account Customer Managed, è responsabile della creazione di un modello operativo cloud. Questa operazione può essere complessa, costosa e dispendiosa in termini di tempo, a seconda della capacità del cliente di trasformare i processi IT tradizionali e formare il personale. Il cliente può risparmiare tempo e costi trasferendo tali carichi di lavoro su un account gestito da AMS e affidando le operazioni dell'infrastruttura ad AMS.

> **Note**
>
> A volte i clienti possono sentire la necessità di spostare gli account delle applicazioni tra il framework di governance della modalità RFC o SSP e la modalità Developer. Ad esempio, i clienti possono ospitare un'applicazione in modalità gestita da AMS come parte della migrazione iniziale, ma col tempo desiderano riscrivere l'applicazione per ottimizzarla per i servizi AWS nativi del cloud. Potrebbero cambiare la modalità dell'account di pre-produzione dalla modalità RFC gestita da AMS alla modalità Developer gestita da AMS, offrendo loro la flessibilità e l'agilità necessarie per il provisioning dell'infrastruttura. Tuttavia, una volta apportate le modifiche al provisioning dell'infrastruttura utilizzando il «ruolo di sviluppatore», la stessa infrastruttura non può essere riportata alla modalità RFC gestita da AMS. Questo perché AMS non può garantire il funzionamento dell'infrastruttura fornita al di fuori del sistema di gestione delle modifiche AMS. I clienti potrebbero dover creare un nuovo account applicativo che offra la modalità RFC gestita da AMS e quindi ridistribuire la configurazione dell'infrastruttura «ottimizzata» tramite CloudFormation modelli o inserendola in modo personalizzato AMIs in un account gestito da AMS. Questo è un modo semplice per implementare una configurazione pronta per la produzione. Una volta implementata, l'applicazione sarà soggetta alla governance e alle operazioni

prescrittive di AMS. Lo stesso vale per il passaggio dalla modalità gestita dal cliente alla modalità gestita da AMS.

modalità RFC

La modalità RFC è la modalità predefinita per i clienti del piano operativo AMS Advanced. Include un sistema di gestione delle modifiche con richieste di modifica o RFCs un catalogo di tipi di modifica da utilizzare per richiedere l'aggiunta o la modifica di cui hai bisogno ai tuoi account. Questo sistema di gestione delle modifiche offre un livello di sicurezza nel limitare chi può apportare modifiche agli account.

Per dettagli sui tipi di modifica di AMS Advanced, consulta Cosa sono i tipi di modifica AMS? .

Per dettagli sull'onboarding in AMS Advanced, consulta AWS Managed Services Onboarding Introduction.

Per esempi di procedura dettagliata relativi al tipo di modifica, consulta la sezione «Informazioni aggiuntive» per il tipo di modifica pertinente nella sezione AMS Advanced Change Type Reference Change Types by Classification.

> **Note**
>
> La modalità RFC era precedentemente chiamata «modalità di gestione delle modifiche» o «modalità CM standard».

Argomenti

- Scopri di più RFCs
- Cosa sono i tipi di modifica?
- Risoluzione degli errori RFC in AMS

Scopri di più RFCs

Le richieste di modifica, oppure RFCs, funzionano in due modi. Innanzitutto, ci sono dei parametri richiesti per la RFC stessa. Queste sono le opzioni dell'`CreateRfc`API. In secondo luogo, ci sono parametri necessari per l'azione dell'RFC (i parametri di esecuzione). Per maggiori informazioni

sulle `CreateRfc` opzioni, consulta la CreateRfcsezione dell'AMS API Reference. Queste opzioni compaiono in genere nell'area Configurazioni aggiuntive delle pagine Crea RFC.

Puoi creare e inviare una RFC con l'`CreateRfc`API, la `aws amscm create-rfc` CLI o utilizzando la console AMS Crea pagine RFC. Per un tutorial sulla creazione di un RFC, vedi. Crea un RFC

Argomenti

- Cosa sono RFCs?
- Autenticazione quando si utilizza l'API/CLI AMS
- Comprendi le revisioni sulla sicurezza RFC
- Comprendi le classificazioni dei tipi di modifica RFC
- Comprendi gli stati di azione e attività della RFC
- Comprendi i codici di stato RFC
- Comprendi l'aggiornamento RFC CTs e il rilevamento della deriva dei CloudFormation modelli
- Pianificazione RFCs
- Approva o rifiuta RFCs
- Richiedi periodi di esecuzione con restrizioni RFC
- Crea, clona, aggiorna, trova e annulla RFCs
- Usa la console AMS con RFCs
- Scopri i parametri RFC più comuni
- Iscriviti all'e-mail quotidiana di RFC

Cosa sono RFCs?

Una richiesta di modifica, o RFC, è il modo in cui apporti una modifica al tuo ambiente gestito da AMS o chiedi ad AMS di apportare una modifica per tuo conto. Per creare un RFC, scegli tra i tipi di modifica AMS, scegli i parametri RFC (come la pianificazione), quindi invia la richiesta utilizzando la console AMS o i comandi API e. CreateRfcSubmitRfc

Un RFC contiene due specifiche, una per la RFC stessa e una per i parametri del tipo di modifica (CT). Nella riga di comando, è possibile utilizzare un comando RFC in linea o un CreateRfc modello standard in formato JSON, da compilare e inviare insieme al file di schema CT JSON creato (in base ai parametri CT). Il nome CT è una descrizione informale del CT. Un CSIO (categoria, sottocategoria, articolo, operazione) è una descrizione più formale di un CT. Quando si crea un RFC, è necessario specificare solo l'ID CT.

RFCs passano attraverso due fasi chiave: convalida ed esecuzione.

1. Nella fase di convalida, AMS esamina la richiesta RFC per verificarne la completezza e la correttezza. AMS valuta inoltre la richiesta di sicurezza in conformità con i nostri standard tecnici di sicurezza. AMS verifica che la modifica richiesta sia valida ed eseguibile.
2. Nella fase di esecuzione, AMS tenta di apportare le modifiche richieste all'account dell'utente.

AMS gestisce entrambe le fasi tramite un processo automatizzato, un processo manuale o una combinazione di entrambi. Il processo manuale è gestito dal team AMS Operations. Per ulteriori informazioni, consulta Automatizzato e manuale CTs.

AMS offre tre modalità di esecuzione per la gestione delle richieste:

- (Consigliato da AMS) Modalità di esecuzione: automatizzata. Queste CTs utilizzano l'automazione per le convalide e le esecuzioni RFC, che è il modo più rapido per raggiungere i risultati aziendali.
- (Consigliata da AMS) Modalità di esecuzione: manuale e designazione: automazione gestita. Questi CTs utilizzano una combinazione di processi automatizzati e manuali per le convalide e le esecuzioni RFC. Se l'automazione non è in grado di eseguire la modifica richiesta, la RFC viene trasferita (tramite routing automatico o mediante la creazione di una RFC sostitutiva) al team AMS Operations per la gestione manuale. L'invio di queste informazioni CTs consente una ricezione più strutturata della richiesta, integrata dall'automazione AMS per migliorare i tempi di gestione ed esecuzione.
- Modalità di esecuzione: manuale e designazione: revisione richiesta. Modifiche richieste tramite ct-1e1xtak34nx76 Management | Altro | Altro | Aggiornamento (revisione richiesta) o ct-0xdawir96cy7k Management | Altro | Altro | Crea (revisione richiesta). CTs Questi si basano sulla gestione manuale per le convalide e le esecuzioni. Questi CTs dipendono dall'interpretazione manuale della richiesta di modifica.

AMS ti avvisa quando la modifica è stata completata correttamente (Operazione riuscita) o meno (Errore).

> **Note**
>
> Per informazioni sulla risoluzione dei problemi relativi agli errori RFC, consulta. Risoluzione degli errori RFC in AMS

L'immagine seguente mostra il flusso di lavoro di una RFC inviata dall'utente.

Autenticazione quando si utilizza l'API/CLI AMS

Quando utilizzi l'API/CLI AMS, devi autenticarti con credenziali temporanee. Per richiedere credenziali di sicurezza temporanee per utenti federati GetFederationTokenAssumeRole, chiama AssumeRoleWithSAML o AssumeRoleWithWebIdentityAWS Security Token Service (STS). APIs

Una scelta comune è SAML. Dopo la configurazione, aggiungi un argomento a ogni operazione che chiami. Ad esempio: `aws --profile saml amscm list-change-type-categories`.

Una scorciatoia per i profili SAML 2.0 consiste nell'impostare la variabile di profilo all'inizio di ogni API/CLI comando `set AWS_DEFAULT_PROFILE=saml` (per Windows; per Linux lo sarebbe`export AWS_DEFAULT_PROFILE=saml`). Per informazioni sull'impostazione delle variabili di ambiente CLI, consulta Configurazione dell'interfaccia a riga di comando AWS, Variabili di ambiente.

Comprendi le revisioni sulla sicurezza RFC

Il processo di approvazione della gestione delle modifiche di AWS Managed Services (AMS) garantisce l'esecuzione di una revisione di sicurezza delle modifiche che apportiamo ai tuoi account.

AMS valuta tutte le richieste di modifica (RFCs) rispetto agli standard tecnici AMS. Qualsiasi modifica che possa ridurre il livello di sicurezza del tuo account deviando dagli standard tecnici viene sottoposta a una revisione di sicurezza. Durante la revisione di sicurezza, AMS evidenzia i rischi pertinenti e, in caso di rischio di sicurezza elevato o molto elevato, il personale di sicurezza autorizzato accetta o rifiuta la RFC. Tutte le modifiche vengono inoltre valutate per valutare l'impatto negativo sulla capacità operativa di AMS. Se vengono rilevati potenziali impatti negativi, sono necessarie ulteriori revisioni e approvazioni all'interno di AMS.

Standard tecnici AMS

Gli standard tecnici AMS definiscono i criteri, le configurazioni e i processi minimi di sicurezza per stabilire la sicurezza di base dei tuoi account. Questi standard devono essere rispettati sia da AMS che da voi.

Qualsiasi modifica che possa potenzialmente ridurre il livello di sicurezza del vostro account deviando dagli standard tecnici viene sottoposta a un processo di accettazione del rischio, in cui il rischio rilevante viene evidenziato da AMS e accettato o respinto dal personale di sicurezza autorizzato da

parte dell'utente. Tutte queste modifiche vengono inoltre valutate per valutare se potrebbero esserci ripercussioni negative sulla capacità di AMS di gestire l'account e, in tal caso, sono necessarie ulteriori revisioni e approvazioni all'interno di AMS.

Processo RFC di gestione del rischio di sicurezza dei clienti (CSRM)

Quando qualcuno della tua organizzazione richiede una modifica all'ambiente gestito, AMS esamina la modifica per determinare se la richiesta potrebbe peggiorare il livello di sicurezza del tuo account non rientrando negli standard tecnici. Se la richiesta riduce il livello di sicurezza dell'account, AMS comunica al team di sicurezza il rischio pertinente ed esegue la modifica; oppure, se la modifica introduce un rischio di sicurezza elevato o molto elevato nell'ambiente, AMS richiede l'approvazione esplicita del contatto del team di sicurezza sotto forma di accettazione del rischio (spiegato di seguito). Il processo AMS Customer Risk Acceptance è progettato per:

- Garantire che i rischi siano chiaramente identificati e comunicati ai legittimi proprietari
- Riducete al minimo i rischi identificati per l'ambiente
- Ottenete e documentate l'approvazione dei contatti di sicurezza designati che comprendono il profilo di rischio della vostra organizzazione
- Riduci i costi operativi continui per i rischi identificati

Come accedere agli standard tecnici e ai rischi elevati o molto elevati

Abbiamo reso disponibile la documentazione sugli standard tecnici AMS https://console.aws.amazon.com/artifact/come riferimento nel rapporto. Utilizzate la documentazione sugli standard tecnici AMS per capire se una modifica richieda l'accettazione del rischio da parte del vostro contatto di sicurezza autorizzato prima di inviare una richiesta di modifica (RFC).

Trova il rapporto sugli standard tecnici cercando «AWS Managed Services (AMS) Technical Standards» nella barra di ricerca della scheda AWS Artifact Rapporti dopo aver effettuato l'accesso con l'impostazione predefinita AWSManagedServicesChangeManagementRole.

> **Note**
>
> Il documento sullo standard tecnico AMS è accessibile per il Customer_ ReadOnly _Role nella landing zone con account singolo. Nella landing zone multiaccount, è possibile AWSManaged ServicesAdminRole utilizzare per accedere al documento quella AWSManaged ServicesChangeManagementRole utilizzata dagli amministratori della sicurezza e quella utilizzata dai team delle applicazioni. Se il tuo team utilizza un ruolo

personalizzato, crea un RFC Other | Other per richiedere l'accesso e aggiorneremo il ruolo personalizzato specificato.

Comprendi le classificazioni dei tipi di modifica RFC

I tipi di modifica utilizzati per inviare una RFC sono suddivisi in due grandi categorie:

- Distribuzione: questa classificazione serve per la creazione di risorse.
- Gestione: questa classificazione serve per l'aggiornamento o l'eliminazione delle risorse. La categoria Gestione contiene anche i tipi di modifica per l'accesso alle istanze, la crittografia o la condivisione e l'avvio AMIs, l'arresto, il riavvio o l'eliminazione degli stack.

Comprendi gli stati di azione e attività della RFC

`RfcActionState`(API)/Activity State (console) ti aiutano a comprendere lo stato dell'intervento o dell'azione umana su una RFC. Utilizzati principalmente a scopo manuale RFCs, ti `RfcActionState` aiutano a capire quando sono necessarie azioni da parte tua o delle operazioni AMS e ti aiuta a vedere quando AMS Operations sta lavorando attivamente sulla tua RFC. Ciò garantisce una maggiore trasparenza sulle azioni intraprese su una RFC durante il suo ciclo di vita.

`RfcActionState`Definizioni (API)/Activity State (console):

- AwsOperatorAssigned: Un operatore AWS sta lavorando attivamente alla tua RFC.
- AwsActionPending: è prevista una risposta o un'azione da parte di AWS.
- CustomerActionPending: È prevista una risposta o un'azione da parte del cliente.
- NoActionPending: non è richiesta alcuna azione da parte di AWS o del cliente.
- NotApplicable: questo stato non può essere impostato dagli operatori o dai clienti AWS e viene utilizzato solo per RFCs quelli creati prima del rilascio di questa funzionalità.

Gli stati di azione RFC variano a seconda che il tipo di modifica inviato richieda una revisione manuale e che la pianificazione sia impostata su ASAP o meno.

- ActionStateModifiche RFC durante la revisione, l'approvazione e l'avvio di un tipo di modifica manuale con pianificazione differita:
  - Dopo aver inviato una RFC manuale e pianificata, questa cambia ActionStateautomaticamente in modo da AwsActionPendingindicare che un operatore deve rivedere e approvare la RFC.

- Quando un operatore inizia a esaminare attivamente la tua RFC, la modifica diventa. ActionStateAwsOperatorAssigned
- Quando l'operatore approva la tua RFC, lo stato della RFC cambia in Pianificato e quindi cambia automaticamente in. ActionStateNoActionPending
- Quando viene raggiunta l'ora di inizio pianificata della RFC, lo stato RFC cambia in e cambia ActionStateautomaticamente per InProgressindicare che è necessario AwsActionPendingassegnare un operatore alla revisione della RFC.
- Quando un operatore inizia a utilizzare attivamente la RFC, cambia in. ActionStateAwsOperatorAssigned
- Una volta completata, l'operatore chiude la RFC. Questo cambia automaticamente in. ActionStateNoActionPending

Important

- Gli stati d'azione non possono essere impostati dall'utente. Vengono impostati automaticamente in base alle modifiche nella RFC o impostati manualmente dagli operatori AMS.
- Se si aggiunge corrispondenza a un RFC, ActionStateviene impostato automaticamente su. AwsActionPending
- Quando viene creata una RFC, viene impostata ActionStateautomaticamente su. NoActionPending
- Quando viene inviata una RFC, ActionStateviene automaticamente impostata su. AwsActionPending
- Quando una RFC viene rifiutata, annullata o completata con lo stato di Successo o Fallimento, ActionStateviene automaticamente reimpostata su. NoActionPending
- Gli stati di azione sono abilitati sia per quelli automatici che manuali RFCs, ma sono importanti soprattutto per quelli manuali, RFCs perché RFCs spesso questi tipi richiedono comunicazioni.

Esamina gli stati d'azione RFC, esempi di casi d'uso

Caso d'uso: visibilità sul processo RFC manuale

- Una volta inviata una RFC manuale, lo stato di azione RFC cambia automaticamente `AwsActionPending` per indicare che un operatore deve rivedere e approvare la RFC. Quando un operatore inizia a esaminare attivamente la tua RFC, lo stato di azione RFC cambia in. `AwsOperatorAssigned`
- Prendi in considerazione una RFC manuale che sia stata approvata e programmata e che sia pronta per iniziare a funzionare. Una volta che lo stato RFC cambia in`InProgress`, lo stato di azione RFC cambia automaticamente in. `AwsActionPending` Cambia nuovamente `AwsOperatorAssigned` quando un operatore inizia a eseguire attivamente la RFC.
- Quando viene completata una RFC manuale (chiusa come «Successo» o «Fallimento»), lo stato di azione RFC cambia `NoActionPending` per indicare che non sono necessarie ulteriori azioni da parte del cliente o dell'operatore.

Caso d'uso: corrispondenza RFC

- Se si utilizza una RFC manuale`Pending Approval`, un operatore AMS potrebbe aver bisogno di ulteriori informazioni da parte dell'utente. Gli operatori pubblicheranno una corrispondenza sulla RFC e modificheranno lo stato di azione RFC in. `CustomerActionPending` Quando rispondi aggiungendo una nuova corrispondenza RFC, lo stato di azione RFC cambia automaticamente in. `AwsActionPending`
- Quando una RFC automatica o manuale ha esito negativo, puoi aggiungere una corrispondenza ai dettagli RFC, chiedendo all'operatore AMS perché la RFC non è riuscita. Quando viene aggiunta la corrispondenza, lo stato di azione RFC viene impostato automaticamente su. `AwsActionPending` Quando l'operatore AMS preleva l'RFC per visualizzare la corrispondenza, lo stato di azione RFC cambia in. `AwsOperatorAssigned` Quando l'operatore risponde aggiungendo una nuova corrispondenza RFC, lo stato di azione RFC può essere impostato su, indicando che è prevista un'altra risposta da parte del cliente`CustomerActionPending`, oppure su`NoActionPending`, a indicare che non è necessaria o prevista alcuna risposta da parte del cliente.

Comprendi i codici di stato RFC

I codici di stato RFC ti aiutano a tenere traccia delle tue richieste. È possibile osservare questi codici di stato durante un'esecuzione RFC nell'output CLI o aggiornando la pagina dell'elenco RFC nella console.

Puoi anche vedere i codici di una RFC nella pagina dei dettagli di quella RFC, che potrebbe avere il seguente aspetto:

Nel tuo elenco potresti vedere una RFC che non hai inviato. Quando gli operatori AMS utilizzano una CT solo interna, la inviano in una RFC e la visualizzano nell'elenco RFC. Per ulteriori informazioni, consulta Tipi di modifiche solo interni.

> **Important**
>
> È possibile richiedere notifiche sulle modifiche dello stato RFC. Per i dettagli, consulta Notifiche di modifica dello stato RFC.

Codici di stato RFC

Completato	Errore
Modifica: la RFC è stata creata ma non inviata PendingApproval /Inviata: la RFC è stata inviata e il sistema sta determinando se richiede l'approvazione e sta ottenendo tale approvazione, se necessario Approvato da AWS /Approvato dal cliente: la RFC è stata approvata. RFCs Gli automatizzati sono approvati da AWS, RFCs i manuali sono approvati dagli operatori e, a volte, dai clienti Pianificato: la RFC ha superato i controlli della sintassi e dei requisiti ed è pianificata per l'esecuzione InProgress: la RFC è in corso di esecuzione, si noti che se si forniscono più risorse o RFCs che hanno tempi di esecuzione prolungati UserData, l'esecuzione richiede più tempo Eseguito: la RFC è stata eseguita	RFCs Rifiutati: vengono rifiutati in genere perché non superano la convalida; ad esempio, viene specificata una risorsa inutilizzabile, ad esempio una sottorete Annullate: RFCs vengono annullate in genere perché non superano la convalida prima che sia trascorsa l'ora di inizio configurata Fallimento: la richiesta RFC non è riuscita; consultate l' StatusReason output per eventuali motivi di errore e AMS Operations crea automaticamente una segnalazione di problemi e comunica con l'utente in base alle esigenze

Completato	Errore
Riuscito/Riuscito: la RFC è stata completata con successo	

> **Note**
>
> L'annullamento o il rifiuto RFCs possono essere inviati nuovamente utilizzando; vedi anche. UpdateRfcAggiorna RFCs

Se la RFC soddisfa tutte le condizioni necessarie (ad esempio, vengono specificati tutti i parametri obbligatori), lo stato cambia in `PendingApproval` (anche automatizzato CTs richiede l'approvazione, cosa che avviene automaticamente se i controlli della sintassi e dei parametri hanno esito positivo). Se non viene superato, lo stato diventa. `Rejected` `StatusReason`Fornisce informazioni sui rifiuti; i `ExecutionOutput` campi forniscono informazioni sull'approvazione e il completamento. I codici di errore includono:

- InvalidRfcStateException: Lo stato dell'RFC non consente l'operazione che è stata chiamata. Ad esempio, se la RFC è passata allo stato Inviato, non può più essere modificata.
- InvalidRfcScheduleException: I TimeoutInMinutes parametri StartTime EndTime, o sono stati violati.
- InternalServerError: è stata riscontrata una difficoltà con il sistema.
- InvalidArgumentException: Un parametro è specificato in modo errato; ad esempio, viene utilizzato un valore non accettabile.
- ResourceNotFoundException: Non è possibile trovare un valore, ad esempio l'ID dello stack.

Se gli orari di inizio e fine pianificati richiesti (noti anche come finestra di esecuzione delle modifiche) si verificano prima dell'approvazione della modifica, lo stato RFC cambia in. `Canceled` Se la modifica viene approvata, lo stato RFC diventa. `Scheduled` La finestra di esecuzione delle modifiche per ASAP RFCs è l'ora di invio più il `ExpectedExecutionDuration` valore per il CT.

In qualsiasi momento prima dell'arrivo della finestra di esecuzione delle modifiche, una modifica pianificata (inviata con una `RequestedStartTime` nella CLI) può essere modificata o annullata. Se la modifica pianificata viene modificata, deve essere inviata nuovamente.

Quando arriva l'ora di inizio della modifica (pianificata o il prima possibile) e dopo il completamento delle approvazioni, lo stato cambia `InProgress` e non è possibile apportare alcuna modifica. Se la modifica viene completata entro la finestra di esecuzione delle modifiche specificata, lo stato cambia in. `Success` Se una parte della modifica fallisce o se la modifica è ancora in corso al termine della finestra di esecuzione della modifica, lo stato cambia in`Failure`.

> **Note**
>
> Durante lo stato `InProgressSuccess`, o `Failure` change, la RFC non può essere modificata o annullata.

Il diagramma seguente illustra gli stati RFC dalla chiamata CreaterFC fino alla risoluzione.

Comprendi l'aggiornamento RFC CTs e il rilevamento della deriva dei CloudFormation modelli

Le risorse fornite in AMS utilizzano un modello modificato CloudFormation . Se un parametro di una risorsa viene modificato direttamente tramite la console di AWS gestione di un servizio, il record di CloudFormation creazione di tale risorsa non è sincronizzato. Se ciò accade e si tenta di utilizzare un tipo di modifica dell'aggiornamento AMS per aggiornare la risorsa in AMS, AMS fa riferimento alla configurazione originale della risorsa e potenzialmente ripristina i parametri modificati. Questo ripristino potrebbe essere dannoso, pertanto AMS non consente l'utilizzo di tipi di modifiche RFCs di aggiornamento se vengono rilevate ulteriori modifiche alla configurazione AMS.

Per un elenco dei tipi di modifiche agli aggiornamenti, usa il filtro della console.

Correzione della deriva FAQs

Domande e risposte sulla correzione della deriva da AMS. Esistono due tipi di modifica che è possibile utilizzare per avviare la correzione della deriva, uno è modalità di esecuzione=manuale o «automazione gestita», l'altro è modalità di esecuzione=automatizzata.

Risorse supportate per la bonifica del drift (ct-3kinq0u4l33zf)

Queste sono le risorse supportate dal tipo di modifica della correzione della deriva (ct-3kinq0u4l33zf). Per la riparazione di qualsiasi risorsa, utilizzate invece il tipo di modifica «managed automation» (ct-34sxfo53yuzah).

```
AWS::EC2::Instance
AWS::EC2::SecurityGroup
AWS::EC2::VPC
AWS::EC2::Subnet
AWS::EC2::NetworkInterface
AWS::EC2::EIP
AWS::EC2::InternetGateway
AWS::EC2::NatGateway
AWS::EC2::NetworkAcl
AWS::EC2::RouteTable
AWS::EC2::Volume
AWS::AutoScaling::AutoScalingGroup
AWS::AutoScaling::LaunchConfiguration
AWS::AutoScaling::LifecycleHook
AWS::AutoScaling::ScalingPolicy
AWS::AutoScaling::ScheduledAction
AWS::ElasticLoadBalancing::LoadBalancer
AWS::ElasticLoadBalancingV2::Listener
AWS::ElasticLoadBalancingV2::ListenerRule
AWS::ElasticLoadBalancingV2::LoadBalancer
AWS::CloudWatch::Alarm
```

Tipi di modifica per la correzione della deriva

Domande e risposte sull'utilizzo dei tipi di modifica della correzione della deriva di AMS.

Per un elenco delle risorse supportate per la funzione di correzione delle deviazioni, consulta. Risorse supportate per la bonifica del drift (ct-3kinq0u4l33zf)

Important

Drift remediation modifica i and/or parametri del modello di stack ed è obbligatorio aggiornare gli archivi di modelli locali o qualsiasi automazione che aggiorna questi stack per utilizzare il modello e i parametri di stack più recenti. L'utilizzo dei vecchi and/or parametri del modello senza sincronizzazione può causare modifiche dannose alle risorse sottostanti.
Il CT automatizzato e non gestito (ct-3kinq0u4l33zf) supporta la correzione di solo 10 risorse per RFC. Per ripristinare le risorse rimanenti in batch da 10, creane di nuove fino a quando tutte le risorse non saranno state riparate. RFCs

Quale tipo di modifica per la correzione della deriva devo utilizzare?

Consigliamo di utilizzare il CT automatico senza automazione gestita (ct-3kinq0u4l33zf) quando:

- Si tenta di eseguire un aggiornamento a una risorsa dello stack esistente utilizzando un CT automatico e la RFC viene rifiutata così come lo stack. `DRIFTED`
- Hai utilizzato un Update CT in passato e non è riuscito perché lo stack era DRIFTED. Non è necessario tentare nuovamente un aggiornamento, ma è possibile utilizzare invece l'automazione gestita, manuale, CT.

Si consiglia di utilizzare l'automazione gestita, CT manuale (ct-34sxfo53yuzah) solo quando i tipi di risorse alla deriva non sono supportati dalla correzione della deriva no managed automation, automatizzata, CT (ct-3kinq0u4l33zf) o quando la correzione della deriva no automazione gestita, automatizzata, CT fallisce.

Quali modifiche vengono apportate allo stack durante la riparazione?

La riparazione richiede aggiornamenti dei and/or parametri del modello dello stack a seconda delle proprietà modificate. La riparazione aggiorna inoltre la politica dello stack dello stack durante la riparazione e ripristina la politica dello stack al suo valore precedente una volta completata la riparazione.

Come possiamo vedere le modifiche apportate ai parametri del modello dello stack? and/or

Nella risposta alla RFC, viene fornito un riepilogo delle modifiche con le seguenti informazioni:

- `ChangeSummaryJson`: contiene un riepilogo delle modifiche ai and/or parametri dello Stack Template come parte della correzione della deriva. La riparazione viene eseguita in più fasi. Questo riepilogo delle modifiche comprende le modifiche relative alle singole fasi. Se la riparazione ha esito positivo, controlla le modifiche dell'ultima fase. Vedi ExecutionPlan nel JSON le fasi eseguite in ordine. Ad esempio, la RestoreReferences sezione, se presente, viene sempre eseguita alla fine e contiene JSON per le modifiche successive alla correzione. Se la riparazione viene eseguita in DryRun modalità, nessuna di queste modifiche sarebbe stata applicata allo stack.
- `PreRemediationStackTemplateAndConfigurationJson`: contiene un'istantanea della configurazione dello CloudFormation stack, tra cui Template, Parameters, Output, StackPolicyBody prima che la riparazione venisse attivata sullo stack.

Cosa devo fare una volta eseguita la riparazione?

> **Important**
>
> È necessario aggiornare gli archivi di modelli locali, o qualsiasi automazione, che aggiorni lo stack riparato, con il modello e i parametri più recenti forniti nel riepilogo RFC. È molto importante farlo perché l'utilizzo dei vecchi and/or parametri del modello può causare ulteriori modifiche distruttive sulle risorse dello stack.

La mia richiesta verrà effettuata durante questa correzione?

La riparazione è un processo offline che viene eseguito solo nella configurazione dello CloudFormation stack. Non viene eseguito alcun aggiornamento sulla risorsa sottostante.

Posso continuare a utilizzare Management | Other | Other RFCs per aggiornare le risorse dopo la riparazione?

Si consiglia di eseguire sempre gli aggiornamenti delle risorse dello stack utilizzando l'aggiornamento automatico disponibile. CTs Quando l'aggiornamento disponibile CTs non supporta il tuo caso d'uso, usa Gestione | Altro | Altre richieste.

La riparazione crea nuove risorse nello stack?

La riparazione non crea nuove risorse nello stack. Tuttavia, la correzione crea nuovi output e aggiorna la sezione dei metadati del modello di stack per archiviare il riepilogo della correzione come riferimento.

La riparazione avrà sempre successo?

La riparazione richiede un'attenta analisi e convalida della configurazione del modello per determinare se è possibile eseguirla. Negli scenari in cui queste convalide falliscono, il processo di riparazione viene interrotto e non viene apportata alcuna modifica al modello o ai parametri dello stack. Inoltre, la correzione può essere eseguita solo sui tipi di risorse supportati.

Come posso aggiornare le risorse dello stack se la riparazione non ha esito positivo?

È possibile utilizzare Management | Other | Other | Update CT (ct-0xdawir96cy7k) per richiedere modifiche. AMS monitora tali scenari e lavora per migliorare la soluzione di riparazione.

Posso rimediare a stack con tipi di risorse supportati e non supportati?

Sì. Tuttavia, la riparazione viene eseguita solo se i tipi di risorse supportati vengono trovati DRIFTED nello stack. Se alcuni tipi di risorse non supportati sono DRIFTED, la riparazione non continua.

Posso richiedere la riparazione per gli stack creati tramite un programma non CFN Ingest? CTs

Sì. La riparazione può essere eseguita sugli stack indipendentemente dal tipo di modifica utilizzato per creare lo stack.

Posso conoscere le modifiche che verrebbero apportate allo stack prima della riparazione?

Sì. Entrambi i tipi di modifiche offrono un'DryRunopzione che puoi utilizzare per richiedere modifiche che verrebbero eseguite se lo stack venisse corretto. Tuttavia, le modifiche correttive finali possono differire a seconda della deriva presente nello stack al momento della correzione.

Pianificazione RFCs

La funzione di pianificazione consente di scegliere un orario di inizio per. RFCs Le seguenti opzioni sono disponibili nella funzionalità di pianificazione:

- Esegui questa modifica il prima possibile: AMS esegue la RFC non appena viene approvata. La maggior parte CTs viene approvata automaticamente. Utilizza questa opzione se non desideri che la RFC inizi in un momento specifico.
- Pianifica questa modifica: imposta un giorno, un'ora e un fuso orario per l'esecuzione della RFC. Per i tipi di modifiche automatizzate, è consigliabile richiedere un'ora di inizio che sia almeno 10 minuti dopo la previsione di inviare la RFC. Per i tipi di modifica dell'automazione gestita, è necessario richiedere un'ora di inizio che sia di almeno 24 ore dopo la previsione di inviare la RFC. Se la RFC non viene approvata entro l'ora di inizio configurata, la RFC viene rifiutata.

Imposta una pianificazione RFC

Per pianificare una RFC, utilizzate uno dei seguenti metodi:

Esegui questa modifica il prima possibile:

- Console: non fare nulla. Viene utilizzata la pianificazione RFC predefinita.
- API o CLI: rimuovi le `RequestedEndTime` opzioni `RequestedStartTime` and nell'operazione Create RFC.

Le «automazioni gestite» ASAP RFCs vengono rifiutate automaticamente se non vengono approvate entro trenta giorni dall'invio.

Pianifica questa modifica:

- Console: seleziona il pulsante di opzione Pianifica questa modifica. Si apre un'area relativa all'ora di inizio. Digita manualmente un giorno o usa il widget del calendario per scegliere un giorno. Inserisci un'ora, in UTC, espressa in formato ISO 8601 e usa l'elenco a discesa per selezionare una località. Per impostazione predefinita, AMS utilizza il formato ISO 8601 Z YYYYMMDDThhmmss YYYY-MM-DDThh o:MM:SSZ, entrambi i formati sono accettati.

  > **Note**
  >
  > L'ora di fine predefinita è di 4 ore dall'ora di inizio inserita. Per impostare l'ora di fine della modifica pianificata oltre le 4 ore, utilizza l'API o la CLI per eseguire la modifica.

- API o CLI: invia i valori per i `RequestedEndTime` parametri `RequestedStartTime` and nell'operazione Create RFC. Il passaggio di un tipo di modifica configurato `RequestedEndTime` non interrompe l'esecuzione di un tipo di modifica automatica che è già stato avviato. Per un tipo di modifica di tipo «automazione gestita», se `RequestedEndTime` viene raggiunta mentre la ricerca di AMS Operations è ancora in corso e sei in contatto con AMS, puoi richiedere un'estensione o ti potrebbe essere chiesto di inviare nuovamente la RFC.

  > **Tip**
  >
  > Per un esempio di lettura dell'ora UTC, consulta UTC sul sito web Time-is. Esempio di formato ISO 8601 per un date/time valore del 05/12/2016 alle 14:20:2016-12-05T 14:20:00 Z o 20161205T142000Z.

Se fornisci...

- solo a`RequestedStartTime`, la RFC è considerata pianificata e `RequestedEndTime` viene compilata utilizzando il `ExecutionDurationInMinutes` valore.
- solo un`RequestedEndTime`, lanciamo un. InvalidArgumentException
- entrambi `RequestedStartTime` e`RequestedEndTime`, sovrascriviamo il `RequestedEndTime` con l'ora di inizio specificata più il `ExecutionDurationInMinutes` valore.

- né `RequestedStartTime` né`RequestedEndTime`, manteniamo tali valori come nulli e la RFC viene trattata come una RFC ASAP.

> **Note**
>
> Per tutte le pianificazioni RFCs, viene scritto che un'ora di fine non specificata corrisponde all'ora specificata `RequestedStartTime` più l'`ExpectedExecutionDurationInMinutes`attributo del tipo di modifica inviato. Ad esempio, se `ExpectedExecutionDurationInMinutes` è «60" (minuti) e il valore specificato `RequestedStartTime` è `2016-12-05T14:20:00Z` (5 dicembre 2016 alle 4:20), l'ora di fine effettiva sarà impostata sul 5 dicembre 2016 alle 5:20. Per trovare il tipo di modifica `ExpectedExecutionDurationInMinutes` per uno specifico, esegui questo comando:
>
> ```
> aws amscm --profile saml get-change-type-version --
> change-type-id CHANGE_TYPE_ID --query "ChangeTypeVersion.
> {ExpectedDuration:ExpectedExecutionDurationInMinutes}"
> ```

Usa l'opzione RFC Priority

Utilizzate l'opzione Priority nei tipi di `execution mode = manual` modifica per avvisare AMS Operations dell'urgenza della richiesta.

Opzione prioritaria in`execution mode = manual`:

Specificate la priorità di una RFC manuale come Alta, Media o Bassa. RFCs Le classificate come Alta vengono esaminate e approvate prima di essere RFCs classificate come Medium, in base agli obiettivi del livello di servizio RFC (SLOs) e ai relativi tempi di invio. RFCs con priorità bassa o nessuna priorità specificata vengono elaborati nell'ordine in cui vengono inviati.

Approva o rifiuta RFCs

RFCs la richiesta di approvazione (manuale) CTs deve essere approvata dall'utente o da AMS. Le approvazioni preliminari vengono elaborate automaticamente CTs . Per ulteriori informazioni, consulta Requisiti di approvazione CT.

> **Note**
>
> Quando si utilizza la CTs modalità manuale, AMS consiglia di utilizzare l'opzione ASAP Scheduling (scegliere ASAP nella console, lasciare vuote le date di inizio e fine nell'API/CLI) in quanto CTs richiedono che un operatore AMS esamini la RFC ed eventualmente comunichi con l'utente prima che possa essere approvata ed eseguita. Se li pianifichi RFCs, assicurati di attendere almeno 24 ore. Se l'approvazione non avviene prima dell'orario di inizio programmato, la RFC viene rifiutata automaticamente.

Se una RFC richiesta per l'approvazione viene inviata con successo da AMS, deve essere approvata esplicitamente dall'utente. Oppure, se invii una RFC richiesta per l'approvazione, questa deve essere approvata da AMS. Se ti viene richiesto di approvare una RFC inviata da AMS, ti verrà inviata un'e-mail o altra comunicazione predeterminata per richiedere l'approvazione. La comunicazione include l'ID RFC. Dopo l'invio della comunicazione, effettuate una delle seguenti operazioni:

- Approvazione o rifiuto della console: utilizza la pagina dei dettagli RFC per la RFC pertinente:

- Approvazione API/CLI: ApproveRfccontrassegna una modifica come approvata. L'azione deve essere intrapresa sia dal proprietario che dall'operatore, se entrambi sono necessari. Di seguito è riportato un esempio di comando CLI approve. Nell'esempio seguente, sostituisci RFC_ID con l'ID RFC appropriato.

  ```
  aws amscm approve-rfc --rfc-id RFC_ID
  ```

- API/CLI Reject: RejectRfccontrassegna una modifica come rifiutata. Di seguito è riportato un esempio di comando CLI reject. Nell'esempio seguente, sostituisci RFC_ID con l'ID RFC appropriato.

  ```
  aws amscm reject-rfc --rfc-id RFC_ID --reason "no longer relevant"
  ```

Richiedi periodi di esecuzione con restrizioni RFC

In precedenza noti come giorni di blackout, è possibile richiedere di limitare determinati periodi di tempo. Non è possibile eseguire alcuna modifica durante questi periodi.

Per impostare un periodo di esecuzione limitato, utilizza l'operazione UpdateRestrictedExecutionTimesAPI e imposta un periodo di tempo specifico, in UTC. Il periodo specificato ha la precedenza su tutti i periodi precedenti specificati. Se si invia una RFC durante il periodo di esecuzione limitato specificato, l'invio ha esito negativo e viene visualizzato l'errore Invalid RFC Schedule. È possibile specificare fino a 200 periodi di tempo limitati. Per impostazione predefinita, non è impostato alcun periodo limitato. Di seguito è riportato un esempio di comando di richiesta (con l'autenticazione SAML configurata):

```
aws amscm  --profile saml update-restricted-execution-times --restricted-execution-
times="[{\"TimeRange\":{\"StartTime\":\"2018-01-01T12:00:00Z\",\"EndTime\":
\"2018-01-01T12:00:01Z\"}}]"
```

Puoi anche visualizzare le tue RestrictedExecutionTimes impostazioni correnti eseguendo l'operazione ListRestrictedExecutionTimesAPI. Esempio:

```
aws amscm  --profile saml list-restricted-execution-times
```

Se desideri inviare una RFC durante un periodo di esecuzione limitato specificato, aggiungi il valore RestrictedExecutionTimesOverrideIdcon il valore di OverrideRestrictedTimeRangese invia la RFC come faresti normalmente. È consigliabile utilizzare questo metodo solo per una RFC critica o di emergenza. Per ulteriori informazioni, consulta il riferimento all'API per SubmitRfc.

Crea, clona, aggiorna, trova e annulla RFCs

Gli esempi seguenti illustrano varie operazioni RFC.

Argomenti

- Crea un RFC
- Clona RFCs (ricrea) con la console AMS
- Aggiorna RFCs
- Trova RFCs
- Annulla RFCs

Crea un RFC

Creazione di un RFC con la console

Quella che segue è la prima pagina del processo RFC Create nella console AMS, con Quick cards aperte e Browse change types attivi:

Quella che segue è la prima pagina del processo RFC Create nella console AMS, con Select by category attivo:

Come funziona:

1. Vai alla pagina Crea RFC: nel riquadro di navigazione a sinistra della console AMS, fai clic RFCsper aprire la pagina dell' RFCs elenco, quindi fai clic su Crea RFC.
2. Scegli un tipo di modifica (CT) popolare nella visualizzazione predefinita Sfoglia i tipi di modifica o seleziona un CT nella visualizzazione Scegli per categoria.
   - Naviga per tipo di modifica: puoi fare clic su un CT popolare nell'area di creazione rapida per aprire immediatamente la pagina Run RFC. Nota che non puoi scegliere una versione CT precedente con creazione rapida.

     Per ordinare CTs, utilizzate l'area Tutti i tipi di modifica nella vista a scheda o tabella. In entrambe le visualizzazioni, selezionate un CT, quindi fate clic su Crea RFC per aprire la pagina Esegui RFC. Se applicabile, accanto al pulsante Crea RFC viene visualizzata l'opzione Crea con una versione precedente.
   - Scegli per categoria: seleziona una categoria, sottocategoria, articolo e operazione e la casella dei dettagli CT si apre con l'opzione Crea con una versione precedente, se applicabile. Fai clic su Crea RFC per aprire la pagina Esegui RFC.
3. Nella pagina Run RFC, apri l'area del nome CT per visualizzare la casella dei dettagli CT. È richiesto un oggetto (questo campo viene compilato automaticamente se si sceglie il CT nella vista Sfoglia i tipi di modifica). Apri l'area di configurazione aggiuntiva per aggiungere informazioni sull'RFC.

   Nell'area di configurazione dell'esecuzione, utilizza gli elenchi a discesa disponibili o inserisci i valori per i parametri richiesti. Per configurare i parametri di esecuzione opzionali, aprite l'area di configurazione aggiuntiva.

4. Al termine, fate clic su Esegui. Se non sono presenti errori, viene visualizzata la pagina RFC creata correttamente con i dettagli RFC inviati e l'output iniziale di Run.
5. Apri l'area dei parametri di esecuzione per visualizzare le configurazioni inviate. Aggiorna la pagina per aggiornare lo stato di esecuzione RFC. Facoltativamente, annulla la RFC o creane una copia con le opzioni nella parte superiore della pagina.

Creazione di un RFC con la CLI

Come funziona:

1. Utilizzate Inline Create (emettete un `create-rfc` comando con tutti i parametri RFC e di esecuzione inclusi) o Template Create (create due file JSON, uno per i parametri RFC e uno per i parametri di esecuzione) ed emettete il `create-rfc` comando con i due file come input. Entrambi i metodi sono descritti qui.
2. Invia il `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con l'ID RFC restituito.

   Monitora il comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Per verificare la versione del tipo di modifica, usa questo comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> È possibile utilizzare qualsiasi `CreateRfc` parametro con qualsiasi RFC, indipendentemente dal fatto che faccia parte o meno dello schema per il tipo di modifica. Ad esempio, per ricevere notifiche quando lo stato RFC cambia, aggiungi questa riga `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` alla parte dei parametri RFC della richiesta (non ai parametri di esecuzione). Per un elenco di tutti i CreateRfc parametri, consulta l'AMS Change Management API Reference.

CREAZIONE IN LINEA:

Esegui il comando create RFC con i parametri di esecuzione forniti in linea (evita le virgolette quando fornisci i parametri di esecuzione in linea), quindi invia l'ID RFC restituito. Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

```
aws amscm create-rfc --change-type-id "CT_ID" --change-type-version "VERSION" --title
 "TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

CREAZIONE DEL MODELLO:

> **Note**
>
> Questo esempio di creazione di una RFC utilizza il tipo di modifica dello stack Load Balancer (ELB).

1. Trova il CT pertinente. Il comando seguente cerca nei riepiloghi delle classificazioni CT quelli che contengono «ELB» nel nome dell'elemento e crea l'output di Categoria, Articolo, Operazione e ChangeType ID sotto forma di tabella (la sottocategoria per entrambi è). `Advanced stack components`

   ```
   aws amscm list-change-type-classification-summaries --query
    "ChangeTypeClassificationSummaries[?contains(Item,'ELB')].
   [Category,Item,Operation,ChangeTypeId]" --output table
   ```

   ```
   ------------------------------------------------------------------------
   |                            CtSummaries                               |
   +-----------+---------------------------+---------------------------+
   | Deployment| Load balancer (ELB) stack | Create | ct-123h45t6uz7jl |
   | Management| Load balancer (ELB) stack | Update | ct-0ltm873rsebx9 |
   +-----------+---------------------------+---------------------------+
   ```

2. Trova la versione più recente del CT:

   `ChangeTypeIdeChangeTypeVersion`: L'ID del tipo di modifica per questa procedura dettagliata è `ct-123h45t6uz7jl` (create ELB). Per scoprire l'ultima versione, esegui questo comando:

   ```
   aws amscm list-change-type-version-summaries --filter
    Attribute=ChangeTypeId,Value=ct-123h45t6uz7jl
   ```

3. Scopri le opzioni e i requisiti. Il comando seguente genera lo schema in un file JSON denominato CreateElbParams .json.

```
aws amscm get-change-type-version --change-type-id "ct-123h45t6uz7jl" --query
 "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateElbParams.json
```

4. Modifica e salva il file JSON dei parametri di esecuzione. Questo esempio nomina il file CreateElbParams .json.

   Per un CT di provisioning, StackTemplateId è incluso nello schema e deve essere inviato nei parametri di esecuzione.

   Per TimeoutInMinutes quanti minuti sono consentiti per la creazione dello stack prima che la RFC fallisca, questa impostazione non ritarderà l'esecuzione della RFC, ma è necessario concedere tempo sufficiente (ad esempio, non specificare «5"). I valori validi sono compresi tra «60" e «360", per CT con esecuzione prolungata UserData: Create EC2 e Create ASG. Consigliamo il valore massimo consentito di «60" per tutti gli altri tipi di provisioning. CTs

   Fornisci l'ID del VPC in cui desideri creare lo stack; puoi ottenere l'ID VPC con il comando CLI. `aws amsskms list-vpc-summaries`

```
{
"Description":      "ELB-Create-RFC",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-sdhopv00000000000",
"Name":             "MyElbInstance",
"TimeoutInMinutes": 60,
"Parameters":   {
    "ELBSubnetIds":                     ["SUBNET_ID"],
    "ELBHealthCheckHealthyThreshold":   4,
    "ELBHealthCheckInterval":           5,
    "ELBHealthCheckTarget":             "HTTP:80/",
    "ELBHealthCheckTimeout":            60,
    "ELBHealthCheckUnhealthyThreshold": 5,
    "ELBScheme":                        false
    }
}
```

5. Esporta il modello JSON RFC in un file nella cartella corrente denominata .json: CreateElbRfc

```
aws amscm create-rfc --generate-cli-skeleton > CreateElbRfc.json
```

6. Modifica e salva il file.json. CreateElbRfc Poiché hai creato i parametri di esecuzione in un file separato, rimuovi la `ExecutionParameters` riga. Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

```
{
"ChangeTypeVersion":    "2.0",
"ChangeTypeId":         "ct-123h45t6uz7jl",
"Title":                "Create ELB"
}
```

7. Crea la RFC. Il comando seguente specifica il file dei parametri di esecuzione e il file modello RFC:

```
aws amscm create-rfc --cli-input-json file://CreateElbRfc.json --execution-
parameters file://CreateElbParams.json
```

   Nella risposta si riceve l'ID della nuova RFC e si può utilizzare per inviare e monitorare la RFC. Finché non la invii, la RFC rimane nello stato di modifica e non si avvia.

Suggerimenti

> **Note**
>
> È possibile utilizzare AMS API/CLI per creare un RFC senza creare un file JSON RFC o un file JSON dei parametri di esecuzione CT. Per fare ciò, si usa il `create-rfc` comando e si aggiungono i parametri RFC e di esecuzione richiesti al comando, questo si chiama «Inline Create». Si noti che tutti i provisioning CTs hanno contenuto all'interno del `execution-parameters` blocco un `Parameters` array con i parametri della risorsa. I parametri devono avere le virgolette separate da una barra rovesciata (\).
> L'altro metodo documentato per creare un RFC è chiamato «Template Create». Qui si crea un file JSON per i parametri RFC e un altro file JSON per i parametri di esecuzione e si inviano i due file con il comando. `create-rfc` Questi file possono fungere da modelli ed essere riutilizzati per future applicazioni. RFCs
> Quando si crea RFCs con modelli, è possibile utilizzare un comando per creare il file JSON con i contenuti desiderati emettendo un comando come illustrato. I comandi creano un file denominato «parameters.json» con il contenuto mostrato; puoi anche usare questi comandi per creare il file JSON RFC.

Clona RFCs (ricrea) con la console AMS

È possibile utilizzare la console AMS per clonare un RFC esistente.

Per clonare o ricreare un RFC utilizzando la console AMS, segui questi passaggi:

1. Trova la RFC pertinente. Dalla barra di navigazione a sinistra, fai clic su RFCs.

   Si apre la RFCs dashboard.
2. Scorri le pagine fino a trovare la RFC che desideri clonare. Usa l'opzione Filtro per restringere l'elenco. Scegliete l'RFC che volete clonare.

   Si apre la pagina dei dettagli RFC.
3. Fai clic su Crea una copia.

   Viene visualizzata la pagina Crea una richiesta di modifica con tutte le opzioni impostate come nella RFC originale.
4. Apporta le modifiche che desideri. Per impostare opzioni aggiuntive, modificate l'opzione Base in Avanzata. Dopo aver impostato tutte le opzioni, scegliete Invia.

   La pagina dei dettagli RFC attiva si apre con un nuovo ID RFC per l'RFC clonato e l'RFC clonato viene visualizzato nella dashboard RFC.

Aggiorna RFCs

È possibile inviare nuovamente una RFC che è stata rifiutata o che non è ancora stata inviata aggiornando la RFC e quindi inviandola o inviandola nuovamente. Tieni presente che la RFCs maggior parte viene rifiutata perché lo specificato `RequestedStartTime` è passato prima dell'invio o perché lo specificato non TimeoutInMinutes è adeguato per eseguire la RFC (poiché TimeoutInMinutes non prolunga una RFC di successo, consigliamo di impostarlo sempre su almeno «60" e fino a «360" per un gruppo Amazon o EC2 Amazon Auto EC2 Scaling con tempi di esecuzione prolungati). UserData Questa sezione descrive come utilizzare la versione CLI del `UpdateRfc` comando per aggiornare un RFC con un nuovo parametro RFC o nuovi parametri utilizzando JSON con stringhe o un file di parametri aggiornato.

Questo esempio descrive l'utilizzo della versione CLI dell' UpdateRfc API AMS (vedi Update RFC). Sebbene esistano tipi di modifica per l'aggiornamento di alcune risorse (DNS privato e pubblico, stack di bilanciamento del carico e configurazione delle patch agli stack), non esiste un CT per aggiornare una RFC.

Ti consigliamo di inviare un'operazione alla volta. UpdateRfc Se invii più aggiornamenti, ad esempio su uno stack DNS, il tentativo di aggiornamento del DNS contemporaneamente potrebbe fallire.

DATI RICHIESTI`RfcId`: L'RFC che stai aggiornando.

DATI FACOLTATIVI`ExecutionParameters`: A meno che tu non stia aggiornando un campo non obbligatorio, ad esempio`Description`, invierai parametri di esecuzione modificati per risolvere i problemi che hanno causato il rifiuto o l'annullamento della RFC. Tutti i valori non nulli inviati sovrascrivono tali valori nella RFC originale.

1. Trova la relativa RFC rifiutata o annullata, puoi usare questo comando (puoi sostituire il valore con): `Canceled`

   ```
   aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Rejected
   ```

2. Puoi modificare uno qualsiasi dei seguenti parametri RFC:

   ```
   {
       "Description": "string",
       "ExecutionParameters": "string",
       "ExpectedOutcome": "string",
       "ImplementationPlan": "string",
       "RequestedEndTime": "string",
       "RequestedStartTime": "string",
       "RfcId": "string",
       "RollbackPlan": "string",
       "Title": "string",
       "WorstCaseScenario": "string"}
   ```

   Esempio di comando che aggiorna il campo Descrizione:

   ```
   aws amscm update-rfc --description "AMSTestNoOpsActionRequired" --rfc-id "RFC_ID"
    --region us-east-1
   ```

   Esempio di comando che aggiorna il ExecutionParameters VpcId campo:

   ```
   aws amscm update-rfc  --execution-parameters "{\"VpcId\":\"VPC_ID\"}" --rfc-id
    "RFC_ID" --region us-east-1
   ```

Comando di esempio che aggiorna la RFC con un file di parametri di esecuzione che contiene gli aggiornamenti; vedi esempio di file di parametri di esecuzione nel passaggio 2 di: EC2 stack | Create:

```
aws amscm update-rfc --execution-parameters file://CreateEc2ParamsUpdate.json --
rfc-id "RFC_ID" --region us-east-1
```

3. Invia nuovamente la RFC utilizzando `submit-rfc` lo stesso ID RFC che hai utilizzato quando la RFC è stata creata per la prima volta:

   ```
   aws amscm submit-rfc --rfc-id RFC_ID
   ```

   Se la RFC ha esito positivo, non riceverai alcun messaggio di conferma o di errore sulla riga di comando.

4. Per monitorare lo stato della richiesta e visualizzare l'output di esecuzione, esegui il comando seguente.

   ```
   aws amscm get-rfc --rfc-id RFC_ID
   ```

Trova RFCs

Trova una richiesta di modifica (RFC) con la console

Per trovare una RFC utilizzando la console AMS, segui questi passaggi.

> **Note**
>
> Questa procedura si applica solo ai programmi pianificati RFCs, ovvero a coloro RFCs che non hanno utilizzato l'opzione ASAP.

1. Dalla barra di navigazione a sinistra, fai clic su RFCs.

   Si apre il RFCs pannello di controllo.

2. Scorri l'elenco o usa l'opzione Filtro per rifinire l'elenco.

   L'elenco RFC cambia in base ai criteri di filtro.

3. Scegli il link Oggetto per la RFC che desideri.

   Viene visualizzata la pagina dei dettagli della RFC relativa a tale RFC con informazioni tra cui l'ID RFC.

4. Se ce ne sono molti RFCs nella dashboard, puoi utilizzare l'opzione Filtro per cercare tramite RFC:

   - Oggetto: l'oggetto o il titolo (nell'API/CLI) assegnato alla RFC al momento della creazione.
   - ID RFC: l'identificatore della RFC.
   - Stato di attività: se conosci lo stato RFC, puoi scegliere se AwsOperatorAssignedsignificare che un operatore sta attualmente esaminando la RFC, AwsActionPendingovvero che un operatore AMS deve eseguire qualcosa prima che l'esecuzione RFC possa procedere o CustomerActionPendingche tu debba intraprendere qualche azione prima che l'esecuzione RFC possa procedere.
   - Stato: se conosci lo stato RFC, puoi scegliere tra:
     - Pianificato: RFCs erano programmati.
     - Annullato: sono stati RFCs annullati.
     - In corso: in corso. RFCs
     - Operazione riuscita: RFCs eseguita con successo.
     - RFCs Rifiutati: sono stati rifiutati.
     - Modifiche: RFCs che vengono modificate.
     - Fallimento: RFCs quello non è riuscito.
     - Approvazione in sospeso: RFCs non è possibile procedere fino all'approvazione da parte tua o di AMS. In genere, ciò indica che è necessario approvare la RFC. Avrai ricevuto una notifica di servizio in merito nell'elenco delle richieste di assistenza.
   - Tipo di modifica: seleziona la categoria, la sottocategoria, l'articolo e l'operazione e l'ID del tipo di modifica verrà recuperato automaticamente.
   - Ora di inizio richiesta o Ora di fine richiesta: questa opzione di filtro consente di scegliere Prima o Dopo, quindi inserire una data e, facoltativamente, un'ora (hh:mm e fuso orario). Questo filtro funziona correttamente solo in base alla pianificazione RFCs (non al più presto). RFCs
   - Stato: Pianificato, Annullato, In corso, Operativo riuscito, Rifiutato, Modificato o Non riuscito.
   - Oggetto: l'oggetto (o il titolo, se la RFC è stata creata con l'API/CLI) che hai fornito alla RFC.
   - ID del tipo di modifica: utilizza l'identificatore per il tipo di modifica inviato con la RFC.

La ricerca consente di aggiungere i filtri, come mostrato nella schermata seguente.

5. Fai clic sul link Oggetto della RFC che desideri.

   Si apre la pagina dei dettagli della RFC relativa a tale RFC con informazioni tra cui l'ID RFC.

Individuazione di una richiesta di modifica (RFC) con la CLI

Puoi utilizzare più filtri per trovare una RFC.

Per verificare la versione del tipo di modifica, usa questo comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> È possibile utilizzare qualsiasi `CreateRfc` parametro con qualsiasi RFC, indipendentemente dal fatto che faccia parte o meno dello schema per il tipo di modifica. Ad esempio, per ricevere notifiche quando lo stato RFC cambia, aggiungi questa riga `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` alla parte dei parametri RFC della richiesta (non ai parametri di esecuzione). Per un elenco di tutti i CreateRfc parametri, consulta l'AMS Change Management API Reference.

Se non scrivi l'ID RFC e hai bisogno di trovarlo in un secondo momento, puoi utilizzare il sistema di gestione delle modifiche AMS (CM) per cercarlo e restringere i risultati con un filtro o una query.

1. Il ListRfcSummariesfunzionamento dell'API CM dispone di filtri. È possibile filtrare i risultati in base a `Attribute` e `Value` combinati in un'operazione AND logica oppure in base a un `AttributeCondition`, a `eValues`.

Filtraggio RFC

Attributo	Valori validi	Condizioni valide	Condizione predefinita	Note
ActualEndTime	Qualsiasi stringa che rappresenta una ISO8601 data e ora (ad esempio, «20170101T000000Z»)	Prima, dopo, tra	Nessuno	La condizione Prima o Dopo accetta solo un valore nel campo Valori. La condizione Between deve avere esattamente due valori nel campo Valori, dove il primo valore deve rappresentare una data precedente al secondo valore
ActualStartTime	Qualsiasi stringa che rappresenta una ISO8601 data e ora (ad esempio, «20170101T000000Z»)	Prima, dopo, tra	Nessuno	La condizione Prima o Dopo accetta solo un valore nel campo Valori. La condizione Between deve avere esattamente due valori nel campo Valori, dove il primo valore deve rappresentare una data precedente al secondo valore
AutomationStatusId	Manuale, automatizzato	Equals	Equals	Esistono solo due stati di automazione

Attributo	Valori validi	Condizioni valide	Condizione predefinita	Note
ChangeTypeId	Qualsiasi ID del tipo di modifica valido, ad esempio ct-123h45t6uz7jl	Equals	Equals	Individuazione di un tipo di modifica o CSIO
ChangeTypeVersion	Qualsiasi ID del tipo di modifica valido, ad esempio 1.0	Equals	Equals	Individuazione di un tipo di modifica o CSIO
CreatedBy	Qualsiasi stringa (la lunghezza massima consentita è di 2048 caratteri)	Contiene	Contiene	Il CreatedBy campo della RFC contiene l'ARN dell'utente che lo ha creato
CreatedTime	Qualsiasi stringa che rappresenta una ISO8601 data e ora (ad esempio, «20170101T000000Z»)	Prima, dopo, tra	Nessuno	La condizione Prima o Dopo accetta solo un valore nel campo Valori. La condizione Between deve avere esattamente due valori nel campo Valori, dove il primo valore deve rappresentare una data precedente al secondo valore

Attributo	Valori validi	Condizioni valide	Condizione predefinita	Note
LastModifiedTime	Qualsiasi stringa che rappresenta una ISO8601 data e ora (ad esempio, «20170101T000000Z»)	Prima, dopo, tra	Nessuno	La condizione Prima o Dopo accetta solo un valore nel campo Valori. La condizione Between deve avere esattamente due valori nel campo Valori, dove il primo valore deve rappresentare una data precedente al secondo valore
LastSubmittedTime	Qualsiasi stringa che rappresenta una ISO8601 data e ora (ad esempio, «20170101T000000Z»)	Prima, dopo, tra	Nessuno	La condizione Prima o Dopo accetta solo un valore nel campo Valori. La condizione Between deve avere esattamente due valori nel campo Valori, dove il primo valore deve rappresentare una data precedente al secondo valore

Attributo	Valori validi	Condizioni valide	Condizione predefinita	Note
RequestedEndTime	Qualsiasi stringa che rappresenta una ISO8601 data e ora (ad esempio, «20170101T000000Z»)	Prima, dopo, tra	Nessuno	La condizione Prima o Dopo accetta solo un valore nel campo Valori. La condizione Between deve avere esattamente due valori nel campo Valori, dove il primo valore deve rappresentare una data precedente al secondo valore
RequestedStartTime	Qualsiasi stringa che rappresenta una ISO8601 data e ora (ad esempio, «20170101T000000Z»)	Prima, dopo, tra	Nessuno	La condizione Prima o Dopo accetta solo un valore nel campo Valori. La condizione Between deve avere esattamente due valori nel campo Valori, dove il primo valore deve rappresentare una data precedente al secondo valore
RfcStatusId	Annullato, Modifica, Errore,,, Rifiutato InProgress, Pianificato PendingApproval, Operato con successo	Equals	Equals	Aggiorna l'elenco RFC nella console AMS o esegui GetRfc

Attributo	Valori validi	Condizioni valide	Condizione predefinita	Note
Titolo	Qualsiasi titolo RFC valido	Contiene	Contiene	Le espressioni regolari in ogni singolo campo non sono supportate. Ricerca senza distinzione tra lettere maiuscole

Esempi:

Per trovare tutto ciò che RFCs riguarda SQS (dove SQS è contenuto nella parte Item del CT), puoi usare questo comando: IDs

```
list-rfc-summaries --query 'RfcSummaries[?contains(Item.Name,`SQS`)].
[Category.Id,Subcategory.Id,Type.Id,Item.Id,RfcId]' --output table
```

Il che restituisce qualcosa del genere:

```
-------------------------------------------------------------------------
|                          ListRfcSummaries                             |
+----------+---------------------------------+-------+-------+----------------+
|Deployment| Advanced Stack Components      |SQS    |Create |ct-123h45t6uz7jl|
|Management| Monitoring & Notification  |SQS    |Update |ct-123h45t6uz7jl|
+----------+---------------------------------+-------+-------+----------------+
```

Un altro filtro disponibile `list-rfc-summaries` è`AutomationStatusId`, da cercare RFCs , automatizzato o manuale:

```
aws amscm list-rfc-summaries --filter Attribute=AutomationStatusId,Value=Automated
```

Un altro filtro disponibile per `list-rfc-summaries` è `Title` (Oggetto nella console):

```
Attribute=Title,Value=RFC-TITLE
```

Esempio della nuova struttura di richiesta in JSON che restituisce RFCs dove:

- (Il titolo CONTIENE la frase «Windows 2012" O «Amazon Linux») E
- (È RfcStatusId UGUALE A «Successo» O "«) E InProgress
- (20170101T000000Z <= <= 20170103T000000Z) E (<= 20170103T000000Z) RequestedStartTime ActualEndTime

```
{
  "Filters": [
    {
      "Attribute": "Title",
      "Values": ["Windows 2012", "Amazon Linux"],
      "Condition": "Contains"
    },
    {
      "Attribute": "RfcStatusId",
      "Values": ["Success", "InProgress"],
      "Condition": "Equals"
    },
    {
      "Attribute": "RequestedStartTime",
      "Values": ["20170101T000000Z", "20170103T000000Z"],
      "Condition": "Between"
    },
    {
      "Attribute": "ActualEndTime",
      "Values": ["20170103T000000Z"],
      "Condition": "Before"
    }
  ]
}
```

> **Note**
>
> Con versioni più avanzate, AMS `Filters` intende rendere obsoleti i seguenti campi in una prossima versione:

- Valore: il campo Valore fa parte del campo Filtri. Utilizza il campo Valori che supporta funzionalità più avanzate.
- RequestedEndTimeRange: utilizza l' RequestedEndTime interno del campo Filtri che supporta funzionalità più avanzate
- RequestedStartTimeRange: Utilizza l' RequestedStartTime interno del campo Filtri che supporta funzionalità più avanzate.

Per informazioni sull'utilizzo delle query CLI, vedere Come filtrare l'output con l'opzione --query e il riferimento al linguaggio di interrogazione, Specificazione. JMESPath

2. Se utilizzi la console AMS:

   Vai alla pagina dell'RFCselenco. Se necessario, puoi filtrare in base all'oggetto RFC, che è quello che hai inserito come RFC al `Title` momento della creazione.

Suggerimenti

> **Note**
>
> Questa procedura si applica solo ai programmi programmati RFCs, ovvero a quelli RFCs che non hanno utilizzato l'opzione ASAP.

Annulla RFCs

È possibile annullare una RFC utilizzando la console o l'API/CLI AMS.

Per annullare una RFC con la console, individua la RFC nell'elenco RFC, aprila e fai clic su Annulla.

Dati richiesti:

- `Reason`: Perché stai annullando la RFC.
- `RfcId`: La RFC che stai annullando.

1. In genere si annulla una RFC subito dopo averla inviata (quindi l'ID RFC dovrebbe essere a portata di mano); in caso contrario, non sarebbe possibile annullarla a meno che non sia stata pianificata prima dell'ora di inizio specificata. Se hai bisogno di trovare l'ID RFC, puoi

usare questo comando (puoi sostituirlo `Value` con un RFC `PendingApproval` approvato manualmente):

```
aws amscm list-rfc-summaries --filter Attribute=RfcStatusId,Value=Scheduled
```

2. Esempio di comando per annullare un RFC:

```
aws amscm cancel-rfc --reason "Bad Stack ID" --rfc-id "RFC_ID" --profile saml --
region us-east-1
```

Usa la console AMS con RFCs

La console AMS offre funzionalità che ti aiutano a creare e inviare RFCs con successo.

Usa la pagina RFC List (Console)

La pagina con l'RFCselenco delle console AMS offre le seguenti opzioni:

- Ricerca RFC avanzata tramite un filtro. Per informazioni, consulta Trova RFCs.
- Ricerca dell'ultima volta che la RFC è stata modificata. Questo valore rappresenta l'ultima volta che lo stato RFC è stato modificato.
- Visualizzazione dei dettagli RFC con l'oggetto RFC. Scegliendo questo link si apre la pagina dei dettagli di quella RFC.
- Visualizzazione dello stato RFC. Per informazioni, consultare, Comprendi i codici di stato RFC

Usa la creazione rapida RFC (console)

Usa la creazione rapida di schede RFC o la tabella degli elenchi oppure scegli i tipi di modifica in RFCs base alla classificazione.

Per ulteriori informazioni, consulta Crea un RFC.

Aggiungi corrispondenza e allegati RFC (console)

È possibile aggiungere corrispondenza a una RFC dopo che è stata inviata e prima dell'approvazione, ad esempio mentre è nello stato "». PendingApproval Dopo l'approvazione di una RFC (nello stato «Programmato» o "InProgress«), la corrispondenza non può essere aggiunta,

poiché potrebbe essere interpretata come una modifica alla richiesta. Una volta completata una RFC (nello stato «Annullato», «Rifiutato», «Successo» o «Errore»), la corrispondenza viene nuovamente abilitata, anche se la corrispondenza viene disattivata quando una RFC viene chiusa per più di 30 giorni.

> **Note**
>
> Ogni corrispondenza è limitata a 5.000 caratteri.

Limitazioni per gli allegati:

- Solo tre allegati per corrispondenza.
- Limite di cinquanta allegati per RFC.
- Ogni allegato deve avere una dimensione inferiore a 5 MB.
- Sono accettati solo file di testo come testo in chiaro (`.txt`), valori separati da virgole (`.csv`), JSON () o YAML (`.json`). `.yaml` Nel caso del formato YAML, il file deve essere allegato utilizzando l'estensione del file. `.yaml`

  > **Note**
  >
  > I file di testo con contenuto XML sono proibiti. Se hai contenuti XML da condividere con AMS, utilizza una richiesta di servizio.

- I nomi dei file sono limitati a 255 caratteri, con solo numeri, lettere, spazi, trattini (-), caratteri di sottolineatura (_) e punti (.).
- L'aggiornamento e l'eliminazione degli allegati su un RFC non sono attualmente supportati.

Per aggiungere corrispondenza e allegati a una RFC, procedi nel seguente modo:

1. Nella console AMS, nella pagina dei dettagli RFC di una RFC, trova la sezione Corrispondenza in fondo alla pagina.

   Prima di qualsiasi corrispondenza:

   Dopo un po' di corrispondenza:

2. Per aggiungere una nuova corrispondenza, digita il messaggio nella casella di testo Rispondi. Per allegare file relativi alla corrispondenza, scegli Aggiungi allegato, quindi scegli i file che desideri.

3. Quando hai finito, scegli Invia.

   La nuova corrispondenza, insieme ai collegamenti ai file allegati, viene visualizzata nell'elenco delle corrispondenze nella pagina dei dettagli RFC.

Configurazione delle notifiche e-mail RFC (console)

La pagina di creazione di Requests for Change della console AMS offre la possibilità di aggiungere indirizzi e-mail per ricevere notifiche sulle modifiche dello stato RFC:

Inoltre, puoi aggiungere indirizzi e-mail per le notifiche relative a qualsiasi tipo di modifica, ad esempio:

```
aws amscm create-rfc --change-type-id <Change type ID>
                     --change-type-version 1.0 --title "TITLE"
                     --notification "{\"Email\": {\"EmailRecipients\" :
 [\"email@example.com\"]}}"
```

Aggiungi una riga (`--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"`) simile a qualsiasi tipo di modifica in linea o richiesta di modello nella parte dei parametri RFC della richiesta, non nella parte dei parametri.

Scopri i parametri RFC più comuni

Di seguito sono riportati i parametri RFC che è necessario inviare e i parametri comunemente utilizzati in: RFCs

- Informazioni sul tipo di modifica: ChangeTypeId e ChangeTypeVersion. Per un elenco del tipo di modifica IDs e dei numeri di versione, consulta Change Type Reference.

  Esegui `list-change-type-classification-summaries` nella CLI con l'`query`argomento per restringere i risultati. Ad esempio, restringi i risultati per modificare i tipi che contengono «Access» nel `Item` nome.

```
aws amscm list-change-type-classification-summaries --query
 "ChangeTypeClassificationSummaries [?contains (Item, 'access')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

Esegui `get-change-type-version` e specifica l'ID del tipo di modifica. Il comando seguente ottiene la versione CT per ct-2tylseo8rxfsc.

```
aws amscm get-change-type-version --change-type-id ct-2tylseo8rxfsc
```

- Titolo: Un nome per la RFC; questo diventa l'oggetto della RFC nell'elenco RFC della console AMS ed è possibile cercarlo con il comando e un filtro su `GetRfc` `Title`
- Pianificazione: se desideri una RFC pianificata, devi includere i `RequestedEndTime` parametri `RequestedStartTime` and o utilizzare l'opzione Pianifica questa modifica della console. Per un RFC ASAP (che viene eseguito non appena viene approvato), quando si utilizza la CLI, leave e null. `RequestedStartTime` `RequestedEndTime` Quando usi la console, accetta l'opzione ASAP.

  Se `RequestedStartTime` viene omesso, la RFC viene rifiutata.
- Fornitura CTs: i parametri di esecuzione o `Parameters` le impostazioni specifiche necessarie per il provisioning della risorsa. Essi variano notevolmente a seconda del CT.
- Mancato provisioning CTs: quelli CTs che non forniscono una risorsa, come access CTs o Other | Other, o delete stack, hanno parametri di esecuzione minimi e nessun blocco. `Parameters`
- Alcuni richiedono RFCs anche che si specifichi uno `TimeoutInMinutes` o quanti minuti sono consentiti per la creazione dello stack prima che la RFC fallisca. I valori validi sono da 60 (minuti) a 360, per le esecuzioni a lungo termine. UserData Se l'esecuzione non può essere completata prima del superamento del `TimeoutInMinutes` limite, la RFC fallisce. Tuttavia, questa impostazione non ritarda l'esecuzione della RFC.
- RFCs che creano istanze, come un bucket S3 o un ELB, generalmente forniscono uno schema che consente di aggiungere fino a sette tag (coppie chiave/valore). Puoi aggiungere altri tag al tuo bucket S3 inviando una RFC utilizzando Deployment | Advanced stack components | Tag | Create change type (ct-3cx7we852p3af). EC2, EFS, RDS e gli schemi a più livelli (HA a due livelli e HA a un livello) consentono fino a cinquanta tag. I tag sono specificati nella parte dello schema. `ExecutionParameters` Fornire tag può essere di grande utilità. Per ulteriori informazioni, consulta Tagging Your Amazon EC2 Resources.

Quando si utilizza la console AMS, è necessario aprire l'area di configurazione aggiuntiva per aggiungere tag.

> **Tip**
>
> Molti schemi CT hanno un `Name` campo `Description` and nella parte superiore dello schema. Questi campi vengono utilizzati per denominare lo stack o il componente dello stack, non la risorsa che stai creando. Alcuni schemi offrono un parametro per denominare la risorsa che stai creando, altri no. Ad esempio, lo schema CT per Create EC2 stack non offre un parametro per denominare l' EC2 istanza. Per fare ciò, devi creare un tag con la chiave «Nome» e il valore di quello che vuoi che sia il nome. Se non crei un tag di questo tipo, l' EC2 istanza viene visualizzata nella EC2 console senza un attributo name.

Utilizza l'opzione RFC AWS Region

L'API AMS e gli endpoint CLI (`amscmeamsskms`) sono attivi. `us-east-1` Se esegui la federazione con Security Assertion Markup Language (SAML), al momento dell'onboarding ti verranno forniti degli script che impostano la tua regione su us-east-1. AWS Se si utilizza SAML, non è necessario specificare l'opzione quando si impartisce un comando. `--region` Se il tuo SAML è configurato per utilizzare us-east-1 ma il tuo account non si trova in AWS quella regione, devi specificare la regione di registrazione dell'account quando impartisci altri comandi (ad esempio,). AWS `aws s3`

> **Note**
>
> La maggior parte degli esempi di comandi forniti in questa guida non include l'opzione. `--region`

Iscriviti all'e-mail quotidiana di RFC

Puoi registrarti per ricevere un'e-mail giornaliera che riepiloga l'attività RFC del tuo account nelle ultime 24 ore utilizzando la funzione RFC digest. La funzione RFC digest è un processo semplificato che riduce il numero di notifiche e-mail che ricevi relative al tuo account. RFCs Il digest RFC potrebbe ridurre la probabilità che tu perda azioni in attesa di risposta.

Per attivare la funzione RFC Digest, contatta il tuo AMS Cloud Service Delivery Manager (CSDM). Il CSDM ti sottoscrive. Puoi richiedere fino a 20 indirizzi e-mail (o alias) da includere nella tua mailing list di RFC Digest. L'attuale pianificazione delle e-mail è fissata alle 09:00 UTC-8.

Per disattivare la funzione RFC Digest, contatta il tuo CSDM con la tua richiesta.

Se non hai configurato RFC digest e desideri ricevere notifiche relative a te RFCs oppure se desideri informazioni più dettagliate su di te RFCs rispetto a quelle fornite dal digest RFC, utilizza il Change Management System per impostare notifiche di CloudWatch eventi o notifiche e-mail per ogni singolo RFC su cui desideri informazioni. Per informazioni sulla configurazione delle notifiche RFC, consulta RFC State Change Notifications.

Gli argomenti contenuti nel digest RFC includono quanto segue:

- In attesa di approvazione da parte del cliente: elenchi RFCs con PendingApprovallo stato attuale, in attesa di approvazione da parte dell'utente
- In attesa di risposta da parte del cliente: elenchi RFCs in attesa di risposta nella corrispondenza RFC
- In attesa di approvazione o risposta da AWS: elenchi RFCs in attesa di risposta o approvazione da parte di AMS
- Completato: elenchi RFCs con stato di successo, non riuscito, annullato e rifiutato

Di seguito è riportato un esempio di digest RFC:

Cosa sono i tipi di modifica?

Il tipo di modifica si riferisce all'azione eseguita da una richiesta di modifica (RFC) di AWS Managed Services (AMS) e comprende l'azione di modifica stessa e il tipo di modifica: manuale o automatizzata. AMS dispone di un'ampia raccolta di tipi di modifiche non utilizzati da altri servizi web Amazon. Utilizzi questi tipi di modifica quando invii una richiesta di modifica (RFC) per distribuire, gestire o accedere a risorse.

Argomenti

- Automatizzato e manuale CTs
- Requisiti di approvazione CT
- Cambia tipo di versioni

- Creare tipi di modifica
- Aggiorna i tipi di modifica
- Tipi di modifiche solo interni
- Cambia gli schemi dei tipi
- Gestione delle autorizzazioni per i tipi di modifica
- Oscurazione di informazioni sensibili dai tipi di modifiche
- Ricerca di un tipo di modifica, utilizzando l'opzione di interrogazione

Automatizzato e manuale CTs

Un vincolo sui tipi di modifica è che siano automatici o manuali, questo è l'`AutomationStatusId`attributo change type, chiamato modalità di esecuzione nella console AMS.

I tipi di modifica automatizzata hanno i risultati e i tempi di esecuzione previsti e vengono eseguiti attraverso il sistema automatizzato AMS, in genere entro un'ora o meno (ciò dipende in gran parte dalle risorse che il CT fornisce). I tipi di modifica manuale sono rari, ma vengono trattati in modo diverso perché richiedono che un operatore AMS agisca sulla RFC prima che questa possa essere eseguita. A volte ciò significa comunicare con il mittente della RFC, pertanto i tipi di modifica manuale richiedono tempi diversi per essere completati.

Per tutti gli orari programmati RFCs, viene scritto che un'ora di fine non specificata corrisponde all'ora specificata `RequestedStartTime` più l'attributo del tipo di modifica inviato. `ExpectedExecutionDurationInMinutes` Ad esempio, se `ExpectedExecutionDurationInMinutes` è «60" (minuti) e il valore specificato `RequestedStartTime` è `2016-12-05T14:20:00Z` (5 dicembre 2016 alle 4:20), l'ora di fine effettiva sarà impostata sul 5 dicembre 2016 alle 5:20. Per trovare il tipo di modifica `ExpectedExecutionDurationInMinutes` per uno specifico, esegui questo comando:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

> **Note**
>
> Pianificato RFCs con modalità di esecuzione = Manuale, nella console, deve essere impostato per funzionare per almeno 24 ore nelle future settimane.

> **Note**
>
> Quando si utilizza la CTs modalità manuale, AMS consiglia di utilizzare l'opzione ASAP Scheduling (scegliere ASAP nella console, lasciare vuote le date di inizio e fine nell'API/CLI) in quanto CTs richiedono che un operatore AMS esamini la RFC ed eventualmente comunichi con l'utente prima che possa essere approvata ed eseguita. Se li pianifichi RFCs, assicurati di attendere almeno 24 ore. Se l'approvazione non avviene prima dell'orario di inizio programmato, la RFC viene rifiutata automaticamente.

AMS intende rispondere a una TAC manuale entro quattro ore e risponderà il prima possibile, ma potrebbe essere necessario molto più tempo prima che la RFC venga effettivamente eseguita.

Per un elenco di quelli CTs che sono manuali e richiedono la revisione da parte di AMS, consulta il file CSV Change Type, disponibile nella pagina Developer's Resources della console.

YouTube Video: Come posso trovare tipi di modifiche automatiche per AMS RFCs?

Per trovare la modalità di esecuzione per un CT nella console AMS, è necessario utilizzare l'opzione di ricerca Sfoglia i tipi di modifica. I risultati mostrano la modalità di esecuzione del tipo o dei tipi di modifica corrispondenti.

Per trovare un tipo di modifica specifico utilizzando la CLI AMS, esegui questo comando: `AutomationStatus`

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

Puoi anche cercare i tipi di modifica nell'AMS Change Type Reference, che fornisce informazioni su tutti i tipi di modifica AMS.

> **Note**
>
> API/CLI Gli AMS non fanno attualmente parte di AWSAPI/CLI. To access the AMS API/CLI, è possibile scaricare l'SDK AMS tramite la console AMS.

Requisiti di approvazione CT

AMS prevede CTs sempre due condizioni di approvazione, AwsApprovalIdCustomerApprovalIdche indicano se la RFC richiede ad AMS o all'utente o a chiunque altro di approvare l'esecuzione.

La condizione di approvazione è in qualche modo correlata alla modalità di esecuzione; per i dettagli, vedere. Automatizzato e manuale CTs

Per scoprire le condizioni di approvazione per un CT, puoi consultare l'AMS Change Type Reference o eseguire GetChangeTypeVersion. Entrambi ti offriranno anche la modalità CT **`AutomationStatusId`** o Execution.

Puoi approvare RFCs utilizzando la console AMS o con il seguente comando:

```
aws amscm approve-rfc --rfc-id RFC_ID
```

Condizione di approvazione CT

Se la condizione di approvazione CT è	Richiede l'approvazione di	And
`AwsApprovalId: Required`	Il sistema AMS cambia tipo,	Nessuna operazione richiesta. Questa condizione è tipica dell'automazione CTs.
`AwsApprovalId: NotRequiredIfSubmitter`	Il sistema AMS cambia tipo e nessun altro, se la RFC inviata riguarda l'account con cui è stata presentata,	Nessuna operazione richiesta. Questa condizione è tipica dei manuali, in CTs quanto verranno sempre esaminati dagli operatori AMS.
`CustomerApprovalId: NotRequired`	Il sistema AMS Change Type,	Se la RFC supera i controlli della sintassi e dei parametri, viene approvata automaticamente.

Se la condizione di approvazione CT è	Richiede l'approvazione di	And
`CustomerApprovalId: Required`	Il sistema AMS cambia tipo e tu,	All'utente viene inviata una notifica ed è necessario approvare esplicita mente la RFC, rispondendo all'avviso o eseguendo l'operazione. ApproveRfc
`CustomerApprovalId: NotRequiredIfSubmitter`	Il sistema AMS cambia tipo e nessun altro, se hai inviato la RFC.	Se la RFC supera i controlli della sintassi e dei parametri, viene approvata automaticamente.
Incidente o patch di sicurezza urgente	AMS	È approvato e implementato automatic amente.

Cambia tipo di versioni

I tipi di modifica vengono versionati e la versione cambia quando viene apportato un aggiornamento importante al tipo di modifica.

Dopo aver selezionato un tipo di modifica utilizzando la console AMS, è possibile aprire l'area di configurazione aggiuntiva e selezionare una versione del tipo di modifica. È inoltre possibile specificare una versione del tipo di modifica nella API/CLI riga di comando. Potresti volerlo fare per vari motivi, tra cui:

- Sai che la versione del tipo di modifica Aggiorna che desideri deve corrispondere alla versione del tipo Crea modifica che hai usato per creare la risorsa che ora desideri aggiornare. Ad esempio, potresti avere un'istanza Elastic Load Balancer (ELB) creata con ELB Create change type versione 1. Per aggiornarla, scegli ELB Update versione 1.
- Desiderate utilizzare una versione del tipo di modifica con opzioni diverse rispetto al tipo di modifica più recente. Non lo consigliamo perché AMS aggiorna i tipi di modifica principalmente per motivi di sicurezza e ti consigliamo di scegliere sempre la versione più recente.

Creare tipi di modifica

I tipi di modifica di creazione corrispondono ai tipi version-to-version di modifica di aggiornamento. In altre parole, la versione del tipo di modifica utilizzata per il provisioning di una risorsa deve corrispondere alla versione del tipo di modifica Update che verrà utilizzata in seguito per modificare tale risorsa. Ad esempio, se crei un bucket S3 con il tipo di modifica Create S3 Bucket versione 2.0 e successivamente desideri inviare una RFC per modificare quel bucket S3, devi utilizzare anche il tipo di modifica Update S3 Bucket versione 2.0, anche se esiste un tipo di modifica Update S3 Bucket con la versione 3.0.

Ti consigliamo di tenere traccia dell'ID del tipo di modifica e della versione che utilizzi quando fornisci a una risorsa il tipo Crea modifica nel caso in cui in seguito desideri utilizzare un tipo di modifica Aggiorna per modificarla.

Aggiorna i tipi di modifica

AMS fornisce i tipi di modifica di aggiornamento per aggiornare le risorse create con Create change types. I tipi di modifica Update devono corrispondere version-to-version al tipo Create change originariamente utilizzato per fornire la risorsa.

Ti consigliamo di tenere traccia del tipo di modifica, dell'ID e della versione utilizzati per il provisioning di una risorsa per facilitarne l'aggiornamento.

YouTube Video: Come posso utilizzare l'aggiornamento CTs per modificare le risorse in un account AWS Managed Services (AMS)?

Tipi di modifiche solo interni

È possibile visualizzare i tipi di modifica solo per uso interno. In questo modo saprai quali azioni può o fa AMS. Se desideri rendere disponibile un tipo di modifica esclusivamente interno, invia una richiesta di assistenza.

Ad esempio, esiste una funzione Gestione | Monitoraggio e notifica | soppressione degli CloudWatch allarmi | Update CT che è solo interna. AMS lo utilizza per implementare gli aggiornamenti dell'infrastruttura (come l'applicazione di patch) per disattivare le notifiche di allarme che gli aggiornamenti potrebbero attivare erroneamente. Una volta inviato questo CT, noterai la relativa RFC nell'elenco delle RFC. Qualsiasi CT esclusivamente interno implementato in una RFC viene visualizzato nell'elenco RFC.

Cambia gli schemi dei tipi

Tutti i tipi di modifica forniscono uno schema JSON per l'input dell'utente nella creazione, modifica o accesso alle risorse. Lo schema fornisce i parametri e le relative descrizioni per la creazione di una richiesta di modifica (RFC).

L'esecuzione corretta di una RFC genera un output di esecuzione. Per il provisioning RFCs, l'output di esecuzione include un «stack_id» che rappresenta lo stack in CloudFormation e può essere cercato nella console. CloudFormation L'output di esecuzione a volte include l'output dell'ID dell'istanza creata e tale ID può essere utilizzato per cercare l'istanza nella console AWS corrispondente. Ad esempio, l'output di esecuzione Create ELB CT include uno «stack_id» ricercabile in CloudFormation e restituisce un valore key=ELB value= <stack-xxxx>che è ricercabile nella console Amazon per Elastic Load Balancing. EC2

Esaminiamo uno schema CT. Questo è lo schema di CodeDeploy Application Create, uno schema abbastanza piccolo. Alcuni schemi hanno `Parameter` aree molto ampie.

```
{
  "$schema": "http://json-schema.org/draft-04/schema#",
  "name": "Create CodeDeploy application",
  "description": "Use to create an AWS CodeDeploy applicati
on
  resource with the specified name.",
  "type": "object",
  "properties": {
    "Description": {
      "description": "The reason for the request.",
      "type": "string",
      "minLength": 1,
      "maxLength": 500
    },
    "VpcId": {
      "description": "ID of the vpc to use, in the form
 vpc-0123abcd or vpc-01234567890abcdef.",
      "type": "string",
      "pattern": "^vpc-[a-z0-9]{8}$"
    },
    "StackTemplateId": {
      "description": "Must be stm-sft6rv00000000000",
      "type": "string",
      "enum": ["stm-sft6rv00000000000"]
```

La prima parte dello schema fornisce informazioni ad AMS sul tipo di modifica richiesto.

```
    },
    "Name":{
      "description": "A name for the stack or stack component
;
      this becomes the Stack Name.",
      "type": "string",
      "minLength": 1,
      "maxLength": 255
    },
    "Tags": {
      "description": "Up to seven tags (key/value pairs) to
      categorize the resource.",
      "type": "array",
      "items": {
        "type": "object",
        "properties": {
          "Key": {
            "type": "string",
            "minLength": 1,
            "maxLength": 127
          },
          "Value": {
            "type": "string",
            "minLength": 1,
            "maxLength": 255
          }
        },
        "additionalProperties": false,
        "required": [
          "Key",
          "Value"
        ]
      },
      "minItems": 1,
      "maxItems": 7
    },
    "TimeoutInMinutes": {
      "description": "The maximum amount of time, in minutes,
 to
     allow for execution of the change. This will not prolong
 execution,
     but the RFC fails if the change is not completed in the
 specified time.
```

Il TimeoutInMinutes parametro consente di indicare un tempo limite per l'esecuzione del tipo di modifica. I valori validi sono compresi tra 60 e 360, per periodi di lunga durata UserData.

La sezione Parametri consente di specifica re le impostazioni per la risorsa che si sta creando o l'azione richiesta.

```
      Valid values are 60 up to 360, for long-running
 UserData.",
      "type": "number",
      "minimum": 0,
      "maximum": 60
    },
    "Parameters": {
      "description": "Specifications for the stack.",
      "type": "object",
      "properties": {
        "CodeDeployApplicationName": {
          "description": "The name of an AWS CodeDeploy
 application.",
          "type": "string",
          "minLength": 1,
          "maxLength": 100,
          "pattern": "^[a-zA-Z0-9._+=,@-]{1,100}$"
        }
      },
      "additionalProperties": false,
      "required": [
        "CodeDeployApplicationName"
      ]
    }
  },
  "additionalProperties": false,
  "required": [
    "Description",
    "VpcId",
    "StackTemplateId",
    "Name",
    "TimeoutInMinutes",
    "Parameters"
  ]
}
```

Le sezioni «proprietà aggiuntive» consentono di sapere quali parametri sono obbligatori e quali sono facoltativi.

Note

Questo schema consente fino a sette tag; tuttavia, EFS EC2, RDS e gli schemi di creazione multilivello consentono fino a 50 tag.

Gestione delle autorizzazioni per i tipi di modifica

È possibile utilizzare una politica personalizzata per limitare i tipi di modifica (CTs) disponibili per diversi gruppi o utenti.

Per ulteriori informazioni su questa operazione, consulta la sezione Impostazione delle autorizzazioni nella Guida per l'utente AMS.

Oscurazione di informazioni sensibili dai tipi di modifiche

Gli schemi dei tipi di modifica AMS offrono un attributo di parametro, `"metadata":"ams:sensitive":"true"` che viene utilizzato per i parametri che potrebbero contenere informazioni riservate, come una password. Quando questo attributo è impostato, l'input fornito è oscurato. Tieni presente che non puoi impostare questo attributo del parametro; tuttavia, se stai lavorando con AMS per creare un tipo di modifica e desideri che un parametro venga oscurato all'input, puoi richiederlo.

Ricerca di un tipo di modifica, utilizzando l'opzione di interrogazione

Questo esempio dimostra come utilizzare la console AMS per trovare il tipo di modifica appropriato per la RFC che si desidera inviare.

Puoi utilizzare la console o il API/CLI per trovare un ID del tipo di modifica (CT) o una versione. Esistono due metodi: la ricerca o la scelta della classificazione. Per entrambi i tipi di selezione, è possibile ordinare la ricerca scegliendo Usato più di frequente, Usato più di recente o Alfabetico.

YouTube Video: Come posso creare una RFC utilizzando la CLI di AWS Managed Services e dove posso trovare lo schema CT?

Nella console AMS, nella RFCspagina -> Crea RFC:

- Con l'opzione Sfoglia per tipo di modifica selezionata (impostazione predefinita), puoi:
  - Utilizza l'area di creazione rapida per selezionare tra i più diffusi di AMS CTs. Fai clic su un'etichetta e si apre la pagina Esegui RFC con l'opzione Oggetto compilata automaticamente per te. Completa le opzioni rimanenti secondo necessità e fai clic su Esegui per inviare la RFC.
  - In alternativa, scorri verso il basso fino all'area Tutti i tipi di modifica e inizia a digitare un nome CT nella casella delle opzioni, non è necessario avere il nome esatto o completo del tipo di modifica. Puoi anche cercare un CT in base alla modifica dell'ID del tipo, alla classificazione o alla modalità di esecuzione (automatica o manuale) inserendo le parole pertinenti.

Con la visualizzazione Carte predefinita selezionata, le schede CT corrispondenti vengono visualizzate durante la digitazione, seleziona una scheda e fai clic su Crea RFC. Con la vista Tabella selezionata, scegli il CT pertinente e fai clic su Crea RFC. Entrambi i metodi aprono la pagina Run RFC.

- In alternativa, e per esplorare le opzioni di modifica, fai clic su Scegli per categoria nella parte superiore della pagina per aprire una serie di caselle di opzioni a discesa.
- Scegli una categoria, una sottocategoria, un articolo e un'operazione. Viene visualizzata la casella delle informazioni per quel tipo di modifica e nella parte inferiore della pagina viene visualizzato un pannello.
- Quando sei pronto, premi Invio per visualizzare un elenco dei tipi di modifica corrispondenti.
- Scegli un tipo di modifica dall'elenco. La casella delle informazioni per quel tipo di modifica viene visualizzata nella parte inferiore della pagina.
- Dopo aver impostato il tipo di modifica corretto, scegli Crea RFC.

> **Note**
>
> Affinché questi comandi funzionino, è necessario installare l'AMS CLI. Per installare l'API o la CLI AMS, vai alla pagina Risorse per gli sviluppatori della console AMS. Per il materiale di riferimento sull'API AMS CM o sull'API AMS SKMS, consulta la sezione AMS Information Resources nella Guida per l'utente. Potrebbe essere necessario aggiungere un'`--profile`opzione per l'autenticazione, `aws amsskms` *`ams-cli-command`* `--profile SAML` ad esempio. Potrebbe essere necessario aggiungere l'`--region`opzione anche perché tutti i comandi AMS non utilizzano us-east-1, ad esempio. `aws amscm` *`ams-cli-command`* `--region=us-east-1`

> **Note**
>
> Gli endpoint AMS API/CLI (amscm e amsskms) si trovano nella regione AWS della Virginia settentrionale,. `us-east-1` A seconda di come è impostata l'autenticazione e della regione AWS in cui si trovano l'account e le risorse, potrebbe essere necessario aggiungerli `--region us-east-1` quando si emettono i comandi. Potrebbe anche essere necessario aggiungere`--profile saml`, se questo è il metodo di autenticazione utilizzato.

Per cercare un tipo di modifica utilizzando l'API AMS CM (vedi ListChangeTypeClassificationSummaries) o la CLI:

Puoi utilizzare un filtro o una query per effettuare la ricerca. L' ListChangeTypeClassificationSummaries operazione dispone delle opzioni di filtro per `CategorySubcategory`,`Item`, e`Operation`, ma i valori devono corrispondere esattamente ai valori esistenti. Per risultati più flessibili quando si utilizza la CLI, è possibile utilizzare l'`--query`opzione.

Filtraggio dei cambi di tipo con l'API/CLI AMS CM

Attributo	Valori validi	Condizione valida/predefinita	Note
ChangeTypeId	Qualsiasi stringa che rappresenta un ChangeTypeId (ad esempio: ct-abc123xyz7890)	Equals	Per il tipo di modifica, vedere il riferimento al tipo di modifica. IDs Per il tipo di modifica IDs, vedere Finding a Change Type o CSIO.
Categoria	Qualsiasi testo in formato libero	Contiene	Le espressioni regolari in ogni singolo campo non sono supportate. Ricerca senza distinzione tra lettere maiuscole
Sottocategoria			
Elemento			
Operazione			

1. Ecco alcuni esempi di classificazione dei tipi di modifica delle inserzioni:

   Il comando seguente elenca tutte le categorie dei tipi di modifica.

   ```
   aws amscm list-change-type-categories
   ```

   Il comando seguente elenca le sottocategorie appartenenti a una categoria specificata.

```
aws amscm list-change-type-subcategories --category CATEGORY
```

Il comando seguente elenca gli elementi appartenenti a una categoria e sottocategoria specificate.

```
aws amscm list-change-type-items --category CATEGORY --subcategory SUBCATEGORY
```

2. Ecco alcuni esempi di ricerca dei tipi di modifica con le query CLI:

   Il comando seguente cerca nei riepiloghi delle classificazioni CT quelli che contengono «S3" nel nome dell'elemento e crea l'output della categoria, della sottocategoria, dell'elemento, dell'operazione e dell'ID del tipo di modifica sotto forma di tabella.

```
aws amscm list-change-type-classification-summaries --query
 "ChangeTypeClassificationSummaries [?contains(Item, 'S3')].
[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
```

```
+-------------------------------------------------------------+
|               ListChangeTypeClassificationSummaries         |
+----------+-------------------------+--+------+--------------+
|Deployment|Advanced Stack Components|S3|Create|ct-1a68ck03fn98r|
+----------+-------------------------+--+------+--------------+
```

3. È quindi possibile utilizzare l'ID del tipo di modifica per ottenere lo schema CT ed esaminare i parametri. Il comando seguente genera lo schema in un file JSON denominato Creates3Params.schema.json.

```
aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateS3Params.schema.json
```

   Per informazioni sull'utilizzo delle query CLI, vedere Come filtrare l'output con l'opzione --query e il riferimento al linguaggio di interrogazione, Specificazione. JMESPath

4. Dopo aver ottenuto l'ID del tipo di modifica, ti consigliamo di verificare la versione del tipo di modifica per assicurarti che sia la versione più recente. Usa questo comando per trovare la versione per un tipo di modifica specificato:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CHANGE_TYPE_ID
```

Per trovare la versione `AutomationStatus` per un tipo di modifica specifico, esegui questo comando:

```
aws amscm --profile saml get-change-type-version --change-type-id CHANGE_TYPE_ID --
query "ChangeTypeVersion.{AutomationStatus:AutomationStatus.Name}"
```

Per trovare il tipo di modifica `ExpectedExecutionDurationInMinutes` per un tipo di modifica specifico, esegui questo comando:

```
aws amscm --profile saml get-change-type-version --change-type-id ct-14027q0sjyt1h
 --query "ChangeTypeVersion.{ExpectedDuration:ExpectedExecutionDurationInMinutes}"
```

Risoluzione degli errori RFC in AMS

Molti errori RFC relativi al provisioning di AMS possono essere esaminati tramite la documentazione. CloudFormation Vedi Risoluzione dei problemi di AWS CloudFormation: Risoluzione degli errori

Ulteriori suggerimenti per la risoluzione dei problemi sono forniti nelle seguenti sezioni.

Errori RFC di «gestione» in AMS

I tipi di cambio di categoria AMS «Management» (CTs) consentono di richiedere l'accesso alle risorse e di gestire le risorse esistenti. Questa sezione descrive alcuni problemi comuni.

Errori di accesso RFC

- Assicurati che il nome utente e il nome di dominio completo che hai specificato nella RFC siano corretti e che esistano nel dominio. Per informazioni su come trovare il tuo FQDN, vedi Ricerca del tuo FQDN.
- Assicurati che l'ID dello stack che hai specificato per l'accesso sia uno stack relativo a EC2. Gli stack come ELB e Amazon Simple Storage Service (S3) non sono candidati RFCs all'accesso, ma utilizza il tuo ruolo di accesso di sola lettura per accedere a queste risorse degli stack. Per assistenza nella ricerca di un ID dello stack, consulta Finding stack IDs
- Assicurati che l'ID dello stack che hai fornito sia corretto e appartenga all'account pertinente.

Per informazioni su altri errori RFC di accesso, consulta Gestione degli accessi.

YouTube Video: Come posso inviare correttamente una Request for Change (RFC) per evitare rifiuti ed errori?

Errori di pianificazione CT RFC (manuale)

La maggior parte dei tipi di modifica sono ExecutionMode =Automatizzati, ma alcuni sono ExecutionMode =Manuali e ciò influisce sulla modalità di pianificazione per evitare errori RFC.

Pianificato RFCs con ExecutionMode =Manual, deve essere impostato per essere eseguito almeno 24 ore nelle future se si utilizza la console AMS per creare la RFC.

AMS mira a rispondere a una CT manuale entro otto ore e risponderà il prima possibile, ma potrebbe essere necessario molto più tempo prima che la RFC venga effettivamente eseguita.

Utilizzo RFCs con aggiornamento manuale CTs

AMS Operations reject Management | Other | Other RFCs per gli aggiornamenti agli stack, quando esiste un tipo di modifica Update per il tipo di stack che si desidera aggiornare.

Errori di eliminazione dello stack RFC

Errori di eliminazione dello stack RFC: se utilizzi Management | Standard stacks | Stack | Delete CT, vedrai gli eventi dettagliati nella Console per lo stack con il nome dello stack AMS. CloudFormation Puoi identificare lo stack confrontandolo con il nome che ha nella console AMS. La CloudFormation console fornisce maggiori dettagli sulle cause dei guasti.

Prima di eliminare uno stack, dovresti considerare come è stato creato lo stack. Se avete creato lo stack utilizzando un CT AMS e non avete aggiunto o modificato le risorse dello stack, potete aspettarvi di eliminarlo senza problemi. Tuttavia, è una buona idea rimuovere tutte le risorse aggiunte manualmente da uno stack prima di inviare un RFC dello stack di eliminazione relativo allo stack. Ad esempio, se crei uno stack utilizzando lo stack CT completo (HA Two Tier), include un gruppo di sicurezza -. SG1 Se poi usi AMS per creare un altro gruppo di sicurezza e fai riferimento al nuovo SG2 gruppo SG1 creato come parte dello stack completo, e poi usi lo stack di eliminazione CT per eliminare lo stack, non SG1 verrà eliminato in quanto è referenziato da. SG2 SG2

> **Important**
>
> L'eliminazione degli stack può avere conseguenze indesiderate e impreviste. Per questo motivo, AMS preferisce *non* eliminare gli stack o le risorse dello stack per conto dei clienti. Tieni presente che AMS eliminerà solo le risorse per tuo conto (tramite un tipo di modifica

inviato in Gestione | Altro | Altro | Aggiorna) che non è possibile eliminare utilizzando il tipo di modifica appropriato e automatizzato da eliminare. Ulteriori considerazioni:

- Se le risorse sono abilitate per la «protezione da eliminazione», AMS può aiutarti a sbloccarla inviando un tipo di modifica Gestione | Altro | Altro | Aggiorna e, dopo aver rimosso la protezione da eliminazione, puoi utilizzare il CT automatico per eliminare quella risorsa.
- Se ci sono più risorse in uno stack e desideri eliminare solo un sottoinsieme delle risorse dello stack, usa il tipo di modifica CloudFormation Update (vedi Ingest Stack: Updating). CloudFormation Puoi anche inviare un tipo di modifica Management | Other | Other | Update e gli ingegneri AMS possono aiutarti a creare il changeset, se necessario.
- In caso di problemi nell'utilizzo di CloudFormation Update CT dovuti a deviazioni, AMS può aiutarti inviando un Management | Other | Other | Update per risolvere la deriva (nella misura supportata dal CloudFormation servizio AWS) e fornirne uno ChangeSet da convalidare ed eseguire utilizzando CT, Management/Custom Stack/Stack From CloudFormation Template/Approve Changeset e Update automatizzati.

AMS mantiene le restrizioni di cui sopra per garantire che non si verifichino eliminazioni di risorse impreviste o impreviste.

Per ulteriori informazioni, consulta Risoluzione dei problemi di AWS CloudFormation: delete stack fail.

Errori DNS di aggiornamento RFC

L'aggiornamento multiplo RFCs di una zona ospitata DNS può fallire, in alcuni casi senza motivo. La creazione RFCs simultanea di più zone ospitate dal DNS per aggiornare (private o pubbliche) può causare il fallimento RFCs di alcune zone perché stanno tentando di aggiornare lo stesso stack contemporaneamente. La gestione delle modifiche AMS rifiuta o RFCs fallisce chi non è in grado di aggiornare uno stack perché lo stack è già aggiornato da un'altra RFC. AMS consiglia di creare una RFC alla volta e di attendere che la RFC abbia esito positivo prima di crearne una nuova per lo stesso stack.

Errori delle entità RFC IAM

AMS fornisce una serie di ruoli e profili IAM predefiniti negli account AMS progettati per soddisfare le tue esigenze. Tuttavia, potrebbe essere necessario richiedere occasionalmente risorse IAM aggiuntive.

Il processo di invio della RFCs richiesta di risorse IAM personalizzate segue il flusso di lavoro standard per il manuale RFCs, ma il processo di approvazione include anche una revisione della sicurezza per garantire che siano in atto controlli di sicurezza appropriati. Pertanto, il processo richiede in genere più tempo rispetto ad altri manuali. RFCs Per ridurre il tempo di ciclo di questi RFCs, segui le seguenti linee guida.

Per informazioni su cosa intendiamo per revisione IAM e su come corrisponda ai nostri standard tecnici e al processo di accettazione dei rischi, consultaComprendi le revisioni sulla sicurezza RFC.

Richieste comuni di risorse IAM:

- Se stai chiedendo una policy relativa a una delle principali applicazioni compatibili con il cloud, ad esempio CloudEndure, consulta la CloudEndure policy IAM preapprovata da AMS: decomprimi il file di esempio WIGs Cloud Endure Landing Zone e apri il `customer_cloud_endure_policy.json`

  > **Note**
  >
  > Se desideri una policy più permissiva, discuti le tue esigenze e richiedi, se necessario, un'AMS Security Review CloudArchitect/CSDM and Signoff prima di inviare una RFC che implementi la policy.

- Se desideri modificare di default una risorsa distribuita da AMS nel tuo account, ti consigliamo di richiedere una copia modificata di quella risorsa anziché modificare quella esistente.
- Se richiedi le autorizzazioni per un utente umano (anziché assegnarle all'utente), allega le autorizzazioni a un ruolo, quindi concedi all'utente il permesso di assumere quel ruolo. Per maggiori dettagli su questa operazione, consulta Accesso temporaneo alla console AMS Advanced.
- Se hai bisogno di autorizzazioni eccezionali per una migrazione o un flusso di lavoro temporanei, fornisci una data di fine per tali autorizzazioni nella richiesta.
- Se avete già discusso l'argomento della richiesta con il team addetto alla sicurezza, fornite al CSDM una prova della loro approvazione nel modo più dettagliato possibile.

Se AMS rifiuta una RFC IAM, forniamo un motivo chiaro per il rifiuto. Ad esempio, potremmo rifiutare una policy IAM, creare una richiesta e spiegare quali aspetti della policy sono inappropriati. In tal caso, puoi apportare le modifiche identificate e inviare nuovamente la richiesta. Se è necessaria

maggiore chiarezza sullo stato di una richiesta, invia una richiesta di assistenza o contatta il tuo CSDM.

L'elenco seguente descrive i rischi tipici che AMS cerca di mitigare mentre esaminiamo il vostro IAM. RFCs Se la tua RFC IAM presenta uno di questi rischi, ciò potrebbe comportare il rifiuto della RFC. Nei casi in cui è necessaria un'eccezione, AMS richiede l'approvazione del team di sicurezza. Per cercare un'eccezione di questo tipo, contattate il vostro CSDM.

> **Note**
>
> AMS può, per qualsiasi motivo, rifiutare qualsiasi modifica alle risorse IAM all'interno di un account. Per dubbi riguardanti il rifiuto di una RFC, contatta AMS Operations tramite una richiesta di assistenza o contatta il tuo CSDM.

- Aumento dei privilegi, ad esempio autorizzazioni che consentono di modificare le proprie autorizzazioni o di modificare le autorizzazioni di altre risorse all'interno dell'account. Esempi:
  - L'uso di con un altro ruolo più `iam:PassRole` privilegiato.
  - Autorizzazione alle politiche attach/detach IAM da parte di un ruolo o di un utente.
  - La modifica delle politiche IAM nell'account.
  - La capacità di effettuare chiamate API nel contesto dell'infrastruttura di gestione.
- Autorizzazioni per modificare risorse o applicazioni necessarie per fornirti i servizi AMS. Esempi:
  - Modifica dell'infrastruttura AMS come i bastions, l'host di gestione o l'infrastruttura EPS.
  - Eliminazione delle funzioni o dei flussi di log di gestione dei log di AWS Lambda.
  - L'eliminazione o la modifica dell'applicazione di CloudTrail monitoraggio predefinita.
  - La modifica di Directory Services Active Directory (AD).
  - Disabilitazione degli CloudWatch allarmi (CW).
  - La modifica dei principi, delle politiche e dei namespace implementati nell'account come parte della landing zone.
- Implementazione dell'infrastruttura al di fuori delle migliori pratiche, ad esempio autorizzazioni che consentono la creazione di infrastrutture in uno stato che mette a rischio la sicurezza delle informazioni. Esempi:
  - La creazione di bucket S3 pubblici o non crittografati o la condivisione pubblica di volumi EBS.
  - Fornitura di indirizzi IP pubblici.
  - La modifica dei gruppi di sicurezza per consentire un ampio accesso.

- Autorizzazioni eccessivamente ampie in grado di influire sulle applicazioni, ad esempio autorizzazioni che possono causare perdita di dati, perdita di integrità, configurazione inappropriata o interruzioni del servizio per l'infrastruttura e le applicazioni all'interno dell'account. Esempi:
  - Disabilitazione o reindirizzamento del traffico di rete tramite like or. APIs `ModifyNetworkInterfaceAttribute` `UpdateRouteTable`
  - La disabilitazione dell'infrastruttura gestita mediante il distacco dei volumi dagli host gestiti.
- Le autorizzazioni per i servizi non fanno parte della descrizione del servizio AMS e non sono supportate da AMS.

  I servizi non elencati nella descrizione del servizio AMS non possono essere utilizzati negli account AMS. Per richiedere assistenza per una funzionalità o un servizio, contatta il tuo CSDM.
- Autorizzazioni che non soddisfano l'obiettivo dichiarato in quanto troppo generose o troppo conservative o applicate a risorse sbagliate. Esempi:
  - Una richiesta di `s3:PutObject` autorizzazioni per un bucket S3 con crittografia KMS obbligatoria, senza `KMS:Encrypt` autorizzazioni per la chiave pertinente.
  - Autorizzazioni relative a risorse che non esistono nell'account.
  - IAM RFCs in cui la descrizione della RFC non sembra corrispondere alla richiesta.

Errori RFC di «implementazione»

I tipi di cambio di categoria AMS «Deployment» (CTs) consentono di richiedere l'aggiunta di varie risorse supportate da AMS al proprio account.

La maggior parte degli AMS CTs che creano una risorsa si basano su CloudFormation modelli. In qualità di cliente hai accesso in sola lettura a tutti i servizi AWS CloudFormation, tra cui puoi identificare rapidamente lo CloudFormation stack che rappresenta il tuo stack in base alla descrizione dello stack utilizzando la Console. CloudFormation Lo stack fallito sarà probabilmente nello stato DELETE_COMPLETE. Una volta identificato lo CloudFormation stack, gli eventi mostreranno la risorsa specifica che non è stata creata e il motivo.

Utilizzo della CloudFormation documentazione per la risoluzione dei problemi

La maggior parte del provisioning AMS RFCs utilizza un CloudFormation modello e tale documentazione può essere utile per la risoluzione dei problemi. Consulta la documentazione relativa a quel CloudFormation modello:

- Errore di creazione del sistema di bilanciamento del carico delle applicazioni: AWS::ElasticLoadBalancingV2::LoadBalancer (Application Load Balancer)
- Crea gruppo di Auto Scaling: AWS::AutoScaling::AutoScalingGroup (Auto Scaling Group)
- Crea cache memcached: AWS::ElastiCache::CacheCluster (Cache Cluster)
- Crea cache Redis: AWS::ElastiCache::CacheCluster (Cache Cluster)
- Crea zona ospitata DNS (utilizzata con Create DNS private/public): (R53 Hosted Zone) AWS::Route53::HostedZone
- Crea set di record DNS (utilizzato con Create DNS private/public): (Resource Record Sets) AWS::Route53::RecordSet
- Crea stack EC2: (Elastic Compute Cloud) AWS::EC2::Instance
- Crea un file system elastico (EFS): AWS::EFS::FileSystem (Elastic File System)
- Crea un sistema di bilanciamento del carico: AWS::ElasticLoadBalancing::LoadBalancer (Elastic Load Balancer)
- Crea DB RDS: AWS::RDS::DBInstance (database relazionale)
- Crea Amazon S3: AWS::S3::Bucket (Servizio di storage semplice)
- Crea coda: AWS::SQS::Queue (Simple Queue Service)

Errori di creazione di RFC AMIs

Un'Amazon Machine Image (AMI) è un modello che contiene una configurazione software (ad esempio un sistema operativo, un server di applicazioni e le applicazioni). Da un'AMI, puoi avviare un'istanza, ovvero una copia dell'AMI in esecuzione come server virtuale nel cloud. Le AMI sono molto utili e necessarie per creare istanze EC2 o gruppi di Auto Scaling; tuttavia, è necessario rispettare alcuni requisiti:

- L'istanza specificata `Ec2InstanceId` deve trovarsi in uno stato interrotto affinché la RFC abbia esito positivo. Non utilizzate istanze del gruppo Auto Scaling (ASG) per questo parametro perché l'ASG terminerà un'istanza interrotta.
- Per creare un'Amazon Machine Image (AMI) AMS, devi iniziare con un'istanza AMS. Prima di poter utilizzare l'istanza per creare l'AMI, è necessario prepararla assicurandosi che venga interrotta e disconnessa dal relativo dominio. Per i dettagli, consulta Creare un'immagine di macchina Amazon standard utilizzando Sysprep

- Il nome specificato per la nuova AMI deve essere univoco all'interno dell'account, altrimenti la RFC fallirà. La procedura per eseguire questa operazione è descritta in AMI | Create e per ulteriori dettagli, consulta AWS AMI Design.

> **Note**
>
> Per ulteriori informazioni sulla preparazione per la creazione di AMI, consulta AMI | Create.

RFCs creazione di errori EC2s ASGs

Per i guasti EC2 o ASG con timeout, AMS consiglia di confermare se l'AMI utilizzato è personalizzato. In tal caso, consulta la procedura di creazione dell'AMI inclusa in questa guida (vedi AMI | Crea) per assicurarti che l'AMI sia stata creata correttamente. Un errore comune quando si crea un'AMI personalizzata è non seguire i passaggi indicati nella guida per rinominare o richiamare Sysprep.

RFCs creazione di errori RDS

I guasti di Amazon Relational Database Service (RDS) possono verificarsi per molte ragioni diverse, perché è possibile utilizzare molti motori diversi quando si crea l'RDS e ogni motore ha i propri requisiti e limitazioni. Prima di tentare di creare uno stack AMS RDS, esamina attentamente i valori dei parametri AWS RDS, consulta Create. DBInstance

Per ulteriori informazioni su Amazon RDS in generale, incluse le raccomandazioni sulle dimensioni, consulta la documentazione di Amazon Relational Database Service.

RFCs creazione di errori Amazon S3s

Un errore comune durante la creazione di un bucket di archiviazione S3 è il mancato utilizzo di un nome univoco per il bucket. Se hai inviato un bucket S3 Create CT con lo stesso nome di uno inviato in precedenza, non riuscirebbe perché esisterebbe già un bucket S3 con quello stesso nome. BucketName Questo verrebbe descritto in dettaglio nella CloudFormation Console, dove vedrai che l'evento stack mostra che il nome del bucket è già in uso.

Validazione RFC rispetto agli errori di esecuzione

Gli errori RFC e i messaggi correlati differiscono nei messaggi di output nella pagina dei dettagli RFC della console AMS per un RFC selezionato:

- I motivi degli errori di convalida sono disponibili solo nel campo Status
- I motivi degli errori di esecuzione sono disponibili in Execution Output e Status Fields.

Messaggi di errore RFC

Quando riscontri il seguente errore per i tipi di modifica elencati (CTs), puoi utilizzare queste soluzioni per individuare l'origine dei problemi e risolverli.

```
{"errorMessage":"An error has occurred during RFC execution. We are
investigating the issue.","errorType":"InternalError"}
```

Se hai bisogno di ulteriore assistenza dopo aver fatto riferimento alle seguenti opzioni di risoluzione dei problemi, contatta AMS tramite corrispondenza RFC. Per ulteriori informazioni, consulta Corrispondenza e allegato RFC (console).

Errori di inserimento del carico di lavoro (WIGS)

> **Note**
>
> Gli strumenti di convalida per Windows e Linux possono essere scaricati ed eseguiti direttamente sui server locali, nonché sulle istanze EC2 in AWS. È possibile trovarli nella AMS Advanced Application Developer's GuideMigrating workload: Linux pre-ingestion validation e Migrating workload: Windows pre-ingestion validation.

- Assicurati che l'istanza EC2 esista nell'account AMS di destinazione. Ad esempio, se hai condiviso il tuo AMI da un account non AMS a un account AMS, dovrai creare un'istanza EC2 nel tuo account AMS con l'AMI condiviso prima di poter inviare un Workload Ingest RFC.
- Verifica se per i gruppi di sicurezza collegati all'istanza è consentito il traffico in uscita. L'agente SSM deve essere in grado di connettersi al suo endpoint pubblico.
- Verifica se l'istanza dispone delle autorizzazioni giuste per connettersi con l'agente SSM. Queste autorizzazioni vengono fornite con`customer-mc-ec2-instance-profile`, puoi verificarle nella console EC2:

Errori di blocco dello stack di istanze EC2

- Verifica se l'istanza è già in uno stato interrotto o terminato.
- Se l'istanza EC2 è online e vedi l'`InternalError`errore, invia una richiesta di servizio per consentire ad AMS di indagare.
- Tieni presente che non puoi utilizzare il tipo di modifica Management | Advanced stack components | EC2 instance stack | Stop ct-3mvvt2zkyveqj per interrompere un'istanza del gruppo Auto Scaling (ASG). Se devi interrompere un'istanza ASG, invia una richiesta di servizio.

Lo stack di istanze EC2 crea errori

Il `InternalError` messaggio proviene da CloudFormation; un motivo dello stato CREATION_FAILED. Puoi trovare dettagli sull'errore dello stack negli eventi dello CloudWatch stack seguendo questi passaggi:

- Nella console di gestione AWS, puoi visualizzare un elenco di eventi dello stack durante la creazione, l'aggiornamento o l'eliminazione dello stack. In questo elenco, trova l'evento relativo al problema e quindi visualizzane il motivo dello stato.

  Il motivo dello stato potrebbe contenere un messaggio di errore di AWS CloudFormation o di un particolare servizio che può aiutarti a comprendere il problema.
- Per ulteriori informazioni sulla visualizzazione degli eventi dello stack, consulta Visualizzazione dei dati e delle risorse di AWS CloudFormation Stack nella Console di gestione AWS.

Errori di ripristino del volume delle istanze EC2

AMS crea una RFC interna per la risoluzione dei problemi quando il ripristino del volume delle istanze EC2 fallisce. Ciò avviene perché il ripristino del volume delle istanze EC2 è una parte importante del disaster recovery (DR) e AMS crea automaticamente questa RFC interna per la risoluzione dei problemi.

Quando viene creata la RFC interna per la risoluzione dei problemi, viene visualizzato un banner che fornisce i collegamenti alla RFC. Questa RFC interna per la risoluzione dei problemi offre una maggiore visibilità sugli errori RFC e, anziché ripetere RFCs i tentativi che generano gli stessi errori o richiedere di contattare manualmente AMS in caso di errore, potete tenere traccia delle modifiche apportate e sapere che AMS sta lavorando sull'errore. In questo modo si riduce anche la metrica time-to-recovery (TTR) relativa alla modifica, in quanto gli operatori AMS lavorano in modo proattivo sull'errore RFC anziché attendere la richiesta dell'utente.

Come ottenere assistenza con un RFC

Puoi contattare AMS per identificare la causa principale del tuo errore. L'orario di lavoro di AMS è 24 ore al giorno, 7 giorni alla settimana, 365 giorni all'anno.

AMS offre diverse possibilità per chiedere aiuto.

- Se hai bisogno di assistenza per una RFC aperta o una RFC completata ma non corretta, contatta AMS tramite corrispondenza bidirezionale RFC. Per ulteriori informazioni, consulta Corrispondenza e allegato RFC (console).
- Per segnalare un problema di prestazioni del servizio AWS o AMS che influisce sull'ambiente gestito, utilizza la console AMS e invia un rapporto sull'incidente. Per i dettagli, consulta Segnalazione di un incidente. Per informazioni generali sulla gestione degli incidenti con AMS, consulta Risposta agli incidenti.
- Per domande specifiche su come voi, le vostre risorse o applicazioni state lavorando con AMS o per segnalare un incidente, inviate un'e-mail a uno o più dei seguenti documenti:
  1. Innanzitutto, se non siete soddisfatti della richiesta di servizio o della risposta alla segnalazione dell'incidente, inviate un'e-mail al vostro CSDM: ams-csdm@amazon.com
  2. Successivamente, se è necessaria un'escalation, puoi inviare un'e-mail all'AMS Operations Manager (ma probabilmente il tuo CSDM lo farà): ams-opsmanager@amazon.com
  3. Un'ulteriore escalation verrebbe indirizzata al direttore di AMS: ams-director@amazon.com
  4. Infine, puoi sempre contattare il vicepresidente di AMS: ams-vp@amazon.com

Modalità Direct Change in AMS

Argomenti

- Guida introduttiva alla modalità Direct Change
- Sicurezza e conformità
- Gestione delle modifiche in modalità Direct Change
- Creazione di pile utilizzando la modalità Direct Change
- Casi d'uso della modalità Direct Change

La modalità Direct Change (DCM) di AWS Managed Services (AMS) estende la gestione delle modifiche di AMS Advanced fornendo AWS accesso nativo agli account AMS Advanced Plus e Premium per fornire e aggiornare AWS le risorse. Con DCM, hai la possibilità di utilizzare AWS API

native (console o CLI/SDK) o richieste di modifica AMS Advanced Change Management (RFCs) e in entrambi i casi le risorse e le modifiche ad esse apportate sono completamente supportate da AMS, tra cui monitoraggio, patch, backup e gestione della risposta agli incidenti. Le risorse fornite tramite DCM sono registrate nel sistema di gestione della conoscenza dei servizi AMS (SKMS), aggiunte al dominio Active Directory gestito da AMS (se applicabile) ed eseguono agenti di gestione AMS. Utilizza gli strumenti esistenti (ad esempio AWS SDK e CDK) per sviluppare e distribuire stack gestiti da AMS. CloudFormation CloudFormation

> **Note**
>
> La modalità Direct Change non rimuove la gestione delle modifiche AMS. RFCs Hai pieno accesso ad AMS RFCs con DCM.

Guardate il video di Akash per saperne di più (6:30)

Guida introduttiva alla modalità Direct Change

Inizia controllando i prerequisiti e poi inviando una richiesta di modifica (RFC) nel tuo account AMS Advanced idoneo.

1. Verifica che l'account che desideri utilizzare con DCM soddisfi i requisiti:

   - L'account è AMS Advanced Plus o Premium.
   - L'account non ha Service Catalog abilitato. Al momento non supportiamo l'onboarding degli account sia su DCM che su Service Catalog allo stesso tempo. Se hai già effettuato l'accesso a Service Catalog ma sei interessato a DCM, discuti le tue esigenze con il tuo cloud service delivery manager (CSDM). Se decidi di passare da Service Catalog a DCM, offboard Service Catalog, per farlo, includi la richiesta nella richiesta di modifica riportata di seguito. Per informazioni dettagliate su Service Catalog in AMS, consulta AMS and Service Catalog.
2. Invia una richiesta di modifica (RFC) utilizzando la modalità Gestione | Account gestito | Modifica diretta | Abilita il tipo di modifica (ct-3rd4781c2nnhp). Per un esempio di procedura dettagliata, consulta la modalità Direct Change | Enable.

   Dopo l'elaborazione del CT, i ruoli IAM predefiniti `AWSManagedServicesUpdateRole` vengono assegnati all'account specificato. `AWSManagedServicesCloudFormationAdminRole`
3. Assegna il ruolo appropriato agli utenti che richiedono l'accesso a DCM utilizzando il processo di federazione interno.

> **Note**
>
> È possibile specificare un numero qualsiasi di SAMLIdentity provider, AWS servizi ed entità IAM (ruoli, utenti, ecc.) per assumere i ruoli. È necessario fornire almeno uno: `SAMLIdentityProviderARNs`, o`AWSServicePrincipals`. Per ulteriori informazioni, rivolgiti al dipartimento IAM della tua azienda o al tuo architetto cloud AMS (CA).

Ruoli e politiche IAM in modalità Direct Change

Quando la modalità Direct Change è abilitata in un account, vengono implementate queste nuove entità IAM:

`AWSManagedServicesCloudFormationAdminRole`: Questo ruolo consente l'accesso alla CloudFormation console, la creazione e l'aggiornamento degli CloudFormation stack, la visualizzazione dei report sulle deviazioni e la creazione e l'esecuzione. CloudFormation ChangeSets L'accesso a questo ruolo è gestito tramite il tuo provider SAML.

Le politiche gestite che vengono implementate e associate al ruolo `AWSManagedServicesCloudFormationAdminRole` sono:

- Account applicativo AMS Advanced multi-account landing zone (MALZ)
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
    - Questa politica rappresenta le autorizzazioni concesse a. `AWSManagedServicesCloudFormationAdminRole` Tu e i tuoi partner utilizzate questa politica per concedere l'accesso a un ruolo esistente nell'account e consentire a tale ruolo di avviare e aggiornare gli CloudFormation stack nell'account. Ciò potrebbe richiedere aggiornamenti aggiuntivi della politica di controllo dei servizi AMS (SCP) per consentire ad altre entità IAM di avviare CloudFormation stack.
- Account di landing zone con account singolo AMS Advanced (SALZ)
  - AWSManagedServices_CloudFormationAdminPolicy1
  - AWSManagedServices_CloudFormationAdminPolicy2
  - cdk-legacy-mode-s3 accessi [politica in linea]
  - AWS ReadOnlyAccess politica

`AWSManagedServicesUpdateRole`: Questo ruolo garantisce un accesso limitato al servizio downstream AWS . APIs Il ruolo viene implementato con policy gestite che forniscono operazioni API mutanti e non mutanti, ma in generale limita le operazioni mutanti (ad esempioCreate/Delete/PUT) rispetto a determinati servizi come IAM, KMS, GuardDuty VPC, risorse e configurazione dell'infrastruttura AMS e così via. L'accesso a questo ruolo è gestito tramite il tuo provider SAML.

Le politiche gestite che vengono implementate e associate al ruolo `AWSManagedServicesUpdateRole` sono:

- Account applicativo AMS Advanced multi-account per la landing zone
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyPolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2E RDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolitica
- Account di landing zone AMS Advanced con account singolo
  - AWSManagedServicesUpdateBasePolicy
  - AWSManagedServicesUpdateDenyProvisioningPolicy
  - AWSManagedServicesUpdateEC2E RDSPolicy
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolitica 1
  - AWSManagedServicesUpdateDenyActionsOnAMSInfraPolitica 2

Oltre a questi, al `AWSManagedServicesUpdateRole` ruolo di policy gestita è `ViewOnlyAccess` associata anche la policy AWS gestita.

Sicurezza e conformità

La sicurezza e la conformità sono una responsabilità condivisa tra AMS Advanced e te, in qualità di nostro cliente. La modalità AMS Advanced Direct Change non modifica questa responsabilità condivisa.

Sicurezza in modalità Direct Change

AMS Advanced offre un valore aggiunto con una landing zone prescrittiva, un sistema di gestione delle modifiche e una gestione degli accessi. Quando si utilizza la modalità Direct Change, questo modello di responsabilità non cambia. Tuttavia, è necessario essere consapevoli dei rischi aggiuntivi.

Il ruolo «Aggiornamento» della modalità Direct Change (vediRuoli e politiche IAM in modalità Direct Change) fornisce autorizzazioni elevate che consentono all'entità che vi ha accesso di apportare modifiche alle risorse di infrastruttura dei servizi supportati da AMS presenti nell'account. Con autorizzazioni elevate, esistono rischi diversi a seconda della risorsa, del servizio e delle azioni, specialmente in situazioni in cui viene apportata una modifica errata a causa di supervisione, errore o mancanza di aderenza al processo interno e al framework di controllo.

In base agli standard tecnici AMS, sono stati identificati i seguenti rischi e vengono formulate le seguenti raccomandazioni. Informazioni dettagliate sugli standard tecnici AMS sono disponibili all'indirizzo AWS Artifact. Per accedervi AWS Artifact, contattate il vostro CSDM per ricevere istruzioni o consultate la sezione Guida introduttiva. AWS Artifact

AMS-STD-001: etichettatura

Standard	Si rompe	Rischi	Raccomandazioni
Tutte le risorse di proprietà di AMS devono avere la seguente coppia chiave-valore Tutti i tag di proprietà di AMS diversi da quelli sopra elencati devono avere prefissi simili a «o in case». `AMS* MC*` upper/lower/mix	Sì. Breaks for CloudFormation,CloudTrail, EFS OpenSearch, CloudWatch Logs, SQS, SSM, Tagging api, poiché questi servizi non supportano la `aws:TagsKey` condizione di limitazione del tagging per lo spazio dei nomi AMS. Lo standard riportato nella tabella AMS-STD-003, che segue, afferma che è possibile modificare l'ambiente e, ma non per le risorse di proprietà di AMS. AppId AppName Non	L'etichettatura errata delle risorse AMS può influire negativamente sulle operazioni di segnalazione, avviso e applicazione di patch delle risorse, da parte di AMS.	L'accesso deve essere limitato per apportare modifiche ai requisiti di etichettatura predefiniti di AMS per chiunque non sia un team AMS.

Standard	Si rompe	Rischi	Raccomandazioni
	realizzabile tramite le autorizzazioni IAM.		
I tag presenti negli stack di proprietà di AMS non devono essere eliminati in base alle richieste di modifica.	Sì. CloudFormation non supporta la `aws:TagsKey` condizione di limitare i tag per lo spazio dei nomi AMS.		
Non è consentito utilizzare la convenzione di denominazione dei tag AMS nella propria infrastruttura, come indicato nella tabella AMS-STD-002, successiva.	Sì. Breaks for CloudFormation, CloudTrail, Elastic File System (EFS), CloudWatch Logs OpenSearch, Amazon Simple Queue Service (SQS), Amazon EC2 Systems Manager (SSM), Tagging API; questi servizi non `aws:TagsKey` supportano la condizione di limitazione del tagging per lo spazio dei nomi AMS.		

AMS-STD-002: Identity and Access Management (IAM)

Standard	Si rompe	Rischi	Raccomandazioni
4.7 Non devono essere consentite azioni che aggirano il processo di gestione	Sì. Lo scopo delle azioni self-service consente di eseguire	Il modello di accesso sicuro è un aspetto tecnico fondamentale di AMS e un utente	L'utente IAM deve disporre di un periodo di tempo limitato e concedere le

Standard	Si rompe	Rischi	Raccomandazioni
delle modifiche (RFC), come l'avvio o l'arresto di un'istanza, la creazione di bucket S3 o istanze RDS e così via. Gli account in modalità sviluppatore e i servizi in modalità Self-Service Provisioned (SSPS) sono esentati a condizione che le azioni vengano eseguite entro i limiti del ruolo assegnato.	azioni aggirando il sistema RFC AMS.	IAM per l'accesso da console o programmatico elude questo controllo di accesso. L'accesso degli utenti IAM non è monitorato dalla gestione delle modifiche di AMS. L'accesso è registrato CloudTrail solo.	autorizzazioni in base al privilegio minimo e. need-to-know

AMS-STD-003: Sicurezza di rete

Standard	Si rompe	Rischi	Raccomandazioni
S2. L'IP elastico sulle EC2 istanze deve essere utilizzato solo con un accordo formale di accettazione del rischio o con un caso d'uso valido da parte dei team interni.	Sì. Le azioni self-service consentono di associare e dissociare gli indirizzi IP elastici (EIP).	L'aggiunta di un IP elastico a un'istanza la espone a Internet. Ciò aumenta il rischio di divulgazione di informazioni e attività non autorizzate.	Blocca il traffico non necessario verso quell'istanza tramite i gruppi di sicurezza e verifica che i gruppi di sicurezza siano collegati all'istanza per garantire che consenta il traffico solo se necessario per motivi aziendali.
S14. È possibile consentire il peering VPC e le connessioni	Sì. Non possibile tramite la policy IAM.	Il traffico in uscita dal tuo account AMS non viene monitorato una	Ti consigliamo di effettuare il peering solo con account AMS

Standard	Si rompe	Rischi	Raccomandazioni
endpoint tra account che appartengono allo stesso cliente.		volta che esce dal confine dell'account.	di tua proprietà. Se il tuo caso d'uso lo richiede, utilizza i gruppi di sicurezza e le tabelle di routing per limitare gli intervalli, le risorse e i tipi di traffico che possono provenire dalla connessione pertinente.
La base AMS AMIs può essere condivisa tra account gestiti da AMS e non gestiti, purché sia possibile verificare che siano di proprietà della stessa organizzazione. AWS		AMIs può contenere dati sensibili e può essere esposto ad account indesiderati.	Condividi solo AMIs con l'account di proprietà della tua organizzazione o convalida il caso d'uso e le informazioni sull'account prima di condividerle all'esterno dell'organizzazione.

AMS-STD-007: Registrazione

Standard	Si rompe	Rischi	Raccomandazioni
19. Qualsiasi registro può essere inoltrato da un account AMS a un altro account AMS dello stesso cliente.	Sì. La potenziale insicurezza dei registri dei clienti, in quanto la verifica degli account dei clienti appartenenti alla stessa organizza	I log possono contenere dati sensibili e possono essere esposti ad account indesiderati.	Condividi i log solo con gli account gestiti dalla tua AWS organizzazione o convalida il caso d'uso e le informazioni sull'account prima di
20. Qualsiasi registro può essere inoltrato			

Standard	Si rompe	Rischi	Raccomandazioni
da AMS a un account diverso da AMS solo se l'account non AMS è di proprietà dello stesso cliente AMS (confermando che si tratta dello stesso AWS Organizations account o abbinando il dominio e-mail al nome dell'azienda del cliente e all'account collegato a PAYER) utilizzando strumenti interni.	zione non può essere ottenuta mediante la politica IAM.		condividerli all'ester no dell'organizzazion e. Possiamo verificar lo in diversi modi, verificalo con il tuo gestore di fornitura dei servizi cloud (CSDM).

Collabora con il tuo team interno di autorizzazione e autenticazione per controllare di conseguenza le autorizzazioni relative ai ruoli della modalità Direct Change.

Conformità in modalità Direct Change

La modalità Direct Change è compatibile con i carichi di lavoro di produzione e non di produzione. È responsabilità dell'utente garantire il rispetto di tutti gli standard di conformità (ad esempio, PHI, HIPAA, PCI) e garantire che l'uso della modalità Direct Change sia conforme ai framework e agli standard di controllo interni.

Gestione delle modifiche in modalità Direct Change

La gestione delle modifiche è il processo utilizzato da AMS Advanced per implementare le richieste di modifica. Una richiesta di modifica (RFC) è una richiesta creata dall'utente o da AMS Advanced tramite l'interfaccia AMS Advanced per apportare una modifica all'ambiente gestito e include un ID di tipo di modifica (CT) AMS Advanced per una particolare operazione. Per ulteriori informazioni, consulta Gestione delle modifiche.

> **Note**
>
> La modalità Direct Change non rimuove la gestione delle RFCs modifiche di AMS; hai comunque pieno accesso ad AMS RFCs con DCM.

La modalità AMS Direct Change (DCM) estende la gestione delle modifiche di AMS Advanced fornendo AWS l'accesso nativo agli account AMS Advanced Plus e Premium per fornire e aggiornare AWS le risorse. Gli utenti a cui è stata concessa l'autorizzazione in modalità Direct Change tramite i ruoli IAM possono utilizzare l'accesso AWS API nativo per fornire e apportare modifiche alle risorse nei propri account AMS Advanced. Gli utenti possono comunque utilizzare la gestione delle modifiche di AMS Advanced RFCs utilizzando gli stessi ruoli IAM. In entrambi i casi, le risorse e le relative modifiche sono pienamente supportate da AMS, tra cui monitoraggio, patch, backup e gestione della risposta agli incidenti. Gli utenti che non hanno il ruolo appropriato in questi account devono utilizzare il processo RFC di AMS Advanced change management per apportare modifiche.

Casi d'uso della gestione delle modifiche

Per motivi di sicurezza, alcune modifiche in AMS Advanced possono essere apportate solo tramite il processo RFC (Change Management Request for Change). `AWSManagedServicesCloudFormationAdminRole`È limitato alle azioni intraprese tramite CloudFormation (CFN). Per ulteriori informazioni su come creare pile tramite DCM, consulta Creazione di pile utilizzando la modalità Direct Change. `AWSManagedServicesUpdateRole`È limitato alle seguenti azioni.

Ad esempio, le procedure dettagliate per ogni tipo di modifica, tra cui Gestione | Account gestito | Modalità Direct Change | Abilita (ct-3rd4781c2nnhp), consulta la sezione «Informazioni aggiuntive» per il tipo di modifica pertinente nella sezione AMS Advanced Change Type Reference Change Type Reference Change Types by Classification.

Servizio	Azione
AWS Key Management Service (AWS KMS)	Aggiorna
AWS Certificate Manager	Crea
AWS Identity and Access Management (IAM)	Qualsiasi
Site-to-Site VPN	Qualsiasi

Servizio	Azione
Pianificatore di risorse AMS	
AWS Backup	Crea un piano di backup
Inserimento del carico di lavoro AMS () WIGs	Qualsiasi
Modifiche all'account AMS Advanced MALZ	
Amazon GuardDuty	
Accesso avanzato allo stack AMS	Qualsiasi
Volume Amazon Elastic Block Store (EBS)	Elimina
Crittografia predefinita di Amazon Elastic Block Store (EBS)	Abilita la crittografia predefinita
Amazon Elastic Compute Cloud (Amazon EC2)	Cambia nome host
Amazon Machine Images (AMI)	Elimina, condividi
Gruppo di sicurezza Amazon EC2	Qualsiasi
SSPS avanzato AMS	
AWS Microsoft AD gestito	
Modalità sviluppatore AMS Advanced	
Amazon Simple Storage Service (Amazon S3)	Crea policy per i bucket S3
AWS Systems Manager	Crea

Creazione di pile utilizzando la modalità Direct Change

Per consentire la gestione dello stack da parte di CloudFormation AMS`AWSManagedServicesCloudFormationAdminRole`, sono necessari due requisiti per avviare gli stack:

- Il modello deve contenere un. `AmsStackTransform`
- Il nome dello stack deve iniziare con il prefisso `stack-` seguito da una stringa alfanumerica di 17 caratteri.

> **Note**
>
> Per utilizzare correttamente lo`AmsStackTransform`, devi riconoscere che il tuo modello di stack contiene la `CAPABILITY_AUTO_EXPAND` funzionalità in order for CloudFormation (CFN) di creare o aggiornare lo stack. Puoi farlo passandolo `CAPABILITY_AUTO_EXPAND` come parte della tua richiesta create-stack. CFN rifiuta la richiesta se questa funzionalità non viene riconosciuta quando viene inclusa nel `AmsStackTransform` modello. La console CFN ti assicura di passare questa funzionalità se hai la trasformazione nel tuo modello, ma questa può essere ignorata quando interagisci con CFN tramite loro. APIs
> Devi passare questa funzionalità ogni volta che utilizzi le seguenti chiamate API CFN:
>
> - CreateChangeSet
> - CreateStack
> - UpdateStack

Quando si crea o si aggiorna uno stack con DCM, sullo stack CTs vengono eseguite le stesse convalide e potenziamenti di CFN Ingest e Stack Update. Per maggiori informazioni, consulta le Linee guida per l'inserimento, le migliori pratiche e le limitazioni.CloudFormation L'eccezione è che i gruppi di sicurezza predefiniti di AMS (SGs) non verranno collegati a nessuna istanza autonoma o EC2 EC2 istanza nei gruppi di Auto Scaling (). ASGs Quando create il CloudFormation modello, con EC2 istanze autonome oppure, potete allegare quello predefinito. ASGs SGs

> **Note**
>
> I ruoli IAM possono ora essere creati e gestiti con. `AWSManagedServicesCloudFormationAdminRole`

L'impostazione predefinita SGs di AMS prevede regole di ingresso e uscita che consentono alle istanze di avviarsi correttamente e di accedervi successivamente tramite SSH o RDP da parte delle operazioni AMS e dell'utente. Se ritieni che i gruppi di sicurezza predefiniti di AMS siano troppo

permissivi, puoi crearne di personalizzati SGs con regole più restrittive e collegarli all'istanza, purché ciò consenta comunque a te e alle operazioni AMS di accedere all'istanza durante gli incidenti.

I gruppi di sicurezza predefiniti di AMS sono i seguenti:

- SentinelDefaultSecurityGroupPrivateOnly: È possibile accedere nel modello CFN tramite questo parametro SSM `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnly`
- SentinelDefaultSecurityGroupPrivateOnlyEgressAll: È possibile accedere nel modello CFN tramite questo parametro SSM `/ams/${VpcId}/SentinelDefaultSecurityGroupPrivateOnlyEgressAll`

Trasforma AMS

Aggiungi una `Transform` dichiarazione al tuo CloudFormation modello. Questo aggiunge una CloudFormation macro che convalida e registra lo stack con AMS al momento del lancio.

Esempio JSON

```
"Transform": {
    "Name": "AmsStackTransform",
    "Parameters": {
      "StackId": {"Ref" : "AWS::StackId"}
    }
  }
```

Esempio YAML

```
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
```

Aggiungi l'`Transform`istruzione anche quando aggiorni il modello di uno stack esistente.

Esempio JSON

```
{
  "AWSTemplateFormatVersion": "2010-09-09",
  "Description" : "Create an SNS Topic",
    "Transform": {
      "Name": "AmsStackTransform",
```

```
      "Parameters": {
        "StackId": {"Ref" : "AWS::StackId"}
     }
  },
  "Parameters": {
    "TopicName": {
      "Type": "String",
      "Default": "HelloWorldTopic"
    }
  },
  "Resources": {
    "SnsTopic": {
      "Type": "AWS::SNS::Topic",
      "Properties": {
        "TopicName": {"Ref": "TopicName"}
      }
    }
  }
}
```

Esempio YAML

```
AWSTemplateFormatVersion: '2010-09-09'
Description: Create an SNS Topic
Transform:
  Name: AmsStackTransform
  Parameters:
    StackId: !Ref 'AWS::StackId'
Parameters:
  TopicName:
    Type: String
    Default: HelloWorldTopic
Resources:
  SnsTopic:
    Type: AWS::SNS::Topic
    Properties:
      TopicName: !Ref TopicName
```

Nome stack

Il nome dello stack deve iniziare con il prefisso `stack-` seguito da una stringa alfanumerica di 17 caratteri. Ciò serve a mantenere la compatibilità con altri sistemi AMS che operano sullo stack AMS. IDs

Di seguito sono riportati alcuni esempi di modi per generare stack compatibili: IDs

Bash:

```
echo "stack-$(env LC_CTYPE=C tr -dc 'a-z0-9' < /dev/urandom | head -c 17)"
```

Python:

```
import string
import random

'stack-' + ''.join(random.choices(string.ascii_lowercase + string.digits, k=17))
```

Powershell:

```
"stack-" + ( -join ((0x30..0x39) + ( 0x61..0x7A) | Get-Random -Count 17  | %
 {[char]$_}) )
```

Casi d'uso della modalità Direct Change

Di seguito sono riportati i casi d'uso della modalità Direct Change:

Fornitura e gestione delle risorse tramite CloudFormation

- Integra CloudFormation gli strumenti e i processi esistenti.

Gestione e aggiornamenti continui delle risorse

- Piccole modifiche atomiche a basso rischio.
- Modifiche che altrimenti verrebbero eseguite tramite una RFC manuale o automatizzata.
- Strumenti che richiedono l'accesso nativo all' AWS API.
- Il ruolo DCM può essere utilizzato se sei in fase di migrazione. I team di migrazione sfruttano le autorizzazioni del DCM per creare o modificare gli stack.
- I ruoli DCM possono essere utilizzati nella CI/CD pipeline per crearne di nuovi AMIs, creare attività Amazon ECS e così via.

Modalità AMS Advanced Developer

Argomenti

- Guida introduttiva alla modalità AMS Advanced Developer
- Sicurezza e conformità in modalità Sviluppatore
- Gestione delle modifiche in modalità Sviluppatore
- Provisioning dell'infrastruttura in modalità AMS Developer
- Controlli Detective in modalità AMS Developer
- Registrazione, monitoraggio e gestione degli eventi in modalità AMS Developer
- Gestione degli incidenti in modalità AMS Developer
- Gestione delle patch in modalità AMS Developer
- Gestione della continuità in modalità AMS Developer
- Gestione della sicurezza e degli accessi in modalità AMS Developer

La modalità sviluppatore di AWS Managed Services (AMS) utilizza autorizzazioni elevate negli account AMS Advanced Plus e Premium per fornire e aggiornare le risorse AWS al di fuori del processo di gestione delle modifiche di AMS Advanced. La modalità AMS Advanced Developer esegue questa operazione sfruttando le chiamate API AWS native all'interno di AMS Advanced Virtual Private Cloud (VPC), consentendoti di progettare e implementare infrastrutture e applicazioni nel tuo ambiente gestito.

Quando si utilizza un account con la modalità Sviluppatore abilitata, vengono fornite la gestione della continuità, la gestione delle patch e la gestione delle modifiche per le risorse fornite tramite il processo di gestione delle modifiche AMS Advanced o utilizzando un'Amazon Machine Image (AMI) AMS. Tuttavia, queste funzionalità di gestione AMS non sono disponibili per le risorse fornite in modalità nativa. AWS APIs

L'utente è responsabile del monitoraggio delle risorse dell'infrastruttura fornite al di fuori del processo di gestione delle modifiche di AMS Advanced. La modalità sviluppatore è compatibile con i carichi di lavoro di produzione e non di produzione. Con autorizzazioni elevate, hai una maggiore responsabilità nel garantire il rispetto dei controlli interni.

> **Important**
>
> Le risorse create utilizzando la modalità Sviluppatore possono essere gestite da AMS Advanced solo se vengono create utilizzando i processi di gestione delle modifiche di AMS Advanced.

La modalità sviluppatore è una delle modalità AMS Advanced che puoi utilizzare. Per ulteriori informazioni, consulta Panoramica delle modalità.

Guida introduttiva alla modalità AMS Advanced Developer

Scopri i vari account AMS Advanced con la modalità AMS Advanced Developer e come implementare con successo la modalità Sviluppatore.

Argomenti

- Prima di iniziare con la modalità AMS Developer
- Prerequisiti per la modalità AMS Developer
- Come implementare la modalità AMS Advanced Developer
- Autorizzazioni in modalità AMS Advanced Developer

Prima di iniziare con la modalità AMS Developer

Prima di implementare la modalità Sviluppatore, ci sono alcune cose che dovresti sapere.

AMS Advanced non è in grado di gestire gli stack o le risorse esistenti in un DevMode account creato al di fuori del processo di gestione delle modifiche di AMS Advanced tramite richieste di modifica (RFCs). Tuttavia, mentre l'account è attivo DevMode, AMS Advanced continua a gestire le risorse fornite tramite il processo di gestione delle modifiche di AMS Advanced con. RFCs

Non è possibile iniziare con un DevMode account e successivamente convertirlo in un account di applicazione gestito da AMS Advanced.

Prerequisiti per la modalità AMS Developer

Di seguito sono riportati i prerequisiti per l'implementazione della modalità Sviluppatore:

- Devi essere un cliente AMS Advanced con almeno un account AMS Advanced Plus o Premium registrato.

- Qualsiasi account utilizzato deve essere un account AMS Advanced Plus o Premium.
- Multi-Account Landing Zone (MALZ): è necessario utilizzare il ruolo `AWSManagedServicesDevelopmentRole` predefinito AWS Identity and Access Management (IAM). Richiedete questo ruolo. La sezione successiva descrive come acquisire le autorizzazioni in modalità Sviluppatore.
- Single-Account Landing Zone (SALZ): è necessario utilizzare il ruolo `customer_developer_role` predefinito AWS Identity and Access Management (IAM). Richiedete questo ruolo. La sezione successiva descrive come acquisire le autorizzazioni in modalità Sviluppatore.

Come implementare la modalità AMS Advanced Developer

Implementate la modalità Developer richiedendo che al vostro account AMS Advanced idoneo venga assegnato il ruolo IAM predefinito:

- MALZ: `AWSManagedServicesDevelopmentRole`
- SALE: `customer_developer_role`

Quindi assegni il ruolo agli utenti pertinenti nella tua rete federata.

AMS Advanced consiglia di assicurarsi che l'uso della modalità Sviluppatore sia conforme ai framework e agli standard di controllo interni in quanto la modalità Sviluppatore crea due vettori di cambiamento: AMS Advanced change management per AMS Advanced e federazione dei ruoli gestita dal cliente per le risorse che, in qualità di nostro cliente, gestisci. Sebbene i processi AMS Advanced rimangano conformi alle nostre dichiarazioni, potrebbe essere necessario aggiornare i processi e i quadri di controllo dei clienti.

Per implementare la modalità Sviluppatore nel tuo account AMS Advanced

1. Verifica che l'account che desideri utilizzare con la modalità Sviluppatore soddisfi i requisiti elencati inPrerequisiti per la modalità AMS Developer.
2. Invia una richiesta di modifica (RFC) utilizzando la modalità Gestione del tipo di modifica (CT) | Account gestito | Modalità sviluppatore | Abilita (automazione gestita). Per un esempio di come utilizzare questo CT, vedi Developer Mode | Enable (Managed Automation).

Dopo l'elaborazione del CT, il ruolo IAM predefinito (`AWSManagedServicesDevelopmentRole`per MALZ, `customer_developer_role` per SALZ) viene fornito nell'account richiesto.

3. Assegna il ruolo appropriato agli utenti che richiedono l'accesso in modalità Sviluppatore utilizzando il processo di federazione interno.

   AMS Advanced consiglia di limitare l'accesso per evitare la fornitura o la modifica delle risorse indesiderate o non approvate.

Autorizzazioni in modalità AMS Advanced Developer

Il ruolo predefinito (`AWSManagedServicesDevelopmentRole`per MALZ, **`customer_developer_role`** per SALZ) concede l'autorizzazione a creare risorse di infrastruttura applicativa all'interno di AMS Advanced VPC, inclusi i ruoli IAM, limitando al contempo l'accesso ai componenti di servizio condivisi gestiti da AMS Advanced (ad esempio, host di gestione, controller di dominio, Trend Micro EPS, bastioni e servizi AWS non supportati). Il ruolo limita anche l'accesso ai seguenti registri Servizi AWS: Amazon GuardDuty e AMS Advanced. AWS Organizations AWS Directory Service APIs

Sebbene il ruolo consenta di creare ruoli IAM aggiuntivi, gli stessi limiti di autorizzazione inclusi nell'accesso in modalità Sviluppatore vengono applicati a qualsiasi ruolo IAM creato da. `AWSManagedServicesDevelopmentRole`

Sicurezza e conformità in modalità Sviluppatore

La sicurezza e la conformità sono una responsabilità condivisa tra AMS Advanced e te come nostro cliente. La modalità AMS Advanced Developer trasferisce all'utente la responsabilità condivisa per le risorse fornite al di fuori del processo di gestione delle modifiche o fornite tramite la gestione delle modifiche ma aggiornate con le autorizzazioni della modalità Sviluppatore. Per ulteriori informazioni sulla responsabilità condivisa, consulta AWS Managed Services.

Avvertenze:

- DevMode consente a te e al tuo team autorizzato di aggirare i deny-by-default principi alla base della sicurezza AMS. I vantaggi, il self-service e la riduzione dei tempi di attesa per AMS devono essere soppesati rispetto agli svantaggi: chiunque può eseguire azioni impreviste e distruttive all'insaputa del proprio team di sicurezza. I tipi di modifiche automatiche per abilitare la modalità

Dev e la modalità Direct Change sono esposti e qualsiasi persona autorizzata dell'organizzazione può eseguirli CTs e abilitarli.

- Sei responsabile della gestione delle autorizzazioni di esecuzione CT dalla tua base di utenti.
- AMS non gestisce i permessi di esecuzione CT

Raccomandazioni:

- Proteggere
  - I clienti possono impedire l'accesso a questo CT tramite autorizzazioni, vedi Restrict permissions with IAM role policy statements
  - Impedisci l'accesso a questo CT implementando un proxy come un sistema ITSM
  - Utilizza politiche di controllo del servizio (SCPs) che impediscono politiche e comportamenti secondo necessità, vedi AMS Preventative and Detective Controls Library
- Rileva
  - Monitora le tue RFC per verificare che queste CTs (abilita la modalità sviluppatore ct-1opjmhuddw194 e la modalità Direct change, abilita ct-3rd4781c2nnhp) vengano eseguite e rispondi di conseguenza
  - Esamina e and/or verifica la presenza delle risorse IAM nei tuoi account per identificare quegli account in cui sono state implementate la modalità Developer o la modalità Direct Change
- Rispondi
  - Se necessario, rimuovi gli account in modalità Sviluppatore

Sicurezza in modalità Sviluppatore

AMS Advanced offre un valore aggiunto con una landing zone prescrittiva, un sistema di gestione delle modifiche e una gestione degli accessi. Quando si utilizza la modalità Sviluppatore, il valore di sicurezza di AMS Advanced viene mantenuto utilizzando la stessa configurazione degli account AMS Advanced standard che stabilisce la rete di base con protezione avanzata AMS Advanced. La rete è protetta dal limite di autorizzazioni applicato nel ruolo (`AWSManagedServicesDevelopmentRole`per MALZ, **`customer_developer_role`** per SALZ), che impedisce all'utente di scomporre le protezioni dei parametri stabilite al momento della configurazione dell'account.

Ad esempio, gli utenti con il ruolo possono accedere ad Amazon Route 53 ma la zona ospitata interna di AMS Advanced è limitata. Gli stessi limiti di autorizzazione

vengono applicati a un ruolo IAM creato da, applicando i limiti di autorizzazione su theAWSManagedServicesDevelopmentRole, AWSManagedServicesDevelopmentRole che impedisce all'utente di scomporre le protezioni dei parametri stabilite al momento dell'onboarding dell'account su AMS Advanced.

Conformità in modalità Sviluppatore

La modalità sviluppatore è compatibile con i carichi di lavoro di produzione e non di produzione. È responsabilità dell'utente garantire il rispetto di tutti gli standard di conformità (ad esempio, PHI, HIPAA, PCI) e garantire che l'uso della modalità Sviluppatore sia conforme ai framework e agli standard di controllo interni.

Gestione delle modifiche in modalità Sviluppatore

La gestione delle modifiche è il processo utilizzato dal servizio AMS Advanced per implementare le richieste di modifica. Una richiesta di modifica (RFC) è una richiesta creata dall'utente o da AMS Advanced tramite l'interfaccia AMS Advanced per apportare una modifica all'ambiente gestito e include un ID del tipo di modifica (CT) per una particolare operazione. Per ulteriori informazioni, consulta Modifiche alle modalità di gestione.

La gestione delle modifiche non viene applicata negli account AMS Advanced a cui sono concesse le autorizzazioni in modalità Sviluppatore. Gli utenti a cui è stata concessa l'autorizzazione in modalità Sviluppatore con il ruolo IAM (`AWSManagedServicesDevelopmentRole`per MALZ, `customer_developer_role` per SALZ), possono utilizzare l'accesso AWS API nativo per fornire e apportare modifiche alle risorse nei propri account AMS Advanced. Gli utenti che non hanno il ruolo appropriato in questi account devono utilizzare il processo di gestione delle modifiche di AMS Advanced per apportare modifiche.

> **Important**
>
> Le risorse create utilizzando la modalità Sviluppatore possono essere gestite da AMS Advanced solo se vengono create utilizzando i processi di gestione delle modifiche di AMS Advanced. Le richieste di modifiche inviate ad AMS Advanced per risorse create al di fuori del processo di gestione delle modifiche di AMS Advanced vengono rifiutate da AMS Advanced perché devono essere gestite dall'utente.

Restrizioni dell'API per i servizi di provisioning self-service

Tutti i servizi autoforniti da AMS Advanced sono supportati dalla modalità Sviluppatore. L'accesso ai servizi forniti autonomamente è soggetto alle limitazioni descritte nelle rispettive sezioni della guida per l'utente per ciascuno di essi. Se un servizio con fornitura automatica non è disponibile con il ruolo in modalità Sviluppatore, puoi richiedere un ruolo aggiornato tramite il tipo di modifica della modalità Sviluppatore.

I seguenti servizi non forniscono l'accesso completo al servizio: APIs

Servizi forniti autonomamente limitati in modalità Sviluppatore

Servizio	Note
Amazon API Gateway	Tutte le APIs chiamate Gateway sono consentite tranne. `SetWebACL`
Application Auto Scaling	Può solo registrare o annullare la registrazione di obiettivi scalabili e inserire o eliminare una politica di scalabilità.
AWS CloudFormation	Non è possibile accedere o modificare gli CloudFormation stack il cui nome è preceduto da. `mc-`
AWS CloudTrail	Non è possibile accedere o modificare CloudTrail risorse il cui nome è preceduto da. `ams-` and/or `mc-`
Amazon Cognito (pool di utenti)	Impossibile associare token software. Impossibile creare pool di utenti, processi di importazione utenti, server di risorse o provider di identità.
AWS Directory Service	Solo le seguenti Directory Service azioni sono richieste da `Connect` and `WorkSpaces` services. Tutte le altre azioni del Directory Service sono negate dalla politica sui limiti delle autorizzazioni della modalità Sviluppatore:

Servizio	Note
	• ds:AuthorizeApplication • ds:CreateAlias • ds:CreateIdentityPoolDirectory • ds:DeleteDirectory • ds:DescribeDirectories • ds:GetAuthorizedApplication Details • ds:ListAuthorizedApplications • ds:UnauthorizeApplication Negli account di landing zone con account singolo, la politica di confine nega esplicita mente l'accesso alla directory gestita di AMS Advanced utilizzata da AMS Advanced per mantenere l'accesso agli account abilitati alla modalità sviluppo.
Amazon Elastic Compute Cloud	Impossibile accedere ad Amazon EC2 APIs che contiene la stringa: DhcpOptio ns Gateway,Subnet,VPC, eVPN. Non è possibile accedere o modificare EC2 le risorse Amazon con un tag preceduto daAMS, mcManagementHostASG , and/or sentinel.
Amazon EC2 (rapporti)	È concesso solo l'accesso alla visualizzazione (non è possibile modificare). Nota: Amazon EC2 Reports si sta trasferendo. La voce del menu Report verrà rimossa dal menu di navigazione EC2 della console Amazon. Per visualizzare i report EC2 sull'utilizzo di Amazon dopo la rimozione, usa la console AWS Billing and Cost Management.

Servizio	Note
AWS Identity and Access Management (IAM)	Non è possibile eliminare i limiti di autorizzazione esistenti o modificare le politiche relative alle password degli utenti IAM. Non è possibile creare o modificare risorse IAM a meno che non si utilizzi il ruolo IAM corretto (`AWSManagedServicesDevelopmentRole` per MALZ, `customer_developer_role` per SALZ)). Non è possibile modificare le risorse IAM con il prefisso:`ams`,,,`mc`. `customer_deny_policy` and/or `sentinel` Quando si crea una nuova risorsa IAM (ruolo, utente o gruppo), è necessario allegare il limite di autorizzazione (MALZ:`AWSManagedServicesDevelopmentRolePermissionsBoundary`, SALZ:`ams-app-infra-permissions-boundary`).
AWS Key Management Service (AWS KMS)	Impossibile accedere o modificare le chiavi KMS gestite da AMS Advanced.
AWS Lambda	Non è possibile accedere o modificare le AWS Lambda funzioni che hanno il prefisso con. `AMS`
CloudWatch Registri	Impossibile accedere ai flussi di CloudWatch log il cui nome è preceduto da:`mc`,,,`aws.lambda` and/or `AMS`
Amazon Relational Database Service (Amazon RDS)	Non è possibile accedere o modificare i database Amazon Relational Database Service (Amazon RDS) DBs () con un nome preceduto da:. `mc-`

Servizio	Note
AWS Resource Groups	Può accedere solo alle azioni `Get` API `List` di `Search` Resource Group e.
Amazon Route 53	Impossibile accedere o modificare le risorse gestite da Route53 AMS Advanced.
Amazon S3	Non è possibile accedere ai bucket Amazon S3 il cui nome è preceduto da:`ams-*`,, `ams` o. `ms-a` `mc-a`
AWS Security Token Service	L'unica API del servizio di token di sicurezza consentita è. `DecodeAuthorizationMessage`
Amazon SNS	Impossibile accedere agli argomenti SNS il cui nome è preceduto da: `AMS-Energon-Topic` , o. `MMS-Topic`
AWS Systems Manager Gestore (SSM)	Impossibile modificare i parametri SSM con il prefisso`ams`, `mc` o. `svc` Non è possibile utilizzare l'API SSM `SendCommand` con EC2 istanze Amazon con un tag preceduto da o. `ams` `mc`
AWS Etichettatura	Hai accesso solo alle azioni dell'API di AWS tagging con il prefisso. `Get`

Servizio	Note
AWS Lake Formation	Le seguenti azioni AWS Lake Formation API sono negate: • `lakeformation:DescribeResource` • `lakeformation:GetDataLakeSettings` • `lakeformation:DeregisterResource` • `lakeformation:RegisterResource` • `lakeformation:UpdateResource` • `lakeformation:PutDataLakeSettings`
Amazon Elastic Inference	Puoi chiamare solo l'azione dell'API Elastic Inference. `elastic-inference:Connect` Questa autorizzazione è inclusa nel `customer_sagemaker_admin_policy` file allegato a. `customer_sagemaker_admin_role` Questa azione consente di accedere all'acceleratore Elastic Inference.
AWS Shield	Nessun accesso a nessuno di questi servizi APIs o console.
Amazon Simple Workflow Service	Nessun accesso a nessuno di questi servizi APIs o console.

Provisioning dell'infrastruttura in modalità AMS Developer

Gli utenti che non dispongono del ruolo IAM in modalità SviluppatoreAWSManagedServicesDevelopmentRole, negli account in cui è abilitata la modalità Sviluppatore, devono seguire il processo di gestione delle modifiche di AMS Advanced che sfrutta AMS Advanced. AMIs Gli utenti con il ruolo corretto (MALZ:**AWSManagedServicesDevelopmentRole**, SALZ:customer_developer_role) possono

utilizzare il sistema di gestione delle modifiche AMS Advanced e AMS Advanced AMIs ma non sono obbligati a farlo.

> **Note**
>
> Un' AWS AMI che non è stata elaborata tramite l'inserimento di carichi di lavoro AMS Advanced o creata in un account AMS Advanced, non includerà le configurazioni richieste da AMS Advanced.

Controlli Detective in modalità AMS Developer

Questa sezione è stata redatta perché contiene informazioni sensibili relative alla sicurezza di AMS. Queste informazioni sono disponibili nella documentazione della console AMS. Per accedere ad AWS Artifact, puoi contattare il tuo CSDM per ricevere istruzioni o andare alla pagina Getting Started with AWS Artifact.

Registrazione, monitoraggio e gestione degli eventi in modalità AMS Developer

La registrazione, il monitoraggio e la gestione degli eventi non sono disponibili per le risorse fornite al di fuori del processo di gestione delle modifiche di AMS Advanced o per le risorse fornite tramite la gestione delle modifiche e successivamente modificate da un account che utilizza le autorizzazioni in modalità Sviluppatore.

Gestione degli incidenti in modalità AMS Developer

Nessuna modifica ai tempi di risposta agli incidenti. La risoluzione degli incidenti è il modo migliore per le risorse fornite al di fuori del processo di gestione delle modifiche o per le risorse fornite tramite la gestione delle modifiche e quindi modificate da un account utilizzando le autorizzazioni della modalità Sviluppatore.

> **Note**
>
> L'accordo sul livello di servizio (SLA) di AMS non si applica alle risorse create o aggiornate al di fuori del sistema di gestione delle modifiche AMS (richieste di modifica o RFCs), inclusa

la modalità sviluppatore; pertanto, le risorse aggiornate o create in modalità sviluppatore vengono automaticamente degradate a un P3 e il supporto AMS è il massimo sforzo.

Gestione delle patch in modalità AMS Developer

La gestione delle patch non è disponibile per le risorse fornite al di fuori del processo di gestione delle modifiche AMS Advanced o per le risorse fornite tramite la gestione delle modifiche e successivamente modificate da un account che utilizza le autorizzazioni in modalità Sviluppatore. Tempi di applicazione delle patch:

- Per un aggiornamento di sicurezza fondamentale: entro 10 giorni lavorativi dal rilascio da parte del fornitore per le risorse fornite tramite la gestione delle modifiche e successivamente modificate da un account che utilizza le autorizzazioni della modalità Sviluppatore.
- Per un aggiornamento importante: entro 2 mesi dal rilascio da parte del fornitore per le risorse fornite tramite la gestione delle modifiche e successivamente modificate da un account che utilizza le autorizzazioni in modalità Sviluppatore.

Gestione della continuità in modalità AMS Developer

La gestione della continuità non è disponibile per le risorse fornite al di fuori del processo di gestione delle modifiche AMS Advanced o per le risorse fornite tramite la gestione delle modifiche e successivamente modificate da un account che utilizza le autorizzazioni della modalità Sviluppatore.

Il tempo di avvio del ripristino dell'ambiente può richiedere fino a 12 ore per le risorse fornite al di fuori del processo di gestione delle modifiche di AMS Advanced o per le risorse fornite tramite la gestione delle modifiche e successivamente modificate da un account che utilizza le autorizzazioni in modalità Sviluppatore.

Gestione della sicurezza e degli accessi in modalità AMS Developer

La protezione antimalware è tua responsabilità per le risorse fornite al di fuori del processo di gestione delle modifiche AMS Advanced o per le risorse fornite tramite la gestione delle modifiche e poi modificate da un account utilizzando le autorizzazioni della modalità Sviluppatore. L'accesso alle istanze Amazon Elastic Compute Cloud (Amazon EC2) non fornite tramite AMS Advanced Change Management potrebbe essere controllato da coppie di chiavi anziché fornire un accesso federato.

Modalità Self-Service Provisioning in AMS

La modalità Self-Service Provisioning (SSP) di AWS Managed Services (AMS) fornisce l'accesso completo alle funzionalità native di AWS servizi e API negli account gestiti AMS. Puoi accedere ai servizi tramite ruoli standardizzati e limitati. AWS Identity and Access Management AMS fornisce richieste di assistenza e gestione degli incidenti. Gli avvisi, il monitoraggio, la registrazione, le patch, il backup e la gestione delle modifiche sono responsabilità dell'utente. In molti casi, i servizi Self-Service Provisioning (SSPS) sono autogestiti o senza server e non richiedono la gestione di determinate attività operative come l'applicazione di patch. Potete trarre vantaggio dall'utilizzo di questi servizi entro i limiti dell'ambiente definiti dai guardrails di AMS e qualsiasi modifica IAM (inclusi ruoli collegati ai servizi, ruoli di servizio, ruoli tra account o aggiornamenti delle policy) deve essere approvata da AMS Operations per mantenere la sicurezza di base della piattaforma. È possibile sfruttare i CloudFormation modelli per automatizzare l'implementazione di questi servizi, ma ciò non è supportato per tutti i servizi SSP.

> **Important**
>
> Usa la modalità SSP nei tuoi account AWS Managed Services (AMS) per accedere e utilizzare AWS i servizi, con le restrizioni indicate.

Ce ne sono alcuni Servizi AWS che puoi usare senza la gestione di AMS, nel tuo account AMS. I servizi in modalità Self-Service Provisioning, o SSPS in breve, spiegano come aggiungerli all'account AMS e FAQs per ciascuno di essi sono descritti nella sezione.

I servizi di provisioning self-service vengono offerti così come sono e l'utente è responsabile della loro gestione. AMS non fornisce avvisi, monitoraggio, registrazione o applicazione di patch per le risorse associate a tali servizi. AMS fornisce ruoli IAM che consentono di utilizzare il servizio nel proprio account AMS in modo sicuro. AMS SLAs non si applicano.

Per le risorse fornite in modalità self-service, AMS fornisce la gestione degli incidenti, i controlli e le barriere investigative, la reportistica, le risorse designate (Cloud Service Delivery Manager e Cloud Architect), la sicurezza e l'accesso e il supporto tecnico tramite le richieste di assistenza. Inoltre, ove applicabile, l'utente si assume la responsabilità della gestione della continuità, della gestione delle patch, del monitoraggio dell'infrastruttura e della gestione delle modifiche per le risorse fornite o configurate al di fuori del sistema di gestione delle modifiche AMS.

Guida introduttiva alla modalità SSP in AMS

Il self-service provisioning è una delle modalità AMS per multi-account landing zone (MALZ) che puoi utilizzare. Per ulteriori informazioni, consulta Panoramica delle modalità.

Per fornire funzionalità di provisioning self-service, AMS ha creato ruoli IAM elevati con limiti di autorizzazione per limitare le modifiche involontarie dovute all'accesso diretto. Servizio AWS I ruoli non impediscono tutte le modifiche e devi rispettare i controlli interni e le politiche di conformità e verificare che tutti Servizi AWS quelli utilizzati soddisfino le certificazioni richieste. Questa è la modalità di provisioning self-service. Per i dettagli sui requisiti di AWS conformità, consulta AWS Conformità.

Per aggiungere un servizio di provisioning self-service all'account dell'applicazione multi-account landing zone, utilizza il Management | AWS service | Self-provisioned service | Add change type (CT), ovvero CT (CT) per la revisione o CT automatizzato, come indicato per il servizio.

> **Note**
>
> Per richiedere ad AMS di fornire un servizio di fornitura self-service aggiuntivo, invia una richiesta di servizio.

Usa AMS SSP per effettuare il provisioning di Amazon API Gateway nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon API Gateway direttamente nel tuo account gestito AMS. Amazon API Gateway è un servizio completamente gestito che semplifica per gli sviluppatori la creazione, la pubblicazione, la manutenzione, il monitoraggio e la protezione APIs su qualsiasi scala. Console di gestione AWS Puoi creare REST WebSocket APIs che fungano da porta d'ingresso per consentire alle applicazioni di accedere ai dati, alla logica di business o alle funzionalità dei tuoi servizi di back-end, come carichi di lavoro in esecuzione su Amazon Elastic Compute Cloud (Amazon EC2), codice in esecuzione su AWS Lambdaqualsiasi applicazione Web o applicazioni di comunicazione in tempo reale.

API Gateway gestisce tutte le attività legate all'accettazione e all'elaborazione di centinaia di migliaia di chiamate API simultanee, tra cui la gestione del traffico, il controllo delle autorizzazioni e degli accessi, il monitoraggio e la gestione delle versioni delle API. API Gateway non prevede tariffe minime o costi di avvio. Paghi solo per le chiamate API che ricevi e per la quantità di dati trasferiti

in uscita e, con il modello di prezzo a più livelli di API Gateway, puoi ridurre i costi man mano che l'utilizzo dell'API aumenta. Per ulteriori informazioni, consulta Amazon API Gateway.

Domande frequenti: API Gateway in AMS

D: Come posso richiedere l'accesso ad Amazon API Gateway nel mio account AMS?

Richiedi l'accesso ad API Gateway inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli IAM al tuo account: e. `customer_apigateway_author_role` `customer_apigateway_cloudwatch_role` Dopo aver effettuato il provisioning nel tuo account, devi integrare i ruoli nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon API Gateway nel mio account AMS?

- La configurazione dell'API Gateway è limitata alle risorse prive `AMS-` di `MC-` prefissi per impedire modifiche all'infrastruttura AMS.
- `CREATE`i privilegi per VPCLink sono disabilitati per impedire la creazione non regolamentata di Elastic Load Balancers. VPCLinks Se necessario, vedere Application Load Balancer | Create.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon API Gateway nel mio account AMS?

Dipende dal tipo di API Gateway che desideri implementare. Può essere un servizio autonomo, ma può anche richiedere l'accesso a servizi esistenti (ad esempio, network load balancer).

Usa AMS SSP per fornire Alexa for Business nel tuo account AMS

Usa la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Alexa for Business direttamente dal tuo account gestito AMS. Alexa for Business è un servizio che consente alla tua organizzazione e ai tuoi dipendenti di utilizzare Alexa per svolgere più lavoro. Con Alexa for Business, puoi usare Alexa come assistente intelligente per essere più produttivo nelle sale riunioni, alla scrivania e persino con i dispositivi Alexa che già usi a casa o in viaggio. I responsabili IT e delle strutture possono utilizzare Alexa for Business per misurare e aumentare l'utilizzo delle sale riunioni esistenti sul posto di lavoro.

Per saperne di più, consulta Alexa for Business.

Domande frequenti su Alexa for Business in AWS Managed Services

D: Come posso richiedere l'accesso ad Alexa for Business nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_alexa_console_role` seguente ruolo IAM al tuo account:. A `customer_alexa_device_setup_user` è stato creato anche per lo strumento di configurazione dei dispositivi fornito da Alexa for Business; questo strumento di configurazione del dispositivo può quindi essere utilizzato per configurare i dispositivi. Una volta effettuato il provisioning nel tuo account, devi inserire i ruoli nella tua soluzione federativa.

Il gateway Alexa for Business ti consente di connettere Alexa for Business agli endpoint Cisco Webex e Poly Group Series per controllare le riunioni con la tua voce. Il software gateway viene eseguito sull'hardware locale e invia in modo sicuro le direttive di conferenza da Alexa for Business all'endpoint Cisco. Il gateway richiede due coppie di AWS credenziali per comunicare con Alexa for Business. Offriamo due utenti IAM ad accesso limitato: `customer_alexa_gateway_installer_user` e `customer_alexa_gateway_execution_user` per i tuoi gateway Alexa for Business, uno per l'installazione del gateway e uno per il funzionamento del gateway; questi possono essere richiesti inviando una RFC con il tipo di modifica Deployment | Advanced stack components | Identity and Access Management (IAM) and Access Management (IAM) | Create entità o policy (automazione gestita) (ct-3dpd8mdd9jn1r).

> **Note**
>
> Per generare report sull'utilizzo e inviarli ad Amazon S3, specifica il nome del bucket Amazon S3 nella RFC del servizio self-provisioned.

D: Quali sono le restrizioni all'uso di Alexa for Business nel mio account AMS?

Non ci sono restrizioni. La funzionalità completa di Alexa for Business è disponibile con il ruolo di servizio self-provisioned Alexa for Business.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Alexa for Business nel mio account AMS?

- Se intendi utilizzare WPA2 Enterprise Wi-Fi per configurare i dispositivi condivisi, specifica questo tipo di sicurezza di rete nello Strumento di configurazione del dispositivo, per il quale è richiesto un AWS Autorità di certificazione privata .

- AMS crea solo chiavi segrete che iniziano con lo spazio dei nomi «A4B». Questo è restrittivo solo per questo spazio dei nomi.

D: Quali funzionalità di Alexa for Business richiedono RFCs separatamente?

Per registrare un dispositivo Alexa Voice Service (AVS) con Alexa for Business, fornisci l'accesso al produttore di dispositivi integrato Alexa. A tale scopo, è necessario creare un ruolo IAM nella console Alexa for Business che può essere distribuito utilizzando il tipo di modifica Gestione | Altro | Altro. Ciò consente al produttore di dispositivi AVS di registrare e gestire i dispositivi con Alexa for Business per tuo conto.

Usa AMS SSP per effettuare il provisioning WorkSpaces delle applicazioni Amazon nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon WorkSpaces Applications (WorkSpaces Applications) direttamente nel tuo account gestito AMS. WorkSpaces Applications ti consente di spostare le tue applicazioni desktop in AWS, senza riscriverle. È possibile installare le applicazioni in WorkSpaces Applicazioni, impostare configurazioni di avvio e rendere le applicazioni disponibili agli utenti. WorkSpaces Applications offre un'ampia selezione di opzioni di macchine virtuali in modo da poter selezionare il tipo di istanza più adatto ai requisiti dell'applicazione e impostare i parametri di scalabilità automatica in modo da soddisfare facilmente le esigenze degli utenti finali. WorkSpaces Applications consente di avviare applicazioni nella propria rete, il che significa che le applicazioni possono interagire con le AWS risorse esistenti.

Amazon WorkSpaces Applications ti consente di installare, testare e aggiornare le tue applicazioni in modo rapido e semplice utilizzando il generatore di immagini. Qualsiasi applicazione eseguita su Microsoft Windows Server 2012 R2, Windows Server 2016 o Windows Server 2019 è supportata e non è necessario apportare alcuna modifica. Una volta completato il test, puoi impostare le configurazioni di avvio dell'applicazione, le impostazioni utente predefinite e pubblicare l'immagine per consentire agli utenti di accedervi.

Per ulteriori informazioni, consulta WorkSpaces Applicazioni.

WorkSpaces Domande frequenti sulle applicazioni in AWS Managed Services

D: Come posso richiedere l'accesso alle WorkSpaces applicazioni nel mio account AMS?

Richiedi l'accesso alle WorkSpaces applicazioni inviando una RFC tramite Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-3qe6io8t6jtny). Questa RFC fornisce `customer_appstream_console_role` il seguente ruolo IAM al tuo account:.

A `customer_appstream_stream_role` viene inoltre distribuito per lo streaming di applicazioni che richiedono l'autenticazione degli utenti utilizzando le proprie credenziali di accesso ad Active Directory.

Una volta effettuato il provisioning nel tuo account, devi inserire i ruoli nella tua soluzione di federazione.

D: Quali sono le restrizioni all'utilizzo delle WorkSpaces applicazioni nel mio account AMS?

- Le seguenti funzionalità devono essere configurate dal team di AMS Support e richiedono specifiche RFCs. Le istruzioni sulla richiesta di funzionalità aggiuntive sono disponibili nella sezione 4.
  - Creazione e streaming dagli endpoint VPC dell'interfaccia.
  - Support per gli endpoint Amazon S3 per le cartelle home e la persistenza delle impostazioni delle applicazioni su una rete privata.
  - Creazione e scelta del ruolo IAM che sarà disponibile su tutte le istanze di streaming del parco istanze.
  - Unire WorkSpaces le flotte di applicazioni e i domini Microsoft Active Directory dei generatori di immagini.
  - Creazione di report di WorkSpaces utilizzo personalizzati per le applicazioni.
  - Il branding personalizzato non è attualmente supportato.

D: Quali sono i prerequisiti o le dipendenze per utilizzare le WorkSpaces applicazioni nel mio account AMS?

Durante l'invio della RFC alle WorkSpaces applicazioni di bordo, includi il nome del bucket Amazon S3 da utilizzare per il report sull'utilizzo delle applicazioni. WorkSpaces Il nome del bucket viene aggiunto a quello creato durante l'onboarding `customer-appstream-usagereports-policy` di Applications. WorkSpaces

D: Quali funzionalità WorkSpaces delle applicazioni richiede una funzionalità separata? RFCs

- Per scegliere un endpoint VPC di interfaccia per WorkSpaces le applicazioni, invia un tipo di modifica Gestione | Altro | Altro | Aggiornamento RFC per creare un endpoint VPC nel tuo account.

Per i passaggi per creare endpoint personalizzati per WorkSpaces le applicazioni, consulta Creazione e streaming dagli endpoint VPC dell'interfaccia nella guida utente WorkSpaces delle applicazioni.

- Il supporto per gli endpoint Amazon S3 per le cartelle home e la persistenza delle impostazioni delle applicazioni su una rete privata possono essere configurati richiedendo gli endpoint VPC Amazon S3 con un RFC Management | Other | Other | Create change type. La RFC deve includere rispettivamente il bucket Amazon S3 di destinazione che ospita il contenuto della cartella home o i bucket Amazon S3 delle impostazioni dell'applicazione. Questa RFC fornirà WorkSpaces alle applicazioni le autorizzazioni necessarie per accedere agli endpoint VPC di Amazon S3. Per i passaggi per creare endpoint personalizzati per gli stream, consulta Using Amazon S3 VPC Endpoints for Home Folders and Application Settings Persistence nella guida per l'utente delle applicazioni. WorkSpaces
- Per creare e scegliere un ruolo IAM che sarà disponibile su tutte le istanze di streaming del parco istanze, invia una RFC Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entità o policy (automazione gestita) (ct-3dpd8mdd9jn1r) richiedendo il ruolo IAM con la policy richiesta. Il nome del ruolo IAM deve sempre iniziare con il prefisso: «customer_appstream».
- WorkSpaces Le flotte e i generatori di immagini di Amazon Applications possono essere aggiunti ai domini in Microsoft Active Directory inviando un RFC di modifica di tipo Management | Other | Other | Update per la creazione dell'account di servizio in Active Directory (AD). Le autorizzazioni minime richieste per accedere a Microsoft Active Directory sono definite nella documentazione delle WorkSpaces applicazioni in Concessione delle autorizzazioni per la creazione e la gestione di oggetti informatici Active Directory.
- Per creare report personalizzati sull'utilizzo WorkSpaces delle applicazioni, invia un tipo RFC di gestione | Altro | Altro | Crea modifica richiedendo quanto segue:
  - "AppStreamUsageReports" Creazione dello stack CFN
  - «customer_appstream_usagereports_role» deve essere inserito nell'account
  - Fornisci inoltre i seguenti dettagli:
    - Fornisci l'espressione CRON per pianificare l'esecuzione del Crawler. Per impostazione predefinita, è alle 23:00 UTC di tutti i giorni.
    - ARN del bucket Amazon S3 da utilizzare per i risultati delle query Athena. Questo bucket deve avere il prefisso: `aws-athena-query-results`
    - Registri dei report sull'utilizzo dell'ARN WorkSpaces for Applications del bucket Amazon S3.

Una volta assegnato il ruolo, inserisci il ruolo nella tua soluzione di federazione ed effettua il login, quindi accedi e AWS GlueAWS Glue Athena per generare report personalizzati utilizzando il ruolo del rapporto di utilizzo. Per informazioni dettagliate sull'utilizzo dei report sull'utilizzo WorkSpaces delle applicazioni, consulta Creare report personalizzati e analizzare i dati sull'utilizzo WorkSpaces delle applicazioni, nella documentazione delle WorkSpaces applicazioni.

Usa AMS SSP per effettuare il provisioning di Amazon Athena nel tuo account AMS

Usa la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Athena (Athena) direttamente nel tuo account gestito AMS. Athena è un servizio di interrogazione interattivo che ti aiuta ad analizzare i dati in Amazon S3 utilizzando SQL standard. Athena è un servizio serverless, perciò non occorre installare o gestire alcuna infrastruttura e vengono addebitati solo i costi relativi all'esecuzione delle query. Indichi i tuoi dati in Amazon S3, definisci lo schema e inizi a eseguire query utilizzando SQL standard. La maggior parte dei risultati viene fornita in pochi secondi. Con Athena, non sono necessari lavori complessi extract-transform-load (ETL) per preparare i dati per l'analisi. In questo modo, chiunque abbia competenze SQL può analizzare rapidamente set di dati su larga scala in modo semplice. Per ulteriori informazioni, consulta Amazon Athena.

Domande frequenti: Athena in AMS

D: Come posso richiedere l'accesso ad Amazon Athena nel mio account AMS?

Richiedi l'accesso ad Athena inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC fornisce il `customer_athena_console_role` seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon Athena nel mio account AMS?

Non ci sono restrizioni. La funzionalità completa di Amazon Athena è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Athena nel mio account AMS?

Athena dipende in larga misura dal AWS Glue servizio, in quanto utilizza i dati catalog/metastore creati con. AWS Glue Pertanto, AWS Glue le autorizzazioni sono incluse nella RFC Athena di successo.

Il ruolo `customer_athena_console_role` ha un prerequisito per un bucket Amazon S3. Per creare un nuovo bucket, usa il CT automatizzato `ct-1a68ck03fn98r` (Deployment | Advanced stack components | S3 storage | Create). Quando si utilizza questo CT automatico per creare un bucket S3 per Athena, il nome del bucket deve iniziare con il prefisso. `athena-query-results-*`

Usa AMS SSP per effettuare il provisioning di Amazon Bedrock nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Bedrock direttamente nel tuo account gestito AMS. Amazon Bedrock è un servizio completamente gestito che rende AWS disponibili per l'uso modelli di base ad alte prestazioni (FMs) delle principali startup di intelligenza artificiale tramite un'API unificata. Puoi scegliere tra un'ampia gamma di modelli di fondazione per trovare il modello più adatto al tuo caso d'uso. Amazon Bedrock offre anche un'ampia gamma di funzionalità per compilare applicazioni di IA generativa con sicurezza, privacy e IA responsabile. Con Amazon Bedrock, puoi sperimentare e valutare facilmente i migliori modelli di fondazione per i tuoi casi d'uso, personalizzarli privatamente con i tuoi dati utilizzando tecniche come l'ottimizzazione e la Retrieval Augmented Generation (RAG) e creare agenti che eseguono attività utilizzando i tuoi sistemi e le tue origini dati aziendali.

Con l'esperienza serverless di Amazon Bedrock, puoi iniziare rapidamente, personalizzare privatamente i modelli di base con i tuoi dati e integrarli e distribuirli in modo semplice e sicuro nelle tue applicazioni utilizzando gli strumenti AWS senza dover gestire alcuna infrastruttura. Per maggiori informazioni, consulta Amazon Bedrock.

Domande frequenti: Amazon Bedrock in AMS

D: Come posso richiedere l'accesso ad Amazon Bedrock nel mio account AMS?

Per richiedere l'accesso ad Amazon Bedrock, invia una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce `customer_bedrock_console_role` il seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon Bedrock nel mio account AMS?

- Le knowledge base di Amazon Bedrock non sono supportate per impostazione predefinita come parte del ruolo SSPS a causa della sua dipendenza da OpenSearch Amazon Service Serverless, che attualmente non è supportato su AMS.
- Bedrock Studio non è supportato a causa della sua dipendenza da servizi non supportati come Amazon. DataZone

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Bedrock nel mio account AMS?

- Gli abbonamenti con modelli di terze parti che richiedono Marketplace AWS autorizzazioni devono essere eseguiti secondo il ruolo predefinito (`AWSManagedServicesAdminRole`su MALZ e su SALZ). `Customer_ReadOnly_Role` Questo perché il ruolo predefinito include le autorizzazioni. Marketplace AWS
- Se viene utilizzata la crittografia dei dati, è necessario fornire l'ARN della AWS KMS chiave quando si richiede la creazione del ruolo della console. Inoltre, il bucket Amazon S3 in uso deve avere «bedrock» nel nome.

Usa AMS SSP per effettuare il provisioning di Amazon CloudSearch nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle CloudSearch funzionalità di Amazon direttamente dal tuo account gestito AMS. Amazon CloudSearch è un servizio gestito nel AWS cloud che utilizzi per configurare, gestire e scalare in modo conveniente una soluzione di ricerca per il tuo sito Web o la tua applicazione. Amazon CloudSearch supporta 34 lingue e le funzioni di ricerca più diffuse come l'evidenziazione, il completamento automatico e la ricerca geospaziale. Per ulteriori informazioni, consulta Amazon CloudSearch.

> **Note**
>
> AWS ha chiuso l'accesso di nuovi clienti ad Amazon CloudSearch a partire dal 25 luglio 2024. I clienti CloudSearch esistenti di Amazon possono continuare a utilizzare il servizio normalmente. AWS continua a investire in sicurezza, disponibilità e miglioramenti delle prestazioni per Amazon CloudSearch, ma non abbiamo intenzione di introdurre nuove funzionalità.
> Per comprendere le differenze tra Amazon CloudSearch e Amazon OpenSearch Service e come passare a OpenSearch Service, contatta il tuo cloud architect (CA) per ricevere

assistenza. Per ulteriori informazioni sulla transizione al OpenSearch servizio Service, consulta Transition from Amazon CloudSearch to Amazon OpenSearch Service service.

Domande frequenti su Amazon CloudSearch in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon CloudSearch nel mio account AMS?

Richiedi l'accesso ad Amazon CloudSearch inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli IAM al tuo account: e. `customer_csearch_admin_role` `customer_csearch_dev_role` Dopo aver effettuato il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione di federazione.

D: Quali sono le restrizioni all'utilizzo di Amazon CloudSearch nel mio account AMS?

La funzionalità completa di Amazon CloudSearch è disponibile nel tuo account AMS. Tutte le soluzioni di database supportate da AMS sono attualmente supportate su Amazon. CloudSearch Tieni presente che, attualmente, DynamoDB è l'unica soluzione di database AWS gestita che non può essere indicizzata.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon CloudSearch nel mio account AMS?

Amazon CloudSearch dipende dalla collaborazione di Amazon S3 con gli Identity Provider per analizzare automaticamente i dati di input e determinare i campi della tabella. L'accesso ad Amazon S3 non è fornito con questa RFC e deve essere richiesto separatamente in una richiesta di servizio.

Usa AMS SSP per effettuare il provisioning di Amazon CloudWatch Synthetics nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Synthetics direttamente nel CloudWatch tuo account gestito AMS. Puoi usare Amazon CloudWatch Synthetics per creare «canaries» per monitorare i tuoi endpoint e. APIs

I Canaries sono script configurabili, scritti in Node.js o Python, che vengono eseguiti secondo una pianificazione. Creano funzioni Lambda nel tuo account che utilizzano Node.js o Python come framework. I canary funzionano su protocolli HTTP e HTTPS. Canaries verifica la disponibilità e la latenza degli endpoint e può archiviare dati sul tempo di caricamento e schermate dell'interfaccia

utente. Monitorano il REST APIs e il contenuto del sito Web e possono verificare eventuali modifiche non autorizzate dovute al phishing, all'iniezione di codice e al cross-site scripting. URLs

Le Canarie seguono gli stessi percorsi ed eseguono le stesse azioni dei clienti, consentendovi di verificare continuamente l'esperienza del cliente anche quando non c'è traffico di clienti sulle vostre applicazioni. Con i canary puoi scoprire i problemi prima che vengano rilevati dai clienti. Per ulteriori informazioni, consulta Amazon CloudWatch: utilizzo del monitoraggio sintetico.

Domande frequenti su Amazon CloudWatch Synthetics in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon CloudWatch Synthetics nel mio account AMS?

Richiedi l'accesso ad Amazon CloudWatch Synthetics inviando una RFC con il tipo di modifica Management AWS | service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC fornisce il seguente ruolo IAM al tuo account: 'customer_cw_synthetics_console_role' e 'customer_cw_synthetics_canary_lambda_role'. Una volta effettuato il provisioning nel tuo account, devi inserire il ruolo «customer_cw_synthetics_console_role» nella tua soluzione di federazione.

D: Quali sono le restrizioni all'uso di Amazon CloudWatch Synthetics nel mio account AMS?

Non ci sono restrizioni all'uso di Amazon CloudWatch Synthetics nel tuo account AMS.
È vietata la creazione di ruoli per i canari al di fuori del ruolo di servizio fornito da AMS «customer_cw_synthetics_canary_lambda_role».

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Synthetics CloudWatch nel mio account AMS?

Canaries crea e utilizza un bucket Amazon CloudWatch Synthetics S3 predefinito: "- -» cw-syn-results *${accountnumber}* *${default-region}*

Usa AMS SSP per effettuare il provisioning dei pool di utenti Amazon Cognito nel tuo account AMS

Usa la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità dei pool di utenti di Amazon Cognito direttamente nel tuo account gestito AMS. I pool di utenti di Amazon Cognito forniscono una directory utente sicura scalabile fino a centinaia di milioni di utenti. Essendo un servizio completamente gestito, i pool di utenti di Amazon Cognito possono essere configurati senza doversi preoccupare di dover installare l'infrastruttura server. Questo servizio consente di gestire un pool di utenti finali che è possibile utilizzare per l'integrazione con le applicazioni interne. Questo

servizio offre un'alternativa a un database personalizzato o a un elenco di utenti finali per applicazioni Web o mobili. Allo stesso tempo, i pool di utenti di Amazon Cognito forniscono il set completo di funzionalità di un servizio di directory, come le politiche sulle password, l'autenticazione a più fattori, il recupero delle password e l'iscrizione automatica ai servizi. Consente inoltre all'applicazione di federare l'accesso ad altri servizi pubblici popolari come OpenID, Facebook, Amazon o Google.

Amazon Cognito è diviso in due prodotti principali. Pool di utenti Amazon Cognito e Amazon Cognito Identity Provider. Questa sezione si concentra sui pool di utenti di Amazon Cognito, che forniscono l'accesso ad altri AWS servizi come Amazon S3 o DynamoDB. Il servizio consente di utilizzare i pool di utenti di Amazon Cognito o un provider di identità di terze parti per fornire l'accesso ai AWS servizi. Fornisce inoltre l'accesso ai AWS servizi utilizzando l'accesso anonimo degli ospiti. A causa della potente natura dei pool di utenti di Amazon Cognito, questi verrebbero gestiti manualmente sulla case-by-case base di un servizio manuale operativo, al fine di evitare potenziali violazioni della sicurezza dell'account. Per ulteriori informazioni, consulta Amazon Cognito User Pools.

Domande frequenti sui pool di utenti di Amazon Cognito in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso ai pool di utenti di Amazon Cognito nel mio account AMS?

L'implementazione dei pool di utenti di Amazon Cognito in AMS è un processo in due fasi:

1. Invia una gestione | Altro | Altro | Crea (ct-1e1xtak34nx76) modifica il tipo e richiedi la creazione dei pool di utenti Amazon Cognito nel tuo account AMS. Includi le seguenti informazioni:
   - AWS Regione.
   - Nome per il pool di utenti di Cognito.
   - Se desideri utilizzare Amazon Simple Email Service (Amazon SES) per inviare messaggi e notifiche anziché il servizio di posta interno predefinito di Cognito, il cliente deve fornire un indirizzo e-mail già convalidato per il servizio Amazon SES nell'account. Questo indirizzo verrà utilizzato per i campi «Da» e «REPLY-TO» del messaggio. Devono inoltre indicare la regione in cui è stato attivato Amazon SES (us-east-1, eu-west-1 o us-west-2).
   - Se desideri utilizzare i messaggi SMS per password monouso e per la verifica, il cliente deve indicarlo.
2. Richiedi l'accesso dell'utente inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli IAM al tuo account: e. `customer_cognito_admin_role` `customer_cognito_importjob_role` Dopo aver effettuato il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione di

federazione. Questi ruoli consentono di gestire i pool di utenti di Amazon Cognito, gestire utenti e gruppi nel pool, creare importjob per gli utenti, modificare i messaggi di notifica e sottoscrizione, associare applicazioni al pool di utenti, gestire automaticamente l'aggiunta di servizi federativi al pool ed eliminare i pool già creati.

D: Quali sono le restrizioni all'utilizzo dei pool di utenti di Amazon Cognito nel mio account AMS?

Non sarai in grado di creare i pool di utenti di Amazon Cognito. Tale azione richiede la creazione di ruoli IAM per sfruttare i servizi utilizzati da Amazon Cognito, come Amazon SES e Amazon Simple Notification Service (Amazon SNS).

D: Quali sono i prerequisiti o le dipendenze per utilizzare i pool di utenti di Amazon Cognito nel mio account AMS?

Se desideri utilizzare Amazon SES per inviare messaggi e notifiche via e-mail ai tuoi pool di utenti, questi devono già attivare il servizio Amazon SES nell'account e convalidare già l'indirizzo e-mail da utilizzare nei campi «FROM» e «REPLY-TO» delle e-mail inviate. Per ulteriori informazioni sulla convalida dell'indirizzo e-mail con Amazon SES, consulta Verifica degli indirizzi e-mail in Amazon SES.

Usa AMS SSP per effettuare il provisioning di Amazon Comprehend nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Comprehend direttamente nel tuo account gestito AMS. Amazon Comprehend è un servizio di elaborazione del linguaggio naturale (NLP) che utilizza l'apprendimento automatico per trovare approfondimenti e relazioni nel testo, non è richiesta alcuna esperienza di apprendimento automatico. Amazon Comprehend utilizza l'apprendimento automatico per aiutarti a scoprire le informazioni e le relazioni nei tuoi dati non strutturati. Il servizio identifica la lingua del testo; estrae frasi chiave, luoghi, persone, marchi o eventi; comprende quanto sia positivo o negativo il testo; analizza il testo utilizzando la tokenizzazione e parti del discorso e organizza automaticamente una raccolta di file di testo per argomento. Puoi anche utilizzare le funzionalità di AutoML in Amazon Comprehend per creare un set personalizzato di entità o modelli di classificazione del testo personalizzati in base alle esigenze della tua organizzazione. Per ulteriori informazioni, consulta Amazon Comprehend.

Domande frequenti su Amazon Comprehend in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon Comprehend nel mio account AMS?

La console Amazon Comprehend e i ruoli di accesso ai dati possono essere richiesti inviando due servizi AMS: RFCs

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (managed automation) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_comprehend_console_role` seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon Comprehend nel mio account AMS?

La funzionalità Create New IAM Role tramite la console Amazon Comprehend è limitata. Altrimenti, la funzionalità completa di Amazon Comprehend è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Comprehend nel mio account AMS?

Amazon S3 e AWS Key Management Service (AWS KMS) sono necessari per utilizzare Amazon Comprehend, se i bucket Amazon S3 sono crittografati con chiavi. AWS KMS

Usa AMS SSP per effettuare il provisioning di Amazon Connect nel tuo account AMS

> **Note**
>
> Dopo un’attenta valutazione, abbiamo deciso di interrompere il supporto per Amazon Connect Voice ID a partire dal 20 maggio 2026. Amazon Connect Voice ID non accetterà più nuovi clienti a partire dal 20 maggio 2025. In qualità di cliente esistente con un account registrato al servizio prima del 20 maggio 2025, puoi continuare a utilizzare le funzionalità di Amazon Connect Voice ID. Dopo il 20 maggio 2026, non potrai più utilizzare Amazon Connect Voice ID.

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Connect direttamente nel tuo account gestito AMS. Amazon Connect è un contact center cloud omnicanale che aiuta le aziende a fornire un servizio clienti di qualità superiore a un costo inferiore. Amazon Connect offre un'esperienza fluida tramite voce e chat per clienti e agenti. Ciò include un set di strumenti per il routing basato sulle competenze, potenti analisi cronologiche e in tempo reale e strumenti di gestione easy-to-use intuitivi, il tutto con prezzi. pay-as-you-go

Puoi creare una o più istanze delle istanze del contact center virtuale negli account AMS multi-account landing zone o negli account di landing zone con account singolo. Puoi utilizzare i provider di identità SAML 2.0 esistenti per l'accesso agli agenti o utilizzare il supporto nativo di Amazon Connect per la gestione del ciclo di vita degli utenti.

Inoltre, puoi richiedere i numeri di free/direct telefono a pagamento per ogni istanza Amazon Connect dalla console Amazon Connect. Puoi creare ricchi flussi di contatti per ottenere l'esperienza e il routing del cliente desiderati utilizzando un' easy-to-useinterfaccia utente grafica. I flussi di contatti possono sfruttare AWS Lambda le funzioni per l'integrazione con gli archivi di dati e le API locali. Puoi anche abilitare lo streaming di dati utilizzando Kinesis Streams e Firehose.

Le registrazioni delle chiamate, le trascrizioni delle chat e i report vengono archiviati in un bucket Amazon S3 crittografato utilizzando una chiave. AWS KMS I log del flusso di contatti possono essere salvati in gruppi di log. CloudWatch

Per ulteriori informazioni, consulta Amazon Connect.

Domande frequenti su Amazon Connect in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon Connect nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce i seguenti `customer_connect_console_role` ruoli IAM al tuo account: e. `customer_connect_user_role` Dopo aver effettuato il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione di federazione.

D: Quali sono le restrizioni all'uso di Amazon Connect nel mio account AMS?

Non ci sono restrizioni. La funzionalità completa di Amazon Connect è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Connect nel mio account AMS?

- È necessario creare una AWS KMS chiave e un bucket Amazon S3 utilizzando AMS standard RFCs; il bucket Amazon S3 è necessario per archiviare le registrazioni delle chiamate e le trascrizioni delle chat.
- Se desideri effettuare l'integrazione con Active Directory (AD), è necessario un AD Connector per l'integrazione tra le istanze Amazon Connect ospitate da AMS e i servizi di directory locali. AD Connector può essere configurato nel tuo account richiedendo una RFC «Gestione | Altro | Altro».

- È possibile abilitare i seguenti servizi opzionali forniti autonomamente in base ai requisiti del flusso di contatti.
  - AWS Lambda: È possibile utilizzare le funzioni Lambda per estendere i flussi di contatti per sfruttare gli archivi dati locali esistenti oppure. APIs Puoi utilizzare il servizio Lambda self-provisioned per creare le funzioni Lambda.
  - Amazon Kinesis Data Streams: puoi creare flussi di dati per abilitare lo streaming di dati verso applicazioni esterne. Puoi trasmettere in streaming i record di tracciamento dei contatti o gli eventi degli agenti.
  - Amazon Kinesis Data Firehose: puoi creare Data Firehose per trasmettere record di tracce di contatti ad alto volume verso applicazioni esterne.
  - Amazon Lex: puoi sfruttare i chatbot di Amazon Lex per creare flussi di contatti intelligenti sfruttando i servizi Amazon Alexa per un'esperienza cliente e un'automazione avanzate.
- D: Come posso richiedere di aggiungere un elenco di paesi per le chiamate in uscita o in entrata?

  Per aggiungere un elenco di paesi per le chiamate in uscita o in entrata, invia una richiesta di servizio ad AMS.

Usa AMS SSP per effettuare il provisioning di Amazon Data Firehose nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Data Firehose direttamente dal tuo account gestito AMS. Firehose è il modo più semplice per caricare in modo affidabile lo streaming di dati in data lake, data store e strumenti di analisi. Può acquisire, trasformare e caricare dati di streaming in Amazon S3, Amazon Redshift, OpenSearch Amazon Service e Splunk, abilitando analisi quasi in tempo reale con gli strumenti e le dashboard di business intelligence esistenti che già utilizzi oggi. È un servizio completamente gestito che si ridimensiona automaticamente in base alla velocità di trasmissione dei dati e non richiede alcuna amministrazione continua. Può anche raggruppare, comprimere, trasformare e crittografare i dati prima di caricarli, riducendo al minimo la quantità di storage utilizzata nella destinazione e aumentando la sicurezza. Per ulteriori informazioni, consulta What Is Amazon Data Firehose?

Domande frequenti su Firehose in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso ad Amazon Data Firehose nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_kinesis_firehose_user_role` seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo di Firehose nel mio account AMS?

Non ci sono restrizioni. La funzionalità completa di Amazon Data Firehose è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Firehose nel mio account AMS?

È necessario richiedere nuovi ruoli IAM collegati ai servizi per ogni flusso di distribuzione. Puoi anche riutilizzare un singolo ruolo collegato al servizio per tutti i flussi aggiornando la politica del ruolo con le autorizzazioni delle risorse richieste (inclusi bucket S3/KMS Keys/Lambda Functions /Kinesis stream).

Dopo aver inviato la RFC per aggiungere Firehose, un tecnico AMS Operations ti contatterà tramite una richiesta di assistenza per ARNs le risorse che desideri collegare a Data Firehose (ad esempio AWS KMS, S3, Lambda e Kinesis Streams).

Usa AMS SSP per effettuare il provisioning di Amazon DevOps Guru nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon DevOps Guru direttamente dal tuo account gestito AMS. Amazon DevOps Guru è un servizio operativo completamente gestito che consente a sviluppatori e operatori di migliorare facilmente le prestazioni e la disponibilità delle loro applicazioni. DevOpsGuru ti consente di alleggerire le attività amministrative associate all'identificazione dei problemi operativi in modo da poter implementare rapidamente i consigli per migliorare la tua applicazione. DevOpsGuru crea informazioni reattive che puoi utilizzare subito per migliorare la tua applicazione. Crea inoltre informazioni proattive per aiutarti a evitare problemi operativi che potrebbero influire sulla tua applicazione in futuro. DevOpsGuru applica l'apprendimento automatico per analizzare i dati operativi e le metriche e gli eventi delle applicazioni per identificare comportamenti che si discostano dai normali schemi operativi. Riceverai una notifica quando DevOps Guru rileva un problema o un rischio operativo. Per ogni numero, DevOps Guru presenta raccomandazioni intelligenti per affrontare i problemi operativi attuali e previsti per il futuro.

Per ulteriori informazioni, consulta Cos'è Amazon DevOps Guru.

Domande frequenti su Amazon DevOps Guru in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon DevOps Guru nel mio account AMS?

Per richiedere l'accesso, invia un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce `customer_devopsguru_role` il seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon DevOps Guru nel mio account AMS?

Non ci sono restrizioni. La funzionalità completa di Amazon DevOps Guru è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon DevOps Guru nel mio account AMS?

Non ci sono prerequisiti. DevOpsGuru sfrutta i seguenti AWS servizi: Amazon CloudWatch Logs, RDS Insights,, AWS X-Ray e. AWS Lambda AWS CloudTrail

Usa AMS SSP per effettuare il provisioning di Amazon DocumentDB (con compatibilità MongoDB) nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon DocumentDB (con compatibilità MongoDB) direttamente nel tuo account gestito AMS. Amazon DocumentDB (con compatibilità con MongoDB) è un servizio di database di documenti veloce, scalabile, altamente disponibile e completamente gestito che supporta i carichi di lavoro MongoDB. Amazon DocumentDB ti offre le prestazioni, la scalabilità e la disponibilità di cui hai bisogno per gestire carichi di lavoro MongoDB mission-critical su larga scala. Amazon DocumentDB implementa l'API open source MongoDB 3.6 di Apache 2.0 emulando le risposte che un client MongoDB si aspetta da un server MongoDB, consentendoti di utilizzare i driver e gli strumenti MongoDB esistenti con Amazon DocumentDB. In Amazon DocumentDB, lo storage e l'elaborazione sono disaccoppiati, consentendo a ciascuno di scalare in modo indipendente. Inoltre, puoi aumentare la capacità di lettura fino a milioni di richieste al secondo aggiungendo fino a 15 repliche di lettura a bassa latenza, indipendentemente dalla dimensione dei dati. Amazon DocumentDB è progettato per una disponibilità del 99,99% e replica sei copie dei dati in tre zone di AWS disponibilità (). AZs Puoi utilizzare AWS Database Migration Service (DMS) gratuitamente (per sei mesi) per migrare i tuoi database locali o Amazon Elastic Compute Cloud (Amazon EC2) MongoDB su Amazon DocumentDB praticamente

senza tempi di inattività. Per ulteriori informazioni, consulta Amazon DocumentDB (con compatibilità con MongoDB).

Domande frequenti su Amazon DocumentDB in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon DocumentDB nel mio account AMS?

La console di Amazon DocumentDB e i ruoli di accesso ai dati possono essere richiesti inviando due moduli AMS RFCs, accesso alla console e accesso ai dati:

Richiedi l'accesso ad Amazon DocumentDB inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC fornisce il `customer_documentdb_role` seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon DocumentDB nel mio account AMS?

Amazon DocumentDB richiede autorizzazioni specifiche di Amazon RDS. Poiché AMS gestisce completamente Amazon RDS, il ruolo IAM per Amazon DocumentDB include alcune restrizioni alle azioni su Amazon RDS. Le restrizioni si applicano come segue:

- L'accesso a `DeleteDBInstance` e `DeleteDBCluster` APIs sono stati limitati. Per utilizzare tali eliminazioni APIs, invia una RFC con il tipo di modifica Management | Advanced stack components | Identity and Access Management (IAM) and Access Management | Update entity o policy (managed automation) (ct-27tuth19k52b4).
- Non puoi aggiungere o rimuovere tag dalle istanze Amazon RDS.
- Non puoi rendere pubblica la tua istanza Amazon DocumentDB.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon DocumentDB nel mio account AMS?

Amazon S3 e AWS KMS sono necessari per utilizzare Amazon DocumentDB, se i bucket Amazon S3 sono crittografati con chiavi. AWS KMS

Usa AMS SSP per effettuare il provisioning di Amazon DynamoDB nel tuo account AMS

Usa la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon DynamoDB (DynamoDB) direttamente nel tuo account gestito AMS. Amazon DynamoDB è un

database di valori e documenti chiave che offre prestazioni a una cifra in millisecondi su qualsiasi scala. È un database multiregionale e multiattivo completamente gestito con sicurezza, backup e ripristino integrati e caching in memoria per applicazioni su scala Internet. Per ulteriori informazioni, consulta Amazon DynamoDB.

Amazon DynamoDB Accelerator (DAX) è un servizio di memorizzazione nella cache write-through progettato per semplificare il processo di aggiunta di una cache alle tabelle DynamoDB. DAX è destinato all'uso in applicazioni che richiedono letture ad alte prestazioni.

Domande frequenti su DynamoDB in AWS Managed Services

D: Come posso richiedere l'accesso a DynamoDB e DAX nel mio account AMS?

Richiedi l'accesso a DynamoDB e DAX inviando una RFC con il tipo di modifica Management AWS | service | Self-provisioned service | Add (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli e policy IAM al tuo account:

- Nome del ruolo DynamoDB: `customer_dynamodb_role`

  Nome del ruolo del servizio DAX: `customer_dax_service_role`
- Nome della policy DynamoDB: `customer_dynamodb_policy`

  Politica del servizio DAX: `customer_dax_service_policy`

Una volta effettuato il provisioning nel proprio account, è necessario effettuare l'integrazione della soluzione `customer_dynamodb_role` nella federazione.

D: Quali sono le restrizioni all'utilizzo di DynamoDB nel mio account AMS?

Sono supportate tutte le funzionalità di DynamoDB, incluso DynamoDB Accelerator (DAX).

Quando si creano allarmi per una determinata tabella, il nome dell'avviso deve avere il prefisso «customer*»; ad esempio,. `customer-employee-table-high-put-latency`

Quando si crea un argomento Amazon SNS per DynamoDB, deve essere denominato:. `dynamodb`

Per eliminare l'argomento Amazon SNS creato da DynamoDB, invia un RFC di tipo Management | Other | Other | Update change.

D: Quali sono i prerequisiti o le dipendenze per utilizzare DynamoDB nel mio account AMS?

Non ci sono prerequisiti o dipendenze per utilizzare DynamoDB nel tuo account AMS.

Usa AMS SSP per effettuare il provisioning di Amazon Elastic Container Registry nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Elastic Container Registry (Amazon ECR) direttamente nel tuo account gestito AMS. Amazon Elastic Container Registry è un registro di container Docker completamente gestito che semplifica per gli sviluppatori l'archiviazione, la gestione e la distribuzione di immagini di container Docker. Amazon ECR è integrato con Amazon Elastic Container Service (Amazon ECS), semplificando il flusso di lavoro dallo sviluppo alla produzione. Amazon ECR elimina la necessità di gestire i propri repository di container o di preoccuparsi della scalabilità dell'infrastruttura sottostante. Amazon ECS ospita le tue immagini in un'architettura altamente disponibile e scalabile, che ti consente di distribuire in modo affidabile contenitori per le tue applicazioni. L'integrazione con AWS Identity and Access Management (IAM) fornisce il controllo a livello di risorsa di ogni repository. Con Amazon ECR, non ci sono commissioni o impegni iniziali. Paghi solo per la quantità di dati archiviati nei tuoi repository e di dati trasferiti su Internet.

Per ulteriori informazioni, consulta Amazon Elastic Container Registry.

Domande frequenti su Amazon Elastic Container Registry in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon ECR nel mio account AMS?

Richiedi l'accesso ad Amazon ECR inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli IAM al tuo account:, e con le politiche IAM associate e, rispettivamente. `customer_ecr_console_role` `customer_ecr_poweruser_instance_profile` `customer_ecr_console_policy` `customer_ecr_poweruser_instance_profile_policy` Una volta effettuato il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione di federazione.

D: Quali sono le restrizioni all'uso di Amazon ECR nel mio account AMS?

Esistono restrizioni sugli spazi dei nomi AMS per l'uso di Amazon ECR nel tuo account AMS. Le immagini dei contenitori non possono avere il prefisso «AMS-» o «Sentinel-».

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon ECR nel mio account AMS?

Non ci sono prerequisiti o dipendenze per utilizzare Amazon ECR nel tuo account AMS.

Usa AMS SSP per effettuare il provisioning di EC2 Image Builder nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di EC2 Image Builder direttamente nel tuo account gestito AMS. EC2 Image Builder è un servizio AWS completamente gestito che semplifica l'automazione della creazione, gestione e distribuzione di immagini server personalizzate up-to-date, sicure e «dorate» preinstallate e preconfigurate con software e impostazioni per soddisfare specifici standard IT.

Puoi utilizzare Console di gestione AWS la AWS CLI o APIs creare immagini personalizzate nel tuo AWS account. Quando utilizzi Console di gestione AWS, la procedura guidata di Amazon EC2 Image Builder ti guida attraverso i passaggi per:

- Fornisci artefatti iniziali
- Aggiungere e rimuovere software
- Personalizza impostazioni e script
- Esegui test selezionati
- Distribuisci le immagini AWS nelle regioni

Le immagini create vengono create nel tuo account e possono essere configurate per le patch del sistema operativo su base continuativa. Per saperne di più, consulta EC2 Image Builder.

Domande frequenti su EC2 Image Builder in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso a EC2 Image Builder nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (automazione gestita) (ct-3qe6io8t6jtny). Tramite questa RFC, nel tuo account verrà assegnato il seguente ruolo IAM:. `customer_ec2_imagebuilder_role` Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni per EC2 Image Builder?

AMS non supporta l'uso di Service Defaults per la configurazione dell'infrastruttura. È possibile creare una nuova configurazione dell'infrastruttura o utilizzarne una esistente.

Attualmente AMS non supporta la creazione di ricette di contenitori.

D: Quali sono i prerequisiti o le dipendenze per abilitare EC2 Image Builder?

- Ruolo collegato ai servizi di EC2 Image Builder: non è necessario creare manualmente un ruolo collegato al servizio. Quando crei la tua prima risorsa Image Builder nella AWS CLI o nell'API, AWS Image Builder crea automaticamente il ruolo collegato al servizio. Console di gestione AWS
- Le istanze utilizzate per creare immagini ed eseguire test utilizzando Image Builder devono avere accesso al servizio Systems Manager. L'agente SSM verrà installato sull'immagine sorgente se non è già presente e verrà rimosso prima della creazione dell'immagine.
- AWS IAM: il ruolo IAM che associ al tuo profilo di istanza deve disporre delle autorizzazioni per eseguire i componenti di compilazione e test inclusi nell'immagine. Le seguenti policy di ruolo IAM devono essere associate al ruolo IAM associato ai profili di istanza: `EC2InstanceProfileForImageBuilder` e`AmazonSSMManagedInstanceCore`. Il nome del ruolo IAM deve contenere la `*imagebuilder*` parola chiave.
- Se configuri la registrazione, il profilo di istanza specificato nella configurazione dell'infrastruttura deve disporre delle `s3:PutObject` autorizzazioni per il bucket di destinazione (). `arn:aws:s3:::{bucket-name}/*` Esempio:

  JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "s3:PutObject"
            ],
            "Resource": "arn:aws:s3:::{bucket-name}/*"
        }
    ]
}
```

- Crea un argomento SNS con nome 'imagebuilder' per ricevere avvisi e notifiche da EC2 Image Builder.

Usa AMS SSP per effettuare il provisioning di Amazon ECS AWS Fargate nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere ad Amazon ECS on AWS Fargate Capabilities direttamente nel tuo account gestito AMS. AWS Fargate è una tecnologia che puoi usare con Amazon ECS per eseguire container (vedi Containers on AWS) senza dover gestire server o cluster di istanze Amazon EC2. Con AWS Fargate, non è più necessario effettuare il provisioning, configurare o ridimensionare i cluster di macchine virtuali per eseguire i contenitori. Viene anche eliminata la necessità di scegliere i tipi di server, di decidere quando dimensionare i cluster o ottimizzarne il packing.

Per ulteriori informazioni, consulta Amazon ECS on AWS Fargate.

Domande frequenti su Amazon ECS su Fargate in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon ECS on Fargate nel mio account AMS?

Richiedi l'accesso ad Amazon ECS su Fargate inviando una RFC con il tipo di modifica Management AWS | service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli IAM al tuo account: `customer_ecs_fargate_console_role` (se non viene fornito alcun ruolo IAM esistente a cui associare la policy ECS),,, e. `customer_ecs_fargate_events_service_role` `customer_ecs_task_execution_service_role` `customer_ecs_codedeploy_service_role` `AWSServiceRoleForApplicationAutoScaling_ECSService` Una volta effettuato il provisioning nel tuo account, devi inserire i ruoli nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon ECS su Fargate nel mio account AMS?

- Il monitoraggio e la registrazione delle attività di Amazon ECS sono considerati una tua responsabilità poiché le attività a livello di container si verificano al di sopra dell'hypervisor e le funzionalità di registrazione sono limitate da Amazon ECS su Fargate. In qualità di utente di Amazon ECS su Fargate, ti consigliamo di adottare le misure necessarie per abilitare la registrazione delle tue attività Amazon ECS. Per ulteriori informazioni, consulta Abilitazione del driver di registro awslogs per i tuoi contenitori.
- Anche la sicurezza e la protezione da malware a livello di container sono considerate di tua responsabilità. Amazon ECS on Fargate non include Trend Micro o componenti di sicurezza di rete preconfigurati.

- Questo servizio è disponibile sia per gli account di landing zone multi-account che per gli account AMS di landing zone con account singolo.
- Amazon ECS Service Discovery è limitato per impostazione predefinita nel ruolo di self-provisioning poiché sono necessarie autorizzazioni elevate per creare zone ospitate private Route 53. Per abilitare Service Discovery su un servizio, invia un tipo di modifica Management | Other | Other | Update. Per fornire le informazioni necessarie per abilitare Service Discovery per il tuo servizio Amazon ECS, consulta il manuale Service Discovery.
- Attualmente AMS non gestisce o limita le immagini utilizzate per la distribuzione in container su Amazon ECS Fargate. Potrai distribuire immagini da Amazon ECR, Docker Hub o qualsiasi altro archivio di immagini privato. Pertanto, abbiamo consigliato di non distribuire immagini pubbliche o non protette, poiché potrebbero provocare attività dannose sull'account.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon ECS on Fargate nel mio account AMS?

- Di seguito sono riportate le dipendenze di Amazon ECS su Fargate; tuttavia, non è richiesta alcuna azione aggiuntiva per abilitare questi servizi con il ruolo assegnato autonomamente:
  - CloudWatch registri
  - CloudWatch eventi
  - CloudWatch allarmi
  - CodeDeploy
  - App Mesh
  - Cloud Map
  - Route 53
- A seconda del caso d'uso, le seguenti sono le risorse su cui si basa Amazon ECS e che potrebbero richiedere prima di utilizzare Amazon ECS on Fargate nel tuo account:
  - Gruppo di sicurezza da utilizzare con il servizio Amazon ECS. È possibile utilizzare Deployment | Advanced stack components | Security Group | Create (auto) (ct-3pc215bnwb6p7) oppure, se il gruppo di sicurezza richiede regole speciali, utilizzare Deployment | Advanced stack components | Security Group | Create (automazione gestita) (ct-1oxx2g2d7hc90). Nota: il gruppo di sicurezza selezionato con Amazon ECS deve essere creato specificamente per Amazon ECS in cui risiede il servizio o il cluster Amazon ECS. Puoi saperne di più nella sezione Security Group in Configurazione con Amazon ECS e sicurezza in Amazon Elastic Container Service.

  - Application load balancer (ALB), network load balancer (NLB), classic load balancer (ELB) per il bilanciamento del carico tra le attività.
  - Gruppi target per. ALBs
  - Risorse mesh per app (ad esempio, router virtuali, servizi virtuali, nodi virtuali) da integrare con il tuo cluster Amazon ECS.
- Attualmente, AMS non è in grado di mitigare automaticamente i rischi associati al supporto delle autorizzazioni dei gruppi di sicurezza se create al di fuori dei tipi di modifica AMS standard. Ti consigliamo di richiedere un gruppo di sicurezza specifico da utilizzare con il tuo cluster Fargate per limitare la possibilità di utilizzare un gruppo di sicurezza non designato per l'uso con Amazon ECS.

Usa AMS SSP per effettuare il provisioning di Amazon EKS AWS Fargate nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere ad Amazon EKS sulle AWS Fargate funzionalità direttamente nel tuo account gestito AMS. AWS Fargate è una tecnologia che fornisce capacità di calcolo on-demand e della giusta dimensione per i container (per informazioni sui contenitori, consulta Cosa sono i contenitori?). Con AWS Fargate, non è più necessario effettuare il provisioning, configurare o ridimensionare gruppi di macchine virtuali per eseguire i contenitori. Viene anche eliminata la necessità di scegliere i tipi di server, di decidere quando dimensionare i gruppi di nodi o ottimizzare il packing dei cluster.

Amazon Elastic Kubernetes Service (Amazon EKS) integra AWS Fargate Kubernetes utilizzando controller AWS creati utilizzando il modello upstream ed estensibile fornito da Kubernetes. Questi controller funzionano come parte del piano di controllo Kubernetes gestito da Amazon EKS e sono responsabili della pianificazione dei pod Kubernetes nativi su Fargate. I controller Fargate includono un nuovo pianificazione che viene eseguito insieme al pianificatore di default di Kubernetes, oltre a diversi controller di ammissione mutanti e convalidanti. Quando si avvia un pod che soddisfa i criteri per l'esecuzione su Fargate, i controller Fargate in esecuzione nel cluster riconoscono, aggiornano e programmano il pod su Fargate.

Per ulteriori informazioni, consulta Amazon EKS on AWS Fargate Now Generally Available e Amazon EKS Best Practices Guide for Security (include «Consigli» come «Rivedi e revoca accessi anonimi non necessari» e altro).

> **Tip**
>
> AMS ha un tipo di modifica, Deployment | Advanced stack components | Identity and Access Managment (IAM) | Create un provider OpenID Connect (ct-30ecvfi3tq4k3), che puoi utilizzare con Amazon EKS. Per un esempio, consulta Identity and Access Management (IAM) | Create OpenID Connect Provider.

Domande frequenti su Amazon EKS AWS Fargate attivo in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon EKS su Fargate nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il seguente ruolo IAM al tuo account.

- `customer_eks_fargate_console_role`.

  Dopo averlo inserito nel tuo account, devi inserire il ruolo nella tua soluzione federativa.
- Questi ruoli di servizio consentono ad Amazon EKS on Fargate di chiamare altri AWS servizi per tuo conto:
  - `customer_eks_pod_execution_role`
  - `customer_eks_cluster_service_role`

D: Quali sono le restrizioni all'uso di Amazon EKS su Fargate nel mio account AMS?

- La creazione di gruppi di nodi EC2 gestiti o autogestiti non è supportata in AMS. Se hai l'esigenza di utilizzare i nodi di lavoro EC2, contatta il tuo AMS Cloud Service Delivery Manager (CSDM) o Cloud Architect (CA).
- AMS non include Trend Micro o componenti di sicurezza di rete preconfigurati per le immagini dei container. È necessario gestire i propri servizi di scansione delle immagini per rilevare immagini dannose dei container prima della distribuzione.
- EKSCTL non è supportato a causa di interdipendenze. CloudFormation
- Durante la creazione del cluster, si dispone delle autorizzazioni per disabilitare la registrazione del piano di controllo del cluster. Per ulteriori informazioni, consulta Amazon EKS control plane logging (Registrazione del piano di controllo di Amazon EKS). Ti consigliamo di abilitare tutte le

principali funzionalità di registrazione delle API, dell'autenticazione e dell'audit durante la creazione del cluster.

- Durante la creazione del cluster, l'accesso agli endpoint del cluster per i cluster Amazon EKS è di default pubblico; per ulteriori informazioni, consulta Amazon EKS Cluster Endpoint Access Control. Consigliamo di impostare gli endpoint Amazon EKS come privati. Se gli endpoint sono necessari per l'accesso pubblico, è consigliabile impostarli come pubblici solo per intervalli CIDR specifici.
- AMS non dispone di un metodo per forzare e limitare le immagini utilizzate per la distribuzione nei container su Amazon EKS Fargate. Puoi distribuire immagini da Amazon ECR, Docker Hub o qualsiasi altro archivio di immagini privato. Pertanto, esiste il rischio di distribuire un'immagine pubblica che potrebbe eseguire attività dannose sull'account.
- La distribuzione di cluster EKS tramite il cloud development kit (CDK) o CloudFormation Ingest non è supportata in AMS.
- È necessario creare il gruppo di sicurezza richiesto utilizzando ct-3pc215bnwb6p7 Deployment | Advanced stack components | Security group | Crea e fai riferimento nel file manifest per la creazione degli ingress. Questo perché il ruolo non è autorizzato a creare gruppi di sicurezza. `customer-eks-alb-ingress-controller-role`

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon EKS su Fargate nel mio account AMS?

Per utilizzare il servizio, è necessario configurare le seguenti dipendenze:

- Per l'autenticazione con il servizio, è aws-iam-authenticator necessario installare sia KUBECTL che KUBECTL; per ulteriori informazioni, vedere Gestione dell'autenticazione del cluster.
- Kubernetes si basa su un concetto chiamato «account di servizio». Per utilizzare la funzionalità degli account di servizio all'interno di un cluster Kubernetes su EKS, è necessario un RFC Management | Other | Other | Update con i seguenti input:
  - [Richiesto] Nome del cluster Amazon EKS
  - [Obbligatorio] Spazio dei nomi del cluster Amazon EKS in cui verrà distribuito l'account di servizio (SA).
  - [Obbligatorio] Nome Amazon EKS Cluster SA.
  - [Obbligatorio] Nome e nome della policy IAM permissions/document da associare.
  - [Obbligatorio] Nome del ruolo IAM richiesto.
  - [Opzionale] URL del provider OpenID Connect. Per ulteriori informazioni, consultare la pagina
    - Abilitazione dei ruoli IAM per gli account di servizio sul cluster

    - Presentazione dei ruoli IAM dettagliati per gli account di servizio
- Si consiglia di configurare e monitorare le regole di Config
    - Endpoint del cluster pubblico
    - Registrazione API disabilitata

    È tua responsabilità monitorare e correggere queste regole di Config.

Se desideri implementare un controller ALB Ingress, invia un RFC Management | Other | Other Update per fornire il ruolo IAM necessario da utilizzare con il pod ALB Ingress Controller. I seguenti input sono necessari per creare risorse IAM da associare a ALB Ingress Controller (includili nella tua RFC):

- [Richiesto] Nome del cluster Amazon EKS
- [Opzionale] URL del provider OpenID Connect
- [Opzionale] Spazio dei nomi Amazon EKS Cluster in cui verrà distribuito il servizio di controller di ingresso ALB (Application Load Balancer). [impostazione predefinita: kube-system]
- [Facoltativo] Nome dell'account del servizio Amazon EKS Cluster (SA). [impostazione predefinita: aws-load-balancer-controller]

Se desideri abilitare la crittografia degli envelope secret nel tuo cluster (opzione consigliata), fornisci la chiave IDs KMS che intendi utilizzare nel campo della descrizione della RFC per aggiungere il servizio (Management | service | Self-provisioned AWS service | Add (ct-1w8z66n899dct). Per ulteriori informazioni sulla crittografia delle buste, consulta Amazon EKS aggiunge la crittografia delle buste per i segreti con AWS KMS.

Usa AMS SSP per effettuare il provisioning di Amazon EMR nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon EMR direttamente dal tuo account gestito AMS. Amazon EMR è la piattaforma cloud di big data leader del settore per l'elaborazione di grandi quantità di dati utilizzando strumenti open source come Apache Spark, Apache Hive, Apache, Apache Flink, Apache Hudi e HBase Presto. Con Amazon EMR puoi eseguire analisi su scala petabyte a meno della metà del costo delle soluzioni locali tradizionali e oltre 3 volte più velocemente rispetto allo standard Apache Spark. Per i lavori di breve durata, puoi attivare e disattivare i cluster e pagare al secondo per le istanze utilizzate.

Per carichi di lavoro di lunga durata, puoi creare cluster ad alta disponibilità che si ridimensionano automaticamente per soddisfare la domanda.

Puoi creare una o più istanze dei cluster Amazon EMR in account AMS con più account di landing zone o con account singolo per supportare cluster Amazon EMR transitori e persistenti. Puoi anche abilitare l'autenticazione Kerberos per consentire l'autenticazione degli utenti dal dominio Active Directory locale.

Puoi sfruttare più archivi di dati con i cluster Amazon EMR per supportare strumenti e librerie Hadoop specifici per i casi d'uso. I cluster Amazon EMR possono essere creati utilizzando OnDemand le nostre istanze Spot e configurare la scalabilità automatica per gestire la capacità e ridurre i costi.

I file di log del cluster possono essere archiviati in un bucket Amazon S3 per la registrazione e il debug. Puoi anche accedere alle interfacce Web ospitate nel cluster Amazon EMR per supportare i requisiti di amministrazione Hadoop o le esperienze di appunti per i clienti.

Per ulteriori informazioni, consulta Amazon EMR.

Domande frequenti su Amazon EMR in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon EMR nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce i seguenti ruoli IAM al tuo account:

- `customer_emr_cluster_instance_profile`
- `customer_emr_cluster_autoscaling_role`
- `customer_emr_console_role`
- `customer_emr_cluster_service_role`

Dopo averne effettuato il provisioning nel tuo account, devi integrare customer_emr_console_role nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon EMR nel mio account AMS?

Durante la creazione di Amazon EMR su un cluster EC2 dalla console AWS, ti consigliamo di utilizzare l'opzione Create Cluster — Advanced. I cluster Amazon EMR devono essere creati aggiungendo il tag con la chiave "for-use-with-amazon-emr-managed-policies" con valore «true». Seleziona le seguenti configurazioni nelle opzioni di sicurezza:

- Seleziona ruoli personalizzati per il tuo cluster:
  - Ruolo EMR: customer_emr_cluster_service_role
  - Profilo dell'istanza EC2: customer_emr_cluster_instance_profile
  - Ruolo Auto Scaling: customer_emr_cluster_autoscaling_role
- Gruppi di sicurezza EC2:
  - Master: ams-emr-master-security -group
  - Core & Task: ams-emr-worker-security -group
  - Accesso al servizio: ams-emr-serviceaccess-security -group

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon EMR nel mio account AMS?

AMS crea gruppi di sicurezza predefiniti per i nodi master, worker e services di Amazon EMR.

I modelli di avvio e i gruppi di sicurezza da utilizzare con i cluster Amazon EMR devono avere la chiave tag "for-use-with-amazon-emr-managed-policies" con valore «true».

Il profilo predefinito dell'istanza del cluster Amazon EMR consente l'accesso a risorse come bucket s3 e tabelle dynamodb i cui nomi contengono «emr». Puoi richiedere politiche IAM aggiuntive per utilizzare qualsiasi risorsa aggiuntiva da utilizzare con Amazon EMR. I seguenti ARN di risorse possono essere utilizzati con i job di Amazon EMR utilizzando customer_emr_cluster_instance_profile:

- arn:aws:dynamodb: *:*:table/*emr*
- arn:aws:kinesis: *:*:stream/*emr*
- arn:aws:sns: *:*: *emr*arn:aws:sqs: *:*: *emr*
- arn:aws:sqs: *:*: *emr*
- arn:aws:sqs: *:*:AWS- -* ElasticMapReduce
- arn:aws:sdb: *:*:dominio: *emr*
- arn:aws:s3: :*emr*

Se è richiesta l'autenticazione kerberos per il cluster Amazon EMR:

- Fornisci il nome dell'area di autenticazione da utilizzare per ogni cluster Amazon EMR kerberizzato e gli indirizzi IP di Active Directory locali.
- Requisiti dell'infrastruttura:

Multi-Account Landing Zone (MALZ): invia una RFC per creare un nuovo account di applicazione gestito o un nuovo VPC in un account di applicazione esistente.

Single-Account Landing Zone (SALZ): invia una RFC per creare una nuova sottorete nel tuo VPC.

- Configura il trust in entrata per il realm del cluster sull'Active Directory locale.
- Invia una RFC per configurare le zone DNS per il realm nel Managed AD.
- Configurazione del realm:

  MALZ: Invia una gestione | Altro | Altro | Aggiorna (ct-0xdawir96cy7k) RFC per aggiornare l'opzione DHCP VPC impostata per utilizzare il nome di realm per il suffisso del nome di dominio.

  SALZ: Invia una gestione | Altro | Altro | Aggiorna (ct-0xdawir96cy7k) RFC per generare una nuova AMI Amazon EMR da utilizzare il realm specifico per il suffisso del nome di dominio.

Per implementare Amazon EMR Studio, il `customer_emr_cluster_service_role` ruolo ha un prerequisito per un bucket Amazon Simple Storage Service. Per creare il bucket, utilizza il CT automatizzato `ct-1a68ck03fn98r` (Deployment | Advanced stack components | S3 storage | Create). Quando utilizzi questo CT automatico per creare un bucket Amazon S3 per Amazon EMR, il nome del bucket deve iniziare con il prefisso. `customer-emr-*` Inoltre, devi creare il bucket nella stessa AWS regione del cluster Amazon EMR.

Usa AMS SSP per effettuare il provisioning di Amazon EventBridge nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle EventBridge funzionalità di Amazon direttamente dal tuo account gestito AMS. Amazon EventBridge è un servizio di bus eventi senza server che semplifica la connessione delle applicazioni con dati provenienti da una varietà di fonti. EventBridge fornisce un flusso di dati in tempo reale dalle tue applicazioni, applicazioni Software-as-a-Service (SaaS) e AWS servizi e indirizza tali dati verso destinazioni come. AWS LambdaÈ possibile configurare regole di instradamento per determinare dove inviare i dati per creare architetture applicative che reagiscono in tempo reale a tutte le origini dati. EventBridge consente di creare architetture basate su eventi, che sono liberamente accoppiate e distribuite.

Per ulteriori informazioni, consulta Amazon EventBridge.

EventBridge nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso EventBridge al mio account AMS?

Richiedi l'accesso EventBridge inviando una RFC con il servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli IAM al tuo account: e. `customer_eventbridge_role` `customer_eventbridge_scheduler_execution_role` Dopo aver effettuato il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione di federazione.

Il ruolo di esecuzione `customer_eventbridge_scheduler_execution_role` è un ruolo IAM che EventBridge Scheduler si assume per interagire con altri Servizi AWS per tuo conto. Le politiche di autorizzazione allegate a questo ruolo concedono a EventBridge Scheduler l'accesso per richiamare gli obiettivi.

> **Note**
>
> Per impostazione predefinita, EventBridge Scheduler utilizza chiavi AWS proprietarie per EventBridge crittografare i dati. Per utilizzare una chiave gestita dal cliente per EventBridge crittografare i dati, invia la RFC utilizzando il servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (automazione gestita) (ct-3qe6io8t6jtny) per la fornitura del servizio.

D: EventBridge Quali sono le restrizioni all'utilizzo nel mio account AMS?

È necessario inviare AMS RFCs e creare le seguenti risorse: ruoli di servizio per attivare il processo batch CodeBuild CodePipeline, coda SQS e comandi SSM.

D: Quali sono i prerequisiti o le dipendenze da utilizzare EventBridge nel mio account AMS?

È necessario richiedere un ruolo di EventBridge servizio con una RFC utilizzando il tipo di modifica Deployment | Advanced stack components | Identity and Access Management (IAM) and Access Management | Create entity o policy (managed automation) (ct-3dpd8mdd9jn1r) prima di utilizzarlo per attivare altre EventBridge risorse, come AWS Lambda, Amazon SNS, Amazon SQS o Amazon Logs. AWS Batch CloudWatch Specificate i servizi da richiamare quando richiedete il vostro ruolo di servizio. Per ulteriori informazioni sulle autorizzazioni necessarie per richiamare gli obiettivi, consulta Using Resource-Based Policies for. EventBridge

EventBridge è integrato con AWS CloudTrail, un servizio che fornisce un registro delle azioni intraprese da un utente, un ruolo o un membro. Servizio AWS EventBridge CloudTrail deve essere abilitato e autorizzato a memorizzare i file di registro nei bucket S3. Nota: tutti gli account AMS sono CloudTrail abilitati, quindi non è necessaria alcuna azione.

D: Il ruolo customer_eventbridge_scheduler_execution_role ha un prerequisito per una chiave (opzionale, se utilizzato per la crittografia). AWS Key Management Service Come AWS KMS CMKs posso adottare la crittografia dei dati a riposo o in transito?

Per impostazione predefinita, EventBridge Scheduler crittografa i metadati degli eventi e i dati dei messaggi archiviati in una chiave AWS proprietaria (crittografia a riposo). EventBridge Scheduler crittografa anche i dati che passano tra EventBridge Scheduler e altri servizi utilizzando Transport Layer Security (TLS) (crittografia in transito).

Se il tuo caso d'uso specifico richiede il controllo e la verifica delle chiavi di crittografia che proteggono i dati su EventBridge Scheduler, puoi utilizzare una chiave gestita dal cliente.

Devi richiedere una RFC utilizzando il tipo di modifica Management | Servizio AWS | Self-provisioned service | Aggiungi (automazione gestita) prima di utilizzare Amazon EventBridge per l'onboarding dell'autorizzazione. AWS KMS

Usa AMS SSP per effettuare il provisioning di Amazon Forecast nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Forecast (Forecast) direttamente nel tuo account gestito AMS. Amazon Forecast è un servizio completamente gestito che utilizza l'apprendimento automatico per fornire previsioni estremamente accurate.

> **Note**
>
> AWS ha chiuso l'accesso dei nuovi clienti ad Amazon Forecast a partire dal 29 luglio 2024. I clienti esistenti di Amazon Forecast possono continuare a utilizzare il servizio normalmente. AWS continua a investire in sicurezza, disponibilità e miglioramenti delle prestazioni per Amazon Forecast, ma AWS non prevede di introdurre nuove funzionalità.
> Se desideri utilizzare Amazon Forecast, contatta il tuo CSDM per ricevere ulteriori informazioni su come trasferire l'utilizzo di Amazon Forecast ad Amazon Canvas. SageMaker

Basato sulla stessa tecnologia utilizzata su Amazon.com, Forecast utilizza l'apprendimento automatico per combinare dati di serie temporali con variabili aggiuntive per creare previsioni. Forecast non richiede alcuna esperienza di machine learning per iniziare. Devi solo fornire dati storici, più eventuali dati aggiuntivi che ritieni possano influire sulle tue previsioni. Ad esempio, la richiesta di un colore particolare di una camicia può cambiare in base alle stagioni e all'ubicazione del negozio. Questa relazione complessa è difficile da determinare da sola, ma l'apprendimento automatico è ideale per riconoscerla. Una volta forniti i dati, Forecast li esaminerà automaticamente, identificherà ciò che è significativo e produrrà un modello di previsione in grado di fare previsioni fino al 50% più accurate rispetto alla sola analisi dei dati delle serie temporali.

Per ulteriori informazioni, consulta Amazon Forecast.

Domande frequenti su Amazon Forecast in AWS Managed Services

D: Come posso richiedere l'accesso a Forecast nel mio account AMS?

Richiedi l'accesso AWS Firewall Manager inviando una RFC tramite Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC `customer_forecast_admin_role` fornisce il seguente ruolo IAM al tuo account:. Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo di Forecast nel mio account AMS?

L'accesso predefinito ai bucket S3 ti consente di accedere solo ai bucket con lo schema di denominazione 'customer-forecast-*'. Se hai una convenzione di denominazione personalizzata per i bucket di dati, discuti della denominazione dei bucket e della relativa configurazione di accesso con il tuo Cloud Architect (CA). Ad esempio:

- Puoi definire il tuo ruolo specifico del servizio Amazon Forecast con nomi come «AmazonForecast- ExecutionRole -*» e associare un accesso appropriato al bucket S3. Consulta il ruolo Service AmazonForecast-ExecutionRole-Admin e la policy IAM customer_forecast_default_s3_access_policy nella console IAM.
- Potrebbe essere necessario associare l'accesso ai bucket S3 correlati al ruolo di federazione IAM. Consulta la policy IAM - customer_forecast_default_s3_access_policy, nella console IAM.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Forecast nel mio account AMS?

- Prima di utilizzare Forecast, è necessario creare bucket Amazon S3 appropriati. In particolare, l'accesso predefinito ai bucket S3 avviene con lo schema di denominazione «customer-forecast-*»

- Se desideri utilizzare modelli di denominazione sui bucket S3 diversi da 'customer-forecast-*', devi creare un nuovo ruolo di servizio con autorizzazioni di accesso S3 sui bucket:
  1. Un nuovo ruolo di servizio da creare con il nome '- - {suffix}'. AmazonForecast ExecutionRole
  2. Sarà creata una nuova policy IAM simile a customer_forecast_default_s3_access_policy e da associare al nuovo ruolo di servizio e al relativo ruolo di amministratore della federazione (ad esempio 'customer_forecast_admin_role')

D: Come posso migliorare la sicurezza dei dati utilizzando Amazon Forecast?

- Per la crittografia dei dati inattivi, puoi utilizzare AWS KMS per fornire una CMK gestita dal cliente per proteggere l'archiviazione dei dati sul servizio Amazon S3:
  - Abilita la crittografia predefinita sul bucket con la chiave di fornitura e imposta la policy del bucket per accettare AWS KMS la crittografia dei dati durante l'immissione dei dati.
  - Abilita il ruolo del servizio Amazon Forecast 'AmazonForecast- ExecutionRole -*' e il ruolo di amministratore della federazione (ad esempio' customer_forecast_admin_role ') come utente chiave. AWS KMS
- Per la crittografia dei dati in transito, puoi configurare il protocollo HTTPS, necessario durante il trasferimento di oggetti sulla policy dei bucket di Amazon S3.
- Ulteriori restrizioni sul controllo degli accessi, abilita una policy bucket per l'accesso approvato per il ruolo del servizio Amazon Forecast 'AmazonForecast- ExecutionRole -*' e il ruolo di amministratore (ad esempio' customer_forecast_admin_role ').

D: Quali sono le best practice per l'utilizzo di Amazon Forecast?

- Dovresti avere una buona conoscenza delle tue pratiche di classificazione dei dati e mappare le relative esigenze di sicurezza dei dati durante l'utilizzo dei bucket S3 con Amazon Forecast.
- Per la configurazione dei bucket Amazon S3, ti consigliamo vivamente di abilitare l'applicazione HTTPS nella tua policy sui bucket S3.
- Devi conoscere il ruolo di amministratore «customer_forecast_admin_role» che supporta l'accesso permissivo (oggetti S3) sui bucket Amazon Get/Delete/Put S3 con il nome «customer-forecast-*». NOTA: se hai bisogno di un controllo granulare degli accessi per più team, segui queste pratiche:
  - Definisci l'identità IAM di accesso basata sul team (ruolo/utente) con accesso con privilegi minimi ai bucket Amazon S3 correlati.

- Crea in base alla concessione dell'accesso adeguato alle identità IAM corrispondenti. team/project AWS KMS CMKs (accesso utente e 'AmazonForecast- ExecutionRole - {team/project}'.
- Imposta la crittografia predefinita del bucket S3 con quella creata. AWS KMS CMKs
- Applica i traffici API S3 con il protocollo HTTPS sulla policy dei bucket S3.
- Applica la configurazione dei bucket S3 per l'accesso approvato per le identità IAM correlate (accesso utente) e «AmazonForecast- - ExecutionRole {team/project}» ai bucket.

- Se desideri utilizzare il 'customer_forecast_admin_role' per scopi generici, prendi in considerazione i punti elencati in precedenza per proteggere i bucket S3.

D: Dove sono le informazioni sulla conformità relative ad Amazon Forecast?

Consulta il programma di conformità dei AWS servizi.

Usa AMS SSP per effettuare il provisioning di Amazon FSx nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle FSx funzionalità di Amazon direttamente dal tuo account gestito AMS. Amazon FSx fornisce file system di terze parti completamente gestiti. Amazon FSx offre la compatibilità nativa dei file system di terze parti con set di funzionalità per carichi di lavoro come lo storage basato su Windows, l'elaborazione ad alte prestazioni (HPC), l'apprendimento automatico e l'automazione della progettazione elettronica (EDA). Amazon FSx automatizza le attività amministrative che richiedono molto tempo come il provisioning dell'hardware, la configurazione del software, l'applicazione di patch e i backup. Amazon FSx integra i file system con AWS servizi nativi del cloud, rendendoli ancora più utili per un set più ampio di carichi di lavoro.

Amazon ti FSx offre due file system tra cui scegliere: Amazon FSx per Windows File Server per applicazioni basate su Windows e Amazon for Lustre FSx per carichi di lavoro a elaborazione intensiva. Per ulteriori informazioni, consulta Amazon FSx.

Domande frequenti su Amazon FSx in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon FSx nel mio account AMS?

Richiedi l'accesso ad Amazon FSx inviando una RFC con il servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce `customer_fsx_admin_role` il seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo di Amazon FSx nel mio account AMS?

Non ci sono restrizioni. È disponibile la piena funzionalità del servizio.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon FSx nel mio account AMS?

Non ci sono prerequisiti. Tuttavia, per configurazioni avanzate come Multi-AZ, è necessario installare e gestire i servizi DFS Replication e DFS Namespaces. Per ulteriori informazioni, vedere Implementazione di file system Multi-AZ.

D: Come faccio a integrare il mio FSx file system Amazon con Managed AD per una landing zone multi-account?

Quando crei un FSx file system Amazon, puoi specificare il tuo MALZ Managed AD come «AWS Managed Microsoft Active Directory» per l'autenticazione di Windows. Per ulteriori informazioni, consulta Usare Amazon FSx with AWS Directory Service per Microsoft Active Directory

Inoltre, devi prima condividere Managed AD con l'account dell'applicazione. A tale scopo, inviare una RFC con il tipo di modifica della directory Management | Directory | Directory | Share directory (ct-369odosk0pd9w).

D: Quali utenti appartengono al gruppo AWS Delegated FSx Administrators?

Solo amministratori di file server IT. Questo gruppo dispone di privilegi di accesso completo su tutte le condivisioni di file.

D: Devo usare la condivisione di file predefinita, share, che viene creata al momento del provisioning del FSx sistema?

No, non è consigliabile utilizzare la condivisione di file predefinita, share, così come fornita. Garantisce l'accesso completo a tutti, il che viola il principio del privilegio minimo. Crea invece condivisioni di file personalizzate più piccole che soddisfino le tue esigenze aziendali.

D: Come posso creare condivisioni di file personalizzate per organizzazioni specifiche della mia azienda?

Vedi Condivisioni di file per istruzioni sulla creazione di condivisioni di file personalizzate. Limita l'accesso a ogni condivisione di file utilizzando il principio del privilegio minimo.

Usa AMS SSP per effettuare il provisioning di Amazon FSx for OpenZFS nel tuo account AMS

Usa la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon FSx for OpenZFS direttamente dal tuo account gestito AMS. FSx for OpenZFS è un servizio di archiviazione di file completamente gestito che semplifica lo spostamento dei dati che risiedono in ZFS locali o in altri file server basati su Linux su AWS senza modificare il codice dell'applicazione o il modo in cui gestisci i dati. Offre uno storage di file altamente affidabile, scalabile, performante e ricco di funzionalità basato sul file system open source OpenZFS, fornendo le caratteristiche e le funzionalità familiari dei file system OpenZFS con l'agilità, la scalabilità e la semplicità di un AWS servizio completamente gestito. Per gli sviluppatori che creano applicazioni native per il cloud, offre uno storage semplice e ad alte prestazioni con ricche funzionalità per lavorare con i dati.

FSx i file system per OpenZFS sono ampiamente accessibili da istanze di calcolo e contenitori Linux, Windows e macOS utilizzando il protocollo NFS standard del settore (v3, v4.0, v4.1, v4.2). Basato sui processori AWS Graviton e sulle più recenti tecnologie di AWS disco e rete (tra cui la rete AWS Scalable Reliable Datagram e il sistema AWS Nitro), FSx per OpenZFS offre fino a 1 milione di IOPS con latenze di centinaia di microsecondi. Con il supporto completo per le funzionalità di OpenZFS come point-in-time istantanee istantanee e clonazione dei dati, FSx per OpenZFS è facile sostituire i file server locali con uno AWS storage che offre funzionalità di file system familiari ed elimina la necessità di eseguire lunghe qualifiche e modificare o riprogettare applicazioni o strumenti esistenti. Inoltre, combinando la potenza delle funzionalità di gestione dei dati di OpenZFS con le alte prestazioni e l'efficienza in termini di costi delle più recenti tecnologie AWS, OpenZFS ti consente di creare ed eseguire applicazioni FSx ad alte prestazioni e ad alta intensità di dati.

Essendo un servizio completamente gestito, FSx OpenZFS semplifica l'avvio, l'esecuzione e la scalabilità di file system completamente gestiti in sostituzione dei file server utilizzati in locale, AWS contribuendo al contempo a fornire una migliore agilità e a ridurre i costi. Con FSx for OpenZFS, non devi più preoccuparti di configurare e fornire file server e volumi di archiviazione, replicare dati, installare e applicare patch al software dei file server, rilevare e risolvere guasti hardware ed eseguire backup manuali. Fornisce inoltre una ricca integrazione con altri AWS servizi, come AWS Identity and Access Management (IAM), AWS Key Management Service (AWS KMS) CloudWatch, Amazon e AWS CloudTrail.

Amazon ti FSx offre due file system tra cui scegliere: Amazon FSx per Windows File Server per applicazioni basate su Windows e Amazon for Lustre FSx per carichi di lavoro a elaborazione intensiva. Per ulteriori informazioni, consulta Amazon FSx.

Domande frequenti su Amazon FSx per OpenZFS in AWS Managed Services

D: Come posso richiedere l'accesso FSx per l'utilizzo di OpenZFS nel mio account AMS?

Richiedi l'accesso ad Amazon FSx OpenZFS inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC fornisce il `customer_fsx_ontap_admin_role` seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo FSx di OpenZFS nel mio account AMS?

La sostituzione del gruppo di sicurezza sulle interfacce di rete FSx elastiche di Amazon (ENIs) richiede l'invio di Management | Other | Other | Update RFCs poiché i gruppi di sicurezza rappresentano un perimetro critico per l'ambiente AMS. Questa è l'unica restrizione.

D: Quali sono i prerequisiti o le dipendenze da utilizzare FSx per OpenZFS nel mio account AMS?

Non ci sono prerequisiti. Tuttavia, è necessario averlo Usa AMS SSP per effettuare il provisioning di Amazon FSx nel tuo account AMS installato.

Usa AMS SSP per fornire Amazon FSx for NetApp ONTAP nel tuo account AMS

Usa la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon FSx for NetApp ONTAP direttamente dal tuo account gestito AMS. Amazon FSx for NetApp ONTAP è un servizio completamente gestito che fornisce uno storage di file altamente affidabile, scalabile, performante e ricco di funzionalità basato sul NetApp popolare file system ONTAP. Fornisce le caratteristiche, le prestazioni, le capacità e i NetApp file system familiari con l'agilità, la scalabilità e la semplicità APIs di un sistema completamente gestito. Servizio AWS

Amazon FSx for NetApp ONTAP offre uno storage di file condiviso ricco di funzionalità, veloce e flessibile, ampiamente accessibile da istanze di calcolo Linux, Windows e macOS in esecuzione in locale o in locale. AWS FSx for ONTAP offre storage SSD ad alte prestazioni con latenze inferiori al millisecondo e semplifica e velocizza la gestione dei dati consentendoti di creare istantanee, clonare e replicare i file con un semplice clic. Inoltre, suddivide automaticamente i dati su uno storage elastico a basso costo, eliminando la necessità di fornire o gestire la capacità e consentendoti di raggiungere livelli di prestazioni SSD per il tuo carico di lavoro pagando lo storage SSD solo per una piccola parte dei tuoi dati. Fornisce uno storage ad alta disponibilità e duraturo con backup completamente gestiti

e supporto per il disaster recovery interregionale e supporta le più diffuse applicazioni antivirus e di sicurezza dei dati che semplificano ulteriormente la protezione e la protezione dei dati. Per i clienti che utilizzano NetApp ONTAP in locale, FSx per ONTAP è la soluzione ideale per migrare, eseguire il backup o eseguire il backup delle applicazioni basate su file da locali a applicazioni basate su file AWS senza la necessità di modificare il codice dell'applicazione o il modo in cui gestisci i dati.

Essendo un servizio completamente gestito, Amazon FSx for NetApp ONTAP semplifica l'avvio e la scalabilità di uno storage di file condiviso affidabile, performante e sicuro nel cloud. Con Amazon FSx for NetApp ONTAP, non devi più preoccuparti di configurare e fornire file server e volumi di storage, replicare dati, installare e applicare patch al software dei file server, rilevare e risolvere i guasti hardware, gestire failover e failback ed eseguire backup manuali. Fornisce inoltre una ricca integrazione con altri Servizi AWS AWS Identity and Access Management, come Amazon WorkSpaces e AWS CloudTrail. AWS Key Management Service

Amazon ti FSx offre due file system tra cui scegliere: Amazon FSx per Windows File Server per applicazioni basate su Windows e Amazon for Lustre FSx per carichi di lavoro a elaborazione intensiva. Per ulteriori informazioni, consulta Amazon FSx.

Domande frequenti su Amazon FSx for NetApp ONTAP in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon FSx for NetApp ONTAP nel mio account AMS?

Richiedi l'accesso ad Amazon FSx for NetApp ONTAP inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC fornisce `customer_fsx_ontap_admin_role` il seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon FSx for NetApp ONTAP nel mio account AMS?

La sostituzione del gruppo di sicurezza sulle interfacce di rete elastiche di Amazon FSx for NetApp ONTAP (ENIs) richiede l'invio di Management | Other | Other | Update RFCs poiché i gruppi di sicurezza rappresentano un perimetro critico per l'ambiente AMS. Questa è l'unica restrizione.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon FSx for NetApp ONTAP nel mio account AMS?

Non ci sono prerequisiti. Tuttavia, è necessario averlo Usa AMS SSP per effettuare il provisioning di Amazon FSx nel tuo account AMS installato.

Usa AMS SSP per effettuare il provisioning di Amazon Inspector Classic nel tuo account AMS

> **Note**
>
> Avviso di fine del supporto: il 20 maggio 2026, AWS terminerà il supporto per Amazon Inspector Classic. Dopo il 20 maggio 2026, non potrai più accedere alla console Amazon Inspector Classic o alle risorse di Amazon Inspector Classic. Amazon Inspector Classic non sarà più disponibile per i nuovi account e per gli account che non hanno completato una valutazione negli ultimi sei mesi. Per tutti gli altri account, l'accesso rimarrà valido fino al 20 maggio 2026, dopodiché non potrai più accedere alla console Amazon Inspector Classic o alle risorse Amazon Inspector Classic. Per ulteriori informazioni, consulta la pagina relativa alla fine del supporto di Amazon Inspector Classic.

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Inspector Classic direttamente nel tuo account gestito AMS. Amazon Inspector Classic è un servizio di valutazione della sicurezza automatizzato che aiuta a migliorare la sicurezza e la conformità delle applicazioni distribuite su. AWS Amazon Inspector Classic valuta automaticamente le applicazioni in base all'esposizione, alle vulnerabilità e alle deviazioni dalle best practice. Dopo aver eseguito una valutazione, Amazon Inspector Classic produce un elenco dettagliato di risultati di sicurezza con priorità in base al livello di gravità. Questi risultati possono essere esaminati direttamente o come parte di report di valutazione dettagliati, disponibili tramite la console o l'API di Amazon Inspector Classic. Per ulteriori informazioni, consulta Amazon Inspector Classic.

Domande frequenti su Amazon Inspector in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon Inspector Classic nel mio account AMS?

Richiedi l'accesso ad Amazon Inspector Classic inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC fornisce il ruolo IAM al tuo account. `customer_inspector_admin_role` Il ruolo include la policy AWS gestita AmazonInspectorFullAccess . Una volta effettuato il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon Inspector Classic nel mio account AMS?

Non ci sono restrizioni. La funzionalità completa di Amazon Inspector Classic è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Inspector Classic nel mio account AMS?

Non ci sono prerequisiti o dipendenze per utilizzare Amazon Inspector Classic nel tuo account AMS.

Usa il nuovo Amazon Inspector in AMS

Ora puoi utilizzare il nuovo Amazon Inspector nel tuo account AMS.

Per Amazon Inspector Classic, `AmazonInspectorFullAccess` erano necessari i dati `customer-inspector-admin-role-ssm-inspector-agent-policy` e. Tuttavia, è stato apportato un aggiornamento al ruolo SSPS`customer-inspector-admin-role`, che ora ne include uno aggiuntivo. `policyAmazonInspector2FullAccess` Questa nuova politica consente le autorizzazioni API per la nuova versione di Amazon Inspector.

Usa AMS SSP per effettuare il provisioning di Amazon Kendra nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Kendra direttamente dal tuo account gestito AMS. Amazon Kendra è un servizio di ricerca intelligente che utilizza l'elaborazione del linguaggio naturale e algoritmi avanzati di apprendimento automatico per restituire risposte specifiche alle domande di ricerca dai tuoi dati. A differenza della ricerca tradizionale basata su parole chiave, Amazon Kendra utilizza le sue capacità di comprensione semantica e contestuale per determinare se un documento è pertinente a una query di ricerca. Amazon Kendra restituisce risposte specifiche a domande, quindi la tua esperienza è simile all'interazione con un esperto umano. Amazon Kendra è altamente scalabile, in grado di soddisfare le esigenze di prestazioni, è strettamente integrato con altri servizi AWS come Amazon S3 e Amazon Lex e offre una sicurezza di livello aziendale. Per ulteriori informazioni, consulta Amazon Kendra;.

Domande frequenti su Amazon Kendra in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon Kendra nel mio account AMS?

Per richiedere l'accesso ad Amazon Inspector Classic, invia una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Add (ct-3qe6io8t6jtny). Questa RFC fornisce il ruolo IAM al tuo account. `customer_kendra_console_role` Dopo aver effettuato il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon Kendra nel mio account AMS?

Non ci sono restrizioni. La funzionalità completa di Amazon Kendra è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Kendra nel mio account AMS?

Non ci sono prerequisiti o dipendenze per iniziare a usare Amazon Kendra. Tuttavia, a seconda del caso d'uso specifico, potrebbe essere necessario accedere ad altri servizi. AWS

Usa AMS SSP per effettuare il provisioning di Amazon Kinesis Data Streams nel tuo account AMS

Usa la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Kinesis Data Streams (KDS) direttamente nel tuo account gestito AMS. Amazon Kinesis Data Streams è un servizio di streaming di dati in tempo reale altamente scalabile e durevole. KDS può acquisire continuamente gigabyte di dati al secondo da centinaia di migliaia di fonti come clickstream di siti Web, flussi di eventi di database, transazioni finanziarie, feed di social media, registri IT ed eventi di tracciamento della posizione. I dati raccolti sono disponibili in millisecondi per consentire casi d'uso di analisi in tempo reale come dashboard in tempo reale, rilevamento di anomalie in tempo reale, prezzi dinamici e altro ancora. Per ulteriori informazioni, consulta Amazon Kinesis Data Streams.

Domande frequenti su Kinesis Data Streams in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso ad Amazon Kinesis Data Streams nel mio account AMS?

Richiedi l'accesso ad Amazon Kinesis Data Streams inviando una RFC con il servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC `customer_kinesis_data_streaming_user_role` fornisce il seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon Kinesis Data Streams nel mio account AMS?

Non ci sono restrizioni. La funzionalità completa di Amazon Kinesis Data Streams è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Kinesis Data Streams nel mio account AMS?

Non ci sono prerequisiti o dipendenze per utilizzare Amazon Kinesis Data Streams nel tuo account AMS.

Usa AMS SSP per effettuare il provisioning di Amazon Kinesis Video Streams nel tuo account AMS

Usa la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Kinesis Video Streams (KVS) direttamente nel tuo account gestito AMS. Amazon Kinesis Video Streams ti aiuta a trasmettere video in modo sicuro dai AWS dispositivi collegati per analisi, apprendimento automatico (ML), riproduzione e altre elaborazioni. Kinesis Video Streams effettua automaticamente il provisioning e ridimensiona elasticamente tutta l'infrastruttura necessaria per importare i dati video in streaming da milioni di dispositivi. Inoltre, archivia, crittografa e indicizza in modo duraturo i dati video nei tuoi stream e ti consente di accedervi tramite. easy-to-use APIs Kinesis Video Streams consente di riprodurre video per la visualizzazione dal vivo e su richiesta e di creare rapidamente applicazioni che sfruttano la visione artificiale e l'analisi video attraverso l'integrazione con Amazon Rekognition Video e librerie per framework ML come Apache e OpenCV. MxNet TensorFlow Per ulteriori informazioni, consulta Amazon Kinesis Video Streams.

Domande frequenti su Amazon Kinesis Video Streams in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso ad Amazon Kinesis Video Streams nel mio account AMS?

Richiedi l'accesso ad Amazon Kinesis Video Streams inviando una RFC con AWS Management | service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC `customer_kinesis_video_streaming_user_role` fornisce il seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon Kinesis Video Streams nel mio account AMS?

Non ci sono restrizioni. La funzionalità completa di Amazon Kinesis Video Streams è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Kinesis Video Streams nel mio account AMS?

Non ci sono prerequisiti o dipendenze per utilizzare Amazon Kinesis Video Streams nel tuo account AMS.

Usa AMS SSP per fornire Amazon Lex nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Lex direttamente nel tuo account gestito AMS. Amazon Lex è un servizio per la creazione di interfacce conversazionali in qualsiasi applicazione utilizzando voce e testo. Amazon Lex offre le funzionalità avanzate di deep learning del riconoscimento vocale automatico (ASR) per convertire la voce in testo e la comprensione del linguaggio naturale (NLU) per riconoscere l'intento del testo, per consentirti di creare applicazioni con esperienze utente altamente coinvolgenti e interazioni conversazionali realistiche. Con Amazon Lex, le stesse tecnologie di deep learning alla base di Amazon Alexa sono ora disponibili per tutti gli sviluppatori, consentendoti di creare bot o chatbot conversazionali sofisticati in linguaggio naturale in modo rapido e semplice. Per ulteriori informazioni, consulta Amazon Lex.

Domande frequenti su Amazon Lex in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso ad Amazon Lex nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce il seguente ruolo IAM al tuo account:. `customer_lex_author_role` Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon Lex nel mio account AMS?

L'integrazione di Amazon Lex con Lambda è limitata alle funzioni Lambda senza prefisso «AMS-», al fine di prevenire eventuali modifiche all'infrastruttura AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Lex nel mio account AMS?

Non ci sono prerequisiti o dipendenze per utilizzare Amazon Lex nel tuo account AMS.

Usa AMS SSP per effettuare il provisioning di Amazon MQ nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon MQ direttamente nel tuo account gestito AMS. Amazon MQ è un servizio di broker di messaggi

gestito per Apache ActiveMQ che ti aiuta a configurare e gestire broker di messaggi nel cloud. I broker di messaggi consentono a diversi sistemi software, spesso utilizzando linguaggi di programmazione diversi e su piattaforme diverse, di comunicare e scambiare informazioni. Amazon MQ riduce il carico operativo gestendo il provisioning, la configurazione e la manutenzione di ActiveMQ, un popolare broker di messaggi open source. La connessione delle applicazioni correnti ad Amazon MQ utilizza standard APIs e protocolli di messaggistica del settore, tra cui JMS, NMS, AMQP, STOMP, MQTT e. WebSocket L'utilizzo degli standard significa che, nella maggior parte dei casi, non è necessario riscrivere alcun codice di messaggistica durante la migrazione a. AWS Per ulteriori informazioni, consulta What Is Amazon MQ?

Domande frequenti su Amazon MQ in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso ad Amazon MQ nel mio account AMS?

L'utilizzo di Amazon MQ nel tuo account AMS è un processo in due fasi:

1. Effettua il provisioning di Amazon MQ Broker. A tale scopo, invia un modello CFN, con Amazon MQ Broker incluso, tramite una RFC con Deployment | Ingestion | Stack from CloudFormation Template | Create change type (ct-36cn2avfrrj9v) oppure invia una RFC con Management | Altro | Altro | Create change type (ct-1e1xtak34nx76) richiedendo il provisioning di Amazon MQ Broker in il tuo account.
2. Accedi alla console Amazon MQ. Dopo aver effettuato il provisioning di Amazon MQ Broker, ottieni l'accesso alla console Amazon MQ inviando una RFC con Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce `customer_mq_console_role` il seguente ruolo IAM al tuo account:.

Dopo aver assegnato il ruolo nel tuo account, devi inserirlo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon MQ nel mio account AMS?

La funzionalità completa di Amazon MQ è disponibile nel tuo account AMS; tuttavia, il provisioning di Amazon MQ Broker non è disponibile tramite la policy a causa dell'elevata autorizzazione richiesta. Vedi sopra per maggiori dettagli su come fornire il broker Amazon MQ nei tuoi account.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon MQ nel mio account AMS?

Non ci sono prerequisiti o dipendenze per utilizzare Amazon MQ nel tuo account AMS.

Usa AMS SSP per fornire Amazon Managed Service for Apache Flink nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Managed Service for Apache Flink direttamente nel tuo account gestito AMS. Managed Service for Apache Flink è il modo più semplice per analizzare i dati in streaming, ottenere informazioni utili e rispondere alle esigenze aziendali e dei clienti in tempo reale. Amazon Managed Service for Apache Flink riduce la complessità di creazione, gestione e integrazione di applicazioni di streaming con altri servizi. AWS Gli utenti SQL possono facilmente interrogare i dati di streaming o creare intere applicazioni di streaming utilizzando modelli e un editor SQL interattivo. Gli sviluppatori Java possono creare rapidamente applicazioni di streaming sofisticate utilizzando librerie e AWS integrazioni Java open source per trasformare e analizzare i dati in tempo reale. Amazon Managed Service per Apache Flink si occupa di tutto il necessario per eseguire le applicazioni in tempo reale in modo continuo e si ridimensiona automaticamente in base al volume e alla velocità effettiva dei dati in ingresso. Con Amazon Managed Service for Apache Flink, paghi solo per le risorse utilizzate dalle tue applicazioni di streaming. Non è prevista alcuna tariffa o costo minimo di installazione. Per ulteriori informazioni, consulta Amazon Managed Service for Apache Flink.

Domande frequenti su Managed Service per Apache Flink in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso ad Amazon Managed Service for Apache Flink nel mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (managed automation) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_kinesis_analytics_application_role` seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo di Amazon Managed Service for Apache Flink nel mio account AMS?

- Le configurazioni sono limitate alle risorse senza prefissi «AMS-» o «MC-» per impedire qualsiasi modifica all'infrastruttura AMS.
- L'autorizzazione a eliminare o creare nuovi Kinesis Data Streams o Firehose è stata rimossa dalla politica. Abbiamo un'altra politica che lo consente.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Kinesis Data Streams nel mio account AMS?

Esistono alcune dipendenze:

- Amazon Managed Service for Apache Flink richiede la creazione di Kinesis Data Streams o Firehose prima di configurare un'applicazione con Managed Service for Apache Flink.
- Le autorizzazioni delle policy basate sulle risorse devono indicare una particolare fonte di dati di input.

Usa AMS SSP per effettuare il provisioning di Amazon Managed Streaming for Apache Kafka nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Managed Streaming for Apache Kafka (Amazon MSK) direttamente nel tuo account gestito AMS. Amazon Managed Streaming for Apache Kafka è un servizio di streaming di dati AWS completamente gestito che semplifica la creazione e l'esecuzione di applicazioni che utilizzano Apache Kafka per elaborare dati in streaming senza dover diventare esperti nella gestione dei cluster Apache Kafka. Amazon MSK gestisce il provisioning, la configurazione e la manutenzione dei cluster Apache Kafka e dei nodi Apache per te. ZooKeeper Amazon MSK mostra anche i principali parametri prestazionali di Apache Kafka nella console. AWS

Amazon MSK offre diversi livelli di sicurezza per i cluster Apache Kafka, tra cui isolamento della rete VPC, autorizzazione API IAM per il piano di controllo AWS , crittografia a riposo, crittografia TLS in transito, autenticazione dei certificati basata su TLS, autenticazione protetta da. SASL/SCRAM Gestione dei segreti AWS Per ulteriori informazioni, consulta Amazon MSK.

Domande frequenti su Amazon MSK in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso ad Amazon MSK nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce le seguenti politiche e ruoli IAM al tuo account:

- `customer-msk-admin-policy.json`
- `AmazonMSKFullAccess`

- `customer-msk-admin-role.json`

Una volta effettuato il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione di federazione.

D: Quali sono le restrizioni all'uso di Amazon MSK?

Affinché Amazon MSK fornisca i log dei broker alle destinazioni che configuri, assicurati che la `AmazonMSKFullAccess` policy sia associata al tuo ruolo IAM. Quindi le autorizzazioni di accesso complete sono già disponibili.

D: Quali sono i prerequisiti o le dipendenze per l'utilizzo di Amazon MSK?

Prima di creare un cluster MSK, è necessario disporre di un VPC e di sottoreti all'interno di tale VPC. Per impostazione predefinita, AMS copre questo aspetto come parte della creazione di VPC AMS predefiniti.

Per informazioni sulle limitazioni di Amazon MSK, consulta Amazon MSK Limits.

Usa AMS SSP per fornire Amazon Managed Service for Prometheus nel tuo account AMS

Usa la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Managed Service for Prometheus (AMP) direttamente nel tuo account gestito AMS. Il servizio gestito da Amazon per Prometheus è un servizio di monitoraggio serverless compatibile con Prometheus per i parametri dei container che semplifica il monitoraggio sicuro di ambienti container su larga scala. Con il servizio gestito da Amazon per Prometheus, puoi utilizzare lo stesso modello di dati open source Prometheus e lo stesso linguaggio di interrogazione che usi oggi per monitorare le prestazioni dei tuoi carichi di lavoro containerizzati e anche godere di una maggiore scalabilità, disponibilità e sicurezza senza dover gestire l'infrastruttura sottostante.

Amazon Managed Service for Prometheus ridimensiona automaticamente l'acquisizione, lo storage e l'interrogazione dei parametri operativi man mano che i carichi di lavoro aumentano e diminuiscono. Si integra con AWS i servizi di sicurezza per consentire un accesso rapido e sicuro ai dati. Per ulteriori informazioni, consulta Cos'è Amazon Managed Service per Prometheus?

Domande frequenti su Amazon Managed Service per Prometheus in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso ad Amazon Managed Service for Prometheus nel mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer-prometheus-console-role` seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il `customer-prometheus-console-role` ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo di Amazon Managed Service for Prometheus nel mio account AMS?

Tutte le funzionalità sono supportate.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Managed Service for Prometheus nel mio account AMS?

Non ci sono prerequisiti o dipendenze per iniziare a usare Amazon Managed Service for Prometheus. Tuttavia, a seconda del caso d'uso specifico, potresti aver bisogno di accedere ad altri servizi. AWS

Usa AMS SSP per effettuare il provisioning di Amazon Personalize nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Personalize direttamente nel tuo account gestito AMS. Amazon Personalize è un servizio di apprendimento automatico che consente agli sviluppatori di creare facilmente consigli personalizzati per i clienti che utilizzano le loro applicazioni.

L'apprendimento automatico viene sempre più utilizzato per migliorare il coinvolgimento dei clienti offrendo consigli personalizzati su prodotti e contenuti, risultati di ricerca personalizzati e promozioni di marketing mirate. Tuttavia, lo sviluppo delle capacità di apprendimento automatico necessarie per produrre questi sofisticati sistemi di raccomandazione è oggi fuori dalla portata della maggior parte delle organizzazioni a causa della complessità. Amazon Personalize consente agli sviluppatori senza precedenti esperienze di machine learning di integrare facilmente sofisticate funzionalità di personalizzazione nelle loro applicazioni, utilizzando una tecnologia di apprendimento automatico perfezionata in anni di utilizzo su Amazon.com.

Con Amazon Personalize, fornisci un flusso di attività dalla tua applicazione (clic, visualizzazioni di pagina, iscrizioni, acquisti e così via) oltre a un inventario degli articoli che desideri consigliare, come articoli, prodotti, video o musica. Puoi anche scegliere di fornire ad Amazon Personalize informazioni

demografiche aggiuntive relative ai tuoi utenti, come età o posizione geografica. Amazon Personalize elaborerà ed esaminerà i dati, identificherà ciò che è significativo, selezionerà gli algoritmi giusti e addestrerà e ottimizzerà un modello di personalizzazione personalizzato per i tuoi dati. Tutti i dati analizzati da Amazon Personalize vengono mantenuti privati e protetti e utilizzati solo per i tuoi consigli personalizzati. Puoi iniziare a fornire consigli personalizzati tramite una semplice chiamata API. Paghi solo quello che usi e non ci sono tariffe minime né impegni anticipati.

Per ulteriori informazioni, consulta Amazon Personalize.

Domande frequenti su Amazon Personalize in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon Personalize nel mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (managed automation) (ct-3qe6io8t6jtny) e devi specificare quale bucket S3 contiene i dati che personalizza deve utilizzare per generare i consigli. AWS Questa RFC `customer_personalize_console_role` `customer_personalize_service_role` fornisce i seguenti ruoli IAM al tuo account: e.

- Una volta effettuato `customer_personalize_console_role` il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione di federazione. Puoi anche associarlo `customer_personalize_console_policy` a un altro ruolo esistente diverso da. `Customer_ReadOnly_Role`
- Dopo averlo fornito al tuo account, puoi fare riferimento al relativo ARN quando crei un nuovo gruppo di set di dati. `customer_personalize_service_role`

Al momento, AMS Operations implementerà anche questo ruolo di servizio nel tuo account:. `aws_code_pipeline_service_role_policy`

D: Quali sono le restrizioni all'uso di Amazon Personalize nel mio account AMS?

La configurazione di Amazon Personalize è limitata alle risorse senza prefissi 'ams-' o 'mc-', per evitare modifiche all'infrastruttura AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Personalize nel mio account AMS?

- Se il bucket S3 in cui sono archiviati i dati è crittografato, è necessario fornire l'ID della chiave KMS, in modo da consentire al ruolo utilizzato da Amazon Personalize di decrittografare il bucket.

Amazon Personalize non supporta la chiave KMS S3 predefinita. Se necessario per utilizzare KMS, crea una chiave personalizzata e aggiungi la seguente policy aprendo una RFC con il tipo di modifica KMS Key | Create (Managed automation):

JSON

```
{
    "Version":"2012-10-17",
    "Id": "key-consolepolicy-3",
    "Statement": [
        {
            "Sid": "Enable IAM User Permissions",
            "Effect": "Allow",
            "Principal": {
                "Service": "personalize.amazonaws.com"
            },
            "Action": "kms:*",
            "Resource": "*"
        }
    ]
}
```

- È necessario creare un bucket S3 con la seguente policy relativa ai bucket. A tale scopo, invia una RFC con tipo di modifica S3 Storage | Create Policy. Questa politica consente ad Amazon Personalize di accedere ai dati; quel bucket conterrà i dati che verranno utilizzati da Amazon Personalize.

  JSON

```
{
"Version":"2012-10-17",
"Id": "PersonalizeS3BucketAccessPolicy",
"Statement": [
{
"Sid": "PersonalizeS3BucketAccessPolicy",
"Effect": "Allow",
"Principal": {
"Service": "personalize.amazonaws.com"
},
"Action": [
"s3:GetObject",
"s3:ListBucket"
```

```
],
"Resource": [
"arn:aws:s3:::bucket-name",
"arn:aws:s3:::bucket-name/*"
]
}
]
}
```

Usa AMS SSP per effettuare il provisioning di Amazon Quick nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità Quick direttamente dal tuo account gestito AMS. Quick è un servizio di business intelligence veloce e basato sul cloud che fornisce informazioni dettagliate a tutti i membri dell'organizzazione. Essendo un servizio completamente gestito, Quick consente di creare e pubblicare facilmente dashboard interattivi che includono approfondimenti sull'apprendimento automatico (ML). Per ulteriori informazioni, consulta Amazon Quick.

Domande frequenti su Quick in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso a Quick nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce il seguente ruolo IAM al tuo account:. `customer_quicksight_console_admin_role` Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo di Quick nel mio account AMS?

- AWS le impostazioni delle risorse su Quick non saranno accessibili a causa della dipendenza dalla politica IAM. Tuttavia, il team AMS abilita ogni risorsa per te in risposta alla tua richiesta di abilitare il servizio.
- L'accesso alle risorse per singoli utenti e gruppi non è supportato in questo modello perché questa funzionalità consente agli utenti di modificare le autorizzazioni IAM che potrebbero compromettere l'infrastruttura AMS.

- La possibilità di invitare identità IAM dall'interno non QuickSight è supportata a causa del rischio legato all'alterazione degli oggetti IAM.
- Quick service offre due edizioni: Enterprise e Standard. Entrambi forniscono un'opzione Single Sign-On (SSO) supportata da AMS. Tuttavia, l'Enterprise Edition offre un'opzione per integrare Quick con Active Directory (AD). Quick on AMS non supporta l'integrazione con AD a causa di incompatibilità tra la struttura degli account AMS e i requisiti Quick Trust.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Quick nel mio account AMS?

- Quando AMS riceve questa RFC per aggiungere Quick, ti viene inviata una richiesta di assistenza per ulteriori informazioni; fornisci loro quanto segue:
  - Nome dell'account Quick (ad esempio, *`CustomerName`*`-quicksight`
  - Quick Edition (Standard o Enterprise)
  - La AWS regione in cui abilitare il servizio Quick (l'impostazione predefinita è la regione AMS AWS).
  - Un indirizzo e-mail di notifica per l'account Quick.
  - (Facoltativo) Il bucket S3 in cui si trovano i file di dati da analizzare.
  - Il VPC e la sottorete IDs che si connettono a Quick supportano una funzionalità per aggiungere una connessione VPC, che consente la connettività privata tra Quick e le risorse all'interno dell'account.

Un operatore AMS esegue la procedura di registrazione per tuo conto e configura due funzionalità: QuickSight

- Rilevamento automatico delle fonti di dati.
- Connessioni VPC.

> **Note**
>
> Queste azioni devono essere eseguite da un operatore AMS perché durante il processo di accesso sono richieste autorizzazioni IAM e VPC elevate.

Usa AMS SSP per effettuare il provisioning di Amazon Rekognition nel tuo account AMS

Usa la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Rekognition direttamente nel tuo account gestito AMS. Amazon Rekognition semplifica l'aggiunta di analisi di immagini e video alle applicazioni utilizzando una tecnologia di deep learning collaudata e altamente scalabile che non richiede competenze di machine learning per essere utilizzata. Con Amazon Rekognition, puoi identificare oggetti, persone, testo, scene e attività in immagini e video, oltre a rilevare eventuali contenuti inappropriati. Amazon Rekognition offre anche funzionalità di analisi e ricerca facciale estremamente accurate che puoi utilizzare per rilevare, analizzare e confrontare i volti per un'ampia varietà di casi d'uso in materia di verifica degli utenti, conteggio delle persone e sicurezza pubblica.

Con Amazon Rekognition Custom Labels, puoi identificare oggetti e scene in immagini specifiche per le tue esigenze aziendali. Ad esempio, puoi creare un modello per classificare parti specifiche della macchina sulla linea di assemblaggio o per rilevare piante non sane. Amazon Rekognition Custom Labels si occupa dello sviluppo di modelli per te, quindi non è richiesta alcuna esperienza di machine learning. Devi semplicemente fornire immagini di oggetti o scene che desideri identificare e il servizio si occuperà del resto.

Per ulteriori informazioni, consulta Amazon Rekognition.

Domande frequenti su Amazon Rekognition in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso ad Amazon Rekognition nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_rekognition_console_role & customer_rekognition_service_role` seguente ruolo IAM al tuo account:. Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon Rekognition nel mio account AMS?

La funzionalità completa di Amazon Rekognition è disponibile con il ruolo di servizio autofornito di Amazon Rekognition.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Rekognition nel mio account AMS?

Se utilizzi Kinesis Video Streams che fornisce lo streaming video di origine per uno stream processor Amazon Rekognition Video o un flusso di dati come destinazione per scrivere dati su Kinesis Data Streams, fornisci ad AMS un messaggio quando crei la RFC. `kinesisStreamName`

Usa AMS SSP per effettuare il provisioning di Amazon SageMaker AI nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon SageMaker AI direttamente nel tuo account gestito AMS. SageMaker L'intelligenza artificiale offre a ogni sviluppatore e data scientist la possibilità di creare, addestrare e implementare rapidamente modelli di apprendimento automatico. Amazon SageMaker AI è un servizio completamente gestito che copre l'intero flusso di lavoro di machine learning per etichettare e preparare i dati, scegliere un algoritmo, addestrare il modello, ottimizzarlo e ottimizzarlo per la distribuzione, fare previsioni e agire. I tuoi modelli entrano in produzione più velocemente con molto meno sforzo e costi inferiori. Per ulteriori informazioni, consulta Amazon SageMaker AI.

SageMaker Domande frequenti sull'intelligenza artificiale in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso all' SageMaker IA nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli IAM al tuo account: e al ruolo di servizio. `customer_sagemaker_admin_role` `AmazonSageMaker-ExecutionRole-Admin` Dopo aver inserito l' SageMaker IA nel tuo account, devi integrare il `customer_sagemaker_admin_role` ruolo nella tua soluzione di federazione. L'utente non può accedere direttamente al ruolo di servizio; il servizio di SageMaker intelligenza artificiale lo utilizza per eseguire varie azioni, come descritto qui: Passing Roles.

D: Quali sono le restrizioni all'uso dell' SageMaker IA nel mio account AMS?

- I seguenti casi d'uso non sono supportati dal ruolo AMS Amazon SageMaker AI IAM:
  - SageMaker AI Studio non è supportato in questo momento.
  - SageMaker AI Ground Truth per la gestione della forza lavoro privata non è supportata poiché questa funzionalità richiede un accesso eccessivamente permissivo alle risorse di Amazon Cognito. Se è necessario gestire una forza lavoro privata, puoi richiedere un ruolo IAM personalizzato con autorizzazioni combinate SageMaker AI e Amazon Cognito. Altrimenti,

consigliamo di utilizzare forza lavoro pubblica (supportata da Amazon Mechanical Turk) Marketplace AWS o fornitori di servizi per l'etichettatura dei dati.

- Creazione di endpoint VPC per supportare le chiamate API SageMaker ai servizi di intelligenza artificiale (aws.sagemaker). {regione} .notebook, com.amazonaws. {regione} .sagemaker.api e com.amazonaws. {region} .sagemaker.runtime) non è supportata in quanto le autorizzazioni non possono essere limitate ai soli servizi relativi all'intelligenza artificiale. SageMaker Per supportare questo caso d'uso, invia una RFC Management | Other | Other per creare endpoint VPC correlati.
- SageMaker La scalabilità automatica degli endpoint AI non è supportata in quanto l' SageMaker IA richiede `DeleteAlarm` autorizzazioni su qualsiasi risorsa («*»). Per supportare la scalabilità automatica degli endpoint, invia una richiesta RFC Management | Other | Other per configurare la scalabilità automatica per un endpoint AI. SageMaker

D: Quali sono i prerequisiti o le dipendenze per utilizzare l'IA nel mio account AMS? SageMaker

- I seguenti casi d'uso richiedono una configurazione speciale prima dell'uso:
  - Se verrà utilizzato un bucket S3 per archiviare artefatti e dati del modello, è necessario richiedere un bucket S3 denominato con le parole chiave richieste (» SageMaker «, «Sagemaker», «sagemaker» o «aws-glue») con Deployment | Advanced stack components | S3 storage | Create RFC.
  - Se verrà utilizzato Elastic File Store (EFS), lo storage EFS deve essere configurato nella stessa sottorete e consentito dai gruppi di sicurezza.
  - Se altre risorse richiedono l'accesso diretto SageMaker ai servizi di intelligenza artificiale (notebook, API, runtime e così via), la configurazione deve essere richiesta da:
    - Invio di una RFC per creare un gruppo di sicurezza per l'endpoint (Deployment | Advanced stack components | Security group | Create (auto)).
    - Invio di una gestione | Altro | Altro | Crea RFC per configurare gli endpoint VPC correlati.

D: Quali sono le convenzioni di denominazione supportate per le risorse a cui possono accedere direttamente? **`customer_sagemaker_admin_role`** (Quanto segue riguarda le autorizzazioni di aggiornamento ed eliminazione; se hai bisogno di convenzioni di denominazione supportate aggiuntive per le tue risorse, contatta un AMS Cloud Architect per una consulenza.)

- Risorsa: ruolo di passaggio `AmazonSageMaker-ExecutionRole-*`

    - Autorizzazioni: il ruolo di servizio con assegnazione automatica dell' SageMaker IA supporta l'utilizzo del ruolo di servizio SageMaker AI (`AmazonSageMaker-ExecutionRole-*`) con AWS Glue, AWS RoboMaker e. AWS Step Functions
- Risorsa: Secrets on AWS Secrets Manager
    - Autorizzazioni: descrivi, crea, ottieni, aggiorna i segreti con un `AmazonSageMaker-*` prefisso.
    - Autorizzazioni: descrivi, ottieni segreti quando il tag della `SageMaker` risorsa è impostato su. `true`
- Risorsa: archivi attivi AWS CodeCommit
    - Autorizzazioni: creare/eliminare repository con un prefisso. `AmazonSageMaker-*`
    - Autorizzazioni: Git Pull/Push su repository con i seguenti prefissi,, `*sagemaker*` e. `*SageMaker* *Sagemaker*`
- Risorsa: repository Amazon ECR (Amazon Elastic Container Registry)
    - Autorizzazioni: Autorizzazioni: imposta, elimina le politiche del repository e carica le immagini dei contenitori, quando viene utilizzata la seguente convenzione di denominazione delle risorse,. `*sagemaker*`
- Risorsa: bucket Amazon S3
    - Autorizzazioni: Get, Put, Delete object, annulla il caricamento multipart di oggetti S3 quando le risorse hanno i seguenti prefissi:,, e. `*SageMaker* *Sagemaker* *sagemaker* aws-glue`
    - Autorizzazioni: ottieni oggetti S3 quando il tag è impostato su. `SageMaker true`
- Risorsa: Amazon CloudWatch Log Group
    - Autorizzazioni: Create Log Group o Stream, Put Log Event, List, Update, Create, Delete log delivery con il seguente prefisso:. `/aws/sagemaker/*`
- Risorsa: Amazon CloudWatch Metric
    - Autorizzazioni: inserisci i dati metrici quando vengono utilizzati i seguenti prefissi:`AWS/SageMaker`,,,, `AWS/SageMaker/aws/SageMaker`, `aws/SageMaker/` e. `aws/sagemaker aws/sagemaker/ /aws/sagemaker/.`
- Risorsa: Amazon CloudWatch Dashboard
    - Autorizzazioni: Create/Delete dashboard quando vengono utilizzati i seguenti prefissi:. `customer_*`
- Risorsa: argomento Amazon SNS (Simple Notification Service)
    - Autorizzazioni: Subscribe/Create argomento in cui vengono utilizzati i seguenti prefissi:`*sagemaker*`, e. `*SageMaker* *Sagemaker*`

D: Qual è la differenza tra e? **`AmazonSageMakerFullAccess`** **`customer_sagemaker_admin_role`**

The `customer_sagemaker_admin_role` with the `customer_sagemaker_admin_policy` fornisce quasi le stesse autorizzazioni AmazonSageMakerFullAccess ad eccezione di:

- Autorizzazione a connettersi con AWS RoboMaker Amazon Cognito e AWS Glue risorse.
- SageMaker Scalabilità automatica degli endpoint AI. È necessario inviare una RFC con il tipo di modifica Management | Advanced stack components | Identity and Access Management (IAM) | Update entità o policy (automazione gestita) (ct-27tuth19k52b4) per elevare le autorizzazioni di scalabilità automatica temporaneamente o permanentemente, poiché la scalabilità automatica richiede l'accesso permissivo al servizio. CloudWatch

D: Come posso adottare la chiave gestita dal cliente nella crittografia dei dati inattivi? AWS KMS

È necessario assicurarsi che la policy delle chiavi sia stata impostata correttamente sulle chiavi gestite dal cliente in modo che gli utenti o i ruoli IAM correlati possano utilizzare le chiavi. Per ulteriori informazioni, consulta il documento AWS KMS Key Policy.

Usa AMS SSP per fornire Amazon Simple Email Service nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Simple Email Service (Amazon SES) direttamente nel tuo account gestito AMS. Amazon Simple Email Service è un servizio di invio e-mail basato sul cloud progettato per aiutare gli esperti di marketing digitale e gli sviluppatori di applicazioni a inviare e-mail di marketing, notifiche e transazionali.

Puoi utilizzare l'interfaccia SMTP o una delle altre AWS SDKs per integrare Amazon SES direttamente nelle tue applicazioni esistenti. Puoi anche integrare le funzionalità di invio e-mail di Amazon SES nel software che già utilizzi, come i sistemi di ticketing e i client di posta elettronica.

Per ulteriori informazioni, consulta Amazon Simple Email Service.

Domande frequenti su Amazon SES in AWS Managed Services

D: Come posso richiedere l'accesso ad Amazon SES nel mio account AMS?

Richiedi l'accesso ad Amazon SES inviando una RFC con il servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce

`customer_ses_admin_role` il seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon SES nel mio account AMS?

- È necessario configurare una policy sui bucket S3 per consentire ad Amazon SES di pubblicare eventi nel bucket.
- È necessario utilizzare una chiave CMK predefinita (AWS SES) o configurare una chiave CMK per consentire ad Amazon SES di crittografare le e-mail e inviare eventi ad altre risorse di servizio come Amazon S3, Amazon SNS, Lambda e Firehose, appartenenti all'account.

D: Quali sono le restrizioni all'uso di Amazon SES nel mio account AMS?

È necessario raccogliere RFCs per creare le seguenti risorse:

- Un utente SMTP e un ruolo di servizio IAM con PutEvents autorizzazione per uno stream Kinesis Firehose.
- È necessario creare nuove AWS risorse come il bucket S3, lo stream Firehose, l'argomento SNS utilizzando i tipi di modifica AMS affinché le destinazioni delle regole e dei set di configurazione di Amazon SES funzionino con tali risorse.
- Credenziali SMTP. Per richiedere nuove credenziali SMTP, usa il tipo di modifica (Gestione | Altro | Altro | Crea). AMS crea le credenziali e le aggiunge a Secrets Manager per te.

Usa AMS SSP per fornire Amazon Simple Workflow Service nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Simple Workflow Service (Amazon SWF) direttamente nel tuo account gestito AMS. Amazon Simple Workflow Service aiuta gli sviluppatori a creare, eseguire e scalare processi in background con passaggi paralleli o sequenziali. Puoi pensare ad Amazon SWF come a un sistema di monitoraggio dello stato e coordinatore di attività completamente gestito nel cloud. Se i passaggi della tua applicazione richiedono più di 500 millisecondi per essere completati, devi monitorare lo stato dell'elaborazione oppure devi ripristinare o riprovare se un'attività fallisce, Amazon SWF può aiutarti. Per ulteriori informazioni, consulta Amazon Simple Workflow Service.

Domande frequenti su Amazon SWF in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso ad Amazon SWF nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce il seguente ruolo IAM al tuo account:. `customer_swf_role` Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon SWF nel mio account AMS?

Le `InvokeFunction` autorizzazioni Lambda sono state incluse in questo servizio, tuttavia, l'AMS aggiunto a tutti i ruoli dei clienti AMS `customer_deny_policy` nega esplicitamente l'accesso alle funzioni AMS Lambda e alle risorse di proprietà di AMS. Per etichettare o rimuovere i tag dalle risorse all'interno di Amazon SWF, invia un tipo di modifica Gestione | Altro | Altro.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon SWF nel mio account AMS?

Amazon SWF dipende dal AWS Lambda servizio, pertanto, le autorizzazioni per richiamare Lambda sono state fornite come parte di questo ruolo e non sono necessarie autorizzazioni aggiuntive per richiamare Lambda da Amazon SWF. Altrimenti, non ci sono prerequisiti per l'utilizzo di Amazon SWF.

Usa AMS SSP per effettuare il provisioning di Amazon Textract nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Textract direttamente nel tuo account gestito AMS. Amazon Textract è un servizio di apprendimento automatico completamente gestito che estrae automaticamente testo stampato, scrittura a mano e altri dati dai documenti scansionati che va oltre il semplice riconoscimento ottico dei caratteri (OCR) per identificare, comprendere ed estrarre dati da moduli e tabelle. Per ulteriori informazioni, consulta Amazon Textract.

Domande frequenti su Amazon Textract in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere la configurazione di Amazon Textract nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce i seguenti ruoli IAM al tuo account:, e. `customer_textract_console_role` `customer_textract_human_review_execution_role` `customer_ec2_textract_instance_profile` Una volta effettuato il provisioning nel tuo account, devi inserire il ruolo `customer_textract_console_role` nella tua soluzione di federazione.

D: Quali sono le restrizioni all'uso di Amazon Textract nel mio account AMS?

Non ci sono restrizioni all'uso di Amazon Textract nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Textract nel mio account AMS?

È necessario richiedere la creazione di un bucket S3 inviando una RFC Deployment | Advanced stack components | S3 storage | Create (ct-1a68ck03fn98r).

Usa AMS SSP per effettuare il provisioning di Amazon Transcribe nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon Transcribe direttamente nel tuo account gestito AMS. Amazon Transcribe è un servizio di riconoscimento vocale automatico completamente gestito e continuamente addestrato che genera automaticamente trascrizioni di testo con data e ora da file audio. Amazon Transcribe consente agli sviluppatori di speech-to-text aggiungere facilmente funzionalità alle proprie applicazioni. La ricerca e l'analisi dei dati audio sono praticamente impossibili da cercare e analizzare per i computer. Pertanto, la voce registrata deve essere convertita in testo prima di poter essere utilizzata nelle applicazioni. Storicamente, i clienti dovevano lavorare con fornitori di servizi di trascrizione che richiedevano loro di firmare contratti costosi ed erano difficili da integrare negli stack tecnologici a loro disposizione per svolgere questo compito. Molti di questi provider utilizzano tecnologie obsolete che non si adattano bene a diversi scenari, come l'audio telefonico a bassa fedeltà, comune nei contact center, che si traduce in una scarsa precisione.

Amazon Transcribe utilizza un processo di deep learning chiamato riconoscimento vocale automatico (ASR) per convertire il parlato in testo, in modo rapido e preciso. Amazon Transcribe può essere utilizzato per trascrivere le chiamate all'assistenza clienti, automatizzare i sottotitoli e i sottotitoli e generare metadati per le risorse multimediali per creare un archivio completamente ricercabile. Puoi usare Amazon Transcribe Medical per aggiungere funzionalità speech-to-text mediche alle applicazioni di documentazione clinica. Per ulteriori informazioni, consulta Amazon Transcribe.

Domande frequenti su Amazon Transcribe in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere la configurazione di Amazon Transcribe nel mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (managed automation) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_transcribe_role` seguente ruolo IAM al tuo account:. Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'uso di Amazon Transcribe nel mio account AMS?

Quando lavori con transcribe, devi usare 'customer-transcribe*' come prefisso per i tuoi bucket, a meno che RA non sia specificato diversamente.

Non puoi creare un ruolo IAM all'interno di Amazon transcribe.

Non puoi utilizzare un bucket S3 gestito dal servizio per i dati di output in SSPS predefinito (se necessario, contatta il tuo account CA).

È necessario inviare Risk Acceptance se si desidera utilizzare chiavi KMS gestite dal cliente che non rientrano nel namespace AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Amazon Transcribe nel mio account AMS?

S3 deve avere accesso ai bucket con il nome 'customer-transcribe*'. KMS è necessario per utilizzare Amazon Transcribe se i bucket S3 sono crittografati con chiavi KMS. Se non è necessario crittografare un bucket, è possibile rimuovere «Consenti». KMStranscribe

Usa AMS SSP per effettuare il provisioning di Amazon WorkSpaces nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle WorkSpaces funzionalità direttamente nel tuo account gestito da AMS. WorkSpaces ti consente di effettuare il provisioning di desktop Microsoft Windows o Amazon Linux virtuali basati su cloud per i tuoi utenti, noti come. WorkSpaces WorkSpaces elimina la necessità di procurarsi e installare hardware o installare software complessi. È possibile aggiungere o rimuovere rapidamente utenti man mano che le proprie esigenze cambiano. Gli utenti vi accedono WorkSpaces utilizzando un'applicazione client da un dispositivo supportato o, per Windows WorkSpaces, un browser Web, e accedono utilizzando le credenziali Active Directory (AD) esistenti in locale.

Per ulteriori informazioni, consulta Amazon WorkSpaces.

WorkSpaces nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso WorkSpaces al mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_workspaces_console_role` seguente ruolo IAM al tuo account:. Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo WorkSpaces nel mio account AMS?

La funzionalità completa di Workspaces è disponibile con il ruolo di servizio WorkSpaces self-provisioned di Amazon.

D: Quali sono i prerequisiti o le dipendenze da utilizzare WorkSpaces nel mio account AMS?

- WorkSpaces sono limitati per AWS regione; pertanto, l'AD Connector deve essere configurato nella stessa AWS regione in cui sono ospitate le WorkSpaces istanze.

  I clienti possono connettersi WorkSpaces al cliente AD utilizzando uno dei due metodi seguenti:

  1. Utilizzo del connettore AD per l'autenticazione tramite proxy al servizio Active Directory locale (preferito):

     Configura Active Directory (AD) Connector nel tuo account AMS prima di integrare l' WorkSpaces istanza con il servizio di directory locale. AD Connector funge da proxy per gli utenti AD esistenti (dal tuo dominio) a cui connettersi WorkSpaces utilizzando le credenziali AD esistenti in locale. Questa opzione è preferibile perché WorkSpaces sono collegate direttamente al dominio locale del cliente, che funge sia da risorsa che da foresta di utenti, garantendo un maggiore controllo da parte del cliente.

     Per ulteriori informazioni, consulta Best Practices for Deploying Amazon WorkSpaces (Scenario 1).
  2. Utilizzo di AD Connector con AWS Microsoft AD, Shared Services VPC e un trust unidirezionale per gli ambienti locali:

     Puoi anche autenticare gli utenti con la tua directory locale stabilendo innanzitutto un trust unidirezionale in uscita da AD gestito da AMS al tuo AD locale. WorkSpaces entrerà a far

parte di AD gestito da AMS utilizzando un AD Connector. WorkSpaces le autorizzazioni di accesso verranno quindi delegate alle WorkSpaces istanze tramite AD gestito da AMS, senza la necessità di stabilire un trust bidirezionale con l'ambiente locale. In questo scenario, la foresta di utenti si troverà nell'AD del cliente e la foresta di risorse sarà nell'AD gestito da AMS (le modifiche all'AD gestito da AMS possono essere richieste tramite RFC). Tieni presente che la connettività tra WorkSpaces VPC e il VPC MALZ Shared Services che esegue AD gestito da AMS viene stabilita tramite Transit Gateway.

Per ulteriori informazioni, consulta Best practice for Deploying Amazon WorkSpaces (Scenario 6).

> **Note**
>
> L'AD Connector può essere configurato inviando un RFC Management | Other | Other | Create change type con i dettagli di configurazione AD prerequisiti; per ulteriori informazioni, consulta Creare un connettore AD. Se si utilizza il metodo 2 per creare una foresta di risorse in AD gestito da AMS, invia un altro RFC di Management | Other | Other | Create change type in AMS shared-services eseguendo l'AD gestito da AMS.

Utilizza AMS SSP per fornire i servizi AMS Code nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità dei servizi AMS Code direttamente nel tuo account gestito AMS. I servizi AMS Code sono un pacchetto proprietario di servizi di gestione del codice AWS, come descritto di seguito. Puoi scegliere di distribuire tutti i servizi di AMS con i servizi AMS Code oppure puoi distribuirli in AMS singolarmente.

I servizi AMS Code includono i seguenti servizi:

- AWS CodeCommit: un servizio di controllo del codice sorgente completamente gestito che ospita repository sicuri basati su Git. Consente ai team di collaborare sul codice in un ecosistema sicuro e altamente scalabile. CodeCommit elimina la necessità di utilizzare il proprio sistema di controllo del codice sorgente o di preoccuparsi di scalarne l'infrastruttura. CodeCommit può essere utilizzato per archiviare in modo sicuro qualunque elemento, dal codice sorgente ai binari, e funziona perfettamente con gli strumenti Git esistenti. Per ulteriori informazioni, consulta AWS CodeCommit

  Per implementarlo nel tuo account AMS indipendentemente dai servizi AMS Code, consulta. Utilizza AMS SSP per il provisioning AWS CodeCommit nel tuo account AMS

- AWS CodeBuild: Un servizio di integrazione continua completamente gestito che compila il codice sorgente, esegue test e produce pacchetti software pronti per l'implementazione. Con CodeBuild, non è necessario fornire, gestire e scalare i propri server di build. CodeBuild esegue la scalabilità continua ed elabora più build contemporaneamente, in modo che le build non restino in attesa in coda. Puoi iniziare a utilizzare CodeBuild velocemente con ambienti di compilazione predefiniti oppure puoi creare ambienti di compilazione personalizzati che utilizzano strumenti di compilazione specifici. Con CodeBuild, ti vengono addebitati al minuto per le risorse di calcolo che utilizzi. Per ulteriori informazioni, consulta AWS CodeBuild

  Per implementarlo nel tuo account AMS indipendentemente dai servizi AMS Code, consulta. Utilizza AMS SSP per il provisioning AWS CodeBuild nel tuo account AMS
- AWS CodeDeploy: un servizio di distribuzione completamente gestito che automatizza le distribuzioni di software su una varietà di servizi di elaborazione come Amazon EC2 e i server locali. AWS CodeDeploy ti aiuta a rilasciare rapidamente nuove funzionalità, ti aiuta a evitare i tempi di inattività durante la distribuzione delle applicazioni e gestisce la complessità dell'aggiornamento delle applicazioni. È possibile utilizzarlo AWS CodeDeploy per automatizzare le distribuzioni del software, eliminando la necessità di operazioni manuali soggette a errori. Il servizio è scalabile in base alle esigenze di implementazione. Per ulteriori informazioni, consulta AWS CodeDeploy

  Per implementarlo nel tuo account AMS indipendentemente dai servizi AMS Code, consulta. Utilizza AMS SSP per il provisioning AWS CodeDeploy nel tuo account AMS
- AWS CodePipeline: Un servizio di distribuzione continua completamente gestito che consente di automatizzare le pipeline di rilascio per aggiornamenti rapidi e affidabili di applicazioni e infrastrutture. CodePipeline automatizza le fasi di compilazione, test e distribuzione del processo di rilascio ogni volta che viene apportata una modifica al codice, in base al modello di rilascio definito dall'utente. Ciò consente di fornire funzionalità e aggiornamenti in modo rapido e affidabile. Puoi integrarti facilmente AWS CodePipeline con servizi di terze parti come GitHub o con il tuo plug-in personalizzato. Con AWS CodePipeline, paghi solo quello che usi. Non sono previste tariffe iniziali né impegni a lungo termine. Per ulteriori informazioni, consulta AWS CodePipeline

  Per implementarlo nel tuo account AMS indipendentemente dai servizi AMS Code, consultaUtilizza AMS SSP per il provisioning AWS CodePipeline nel tuo account AMS.

Domande frequenti sui servizi AMS Code in AWS Managed Services

D: Come posso richiedere l'accesso ai servizi AMS Code nel mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_code_suite_console_role` seguente ruolo IAM al tuo account:. Dopo aver effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa. A questo puntocustomer_codebuild_service_role, `customer_codedeploy_service_role` AMS Operations implementerà anche i ruoli di `aws_code_pipeline_service_role` servizio nell'account e nei servizi dell'utente CodeBuild. CodeDeploy CodePipeline Se sono necessarie autorizzazioni IAM aggiuntive per `customer_codebuild_service_role` i, invia una richiesta di servizio AMS.

> **Note**
>
> Puoi anche aggiungere questi servizi separatamente; per informazioni, consulta rispettivamente Utilizza AMS SSP per il provisioning AWS CodeBuild nel tuo account AMS Utilizza AMS SSP per il provisioning AWS CodeDeploy nel tuo account AMSUtilizza AMS SSP per il provisioning AWS CodePipeline nel tuo account AMS, e.

D: Quali sono le restrizioni all'utilizzo dei servizi AMS Code nel mio account AMS?

- AWS CodeCommit: La funzionalità di attivazione CodeCommit è disattivata in base ai diritti associati alla creazione di argomenti SNS. L'autenticazione diretta CodeCommit è limitata; gli utenti devono autenticarsi con Credential Helper. Anche alcuni comandi KMS sono soggetti a restrizioni: kms: Encrypt, Decrypt,,, e kms:. kms: ReEncrypt kms: GenereteDataKey kms: GenerateDataKeyWithoutPlaintext kms: DescribeKey
- CodeBuild: Per l'accesso da amministratore AWS CodeBuild della console, le autorizzazioni sono limitate a livello di risorsa; ad esempio, CloudWatch le azioni sono limitate a risorse specifiche e l'autorizzazione è controllata. `iam:PassRole`
- CodeDeploy: attualmente CodeDeploy supporta le distribuzioni solo su Amazon EC2/on-premise. Le distribuzioni su ECS e Lambda tramite non sono supportate. CodeDeploy
- CodePipeline: CodePipeline le funzionalità, le fasi e i provider sono limitati a quanto segue:
  - Fase di implementazione: Amazon S3 e AWS CodeDeploy
  - Fase di origine: Amazon S3 AWS CodeCommit, Bit Bucket e GitHub
  - Build Stage: AWS CodeBuild e Jenkins
  - Fase di approvazione: Amazon SNS

- Fase di test: AWS CodeBuild, Jenkins BlazeMeter, test dell'interfaccia utente di Ghost Inspector, Micro StormRunner Focus Load, monitoraggio dell'API Runscope
- Invoke Stage: Step Functions e Lambda

> **Note**
>
> AMS Operations lo distribuisce `customer_code_pipeline_lambda_policy` nel tuo account; deve essere associato al ruolo di esecuzione Lambda per la fase di invoca Lambda. Fornisci il nome del service/execution ruolo Lambda con cui desideri aggiungere questa policy. Se non esiste un service/execution ruolo Lambda personalizzato, AMS crea un nuovo ruolo denominato`customer_code_pipeline_lambda_execution_role`, ovvero una copia di `customer_lambda_basic_execution_role`. `customer_code_pipeline_lambda_policy`

D: Quali sono i prerequisiti o le dipendenze per utilizzare i servizi AMS Code nel mio account AMS?

- CodeCommit: Se i bucket S3 sono crittografati con AWS KMS chiavi, è necessario utilizzare S3. AWS KMS AWS CodeCommit
- CodeBuild: Se sono necessarie autorizzazioni IAM aggiuntive per il ruolo di AWS CodeBuild servizio definito, richiedile tramite una richiesta di servizio AMS.
- CodeDeploy: Nessuna.
- CodePipeline: Nessuno. AWS i servizi supportati—AWS CodeCommit AWS CodeBuild,, AWS CodeDeploy—devono essere lanciati prima o insieme al lancio di CodePipeline. Tuttavia, ciò viene eseguito da un tecnico AMS.

Utilizza AMS SSP per il provisioning AWS Amplify nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Amplify funzionalità direttamente nel tuo account gestito da AMS. AWS Amplify È una soluzione completa che consente agli sviluppatori web e mobili di frontend di creare, connettere e ospitare facilmente applicazioni fullstack. Amplify offre la flessibilità necessaria per sfruttare l'ampia gamma di servizi man mano che i casi d'uso si evolvono AWS . Amplify fornisce prodotti per creare app complete per iOS, Android, Flutter, Web e React Native. Per ulteriori informazioni, consulta AWS Amplify.

AWS Amplify nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere AWS Amplify di essere configurato nel mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_amplify_console_role` seguente ruolo IAM al tuo account:. Dopo aver effettuato il provisioning del tuo account, devi integrare il ruolo nella tua soluzione federativa.

Inoltre, è necessario fornire l'opzione Risk Acceptance, in quanto AWS Amplify dispone di autorizzazioni che modificano l'infrastruttura. A tale scopo, utilizza il Cloud Service Delivery Manager (CSDM).

D: Quali sono le restrizioni all'utilizzo AWS Amplify nel mio account AMS?

È necessario utilizzare `'amplify*'` come prefisso per i bucket quando si lavora con Amplify, a meno che RA e diversamente specificato.

D: Quali sono i prerequisiti o le dipendenze da utilizzare nel mio account AMS? AWS Amplify

Non ci sono prerequisiti per l'utilizzo di AWS Amplify nel tuo account AMS.

Solo ambienti Malz: il ruolo integrato predefinito per Amplify è «customer_amplify_console_role». Per utilizzare un ruolo personalizzato, distribuisci prima le entità IAM. Quindi, crea una RFC aggiuntiva per aggiungere il tuo ruolo personalizzato all'elenco consentito della Service Control Policy for Application Accounts.

Usa AMS SSP per il provisioning AWS AppSync

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS AppSync funzionalità direttamente nel tuo account gestito da AMS. AWS AppSync semplifica lo sviluppo di applicazioni consentendoti di creare un'API flessibile per accedere, manipolare e combinare in modo sicuro i dati provenienti da una o più fonti di dati. AWS AppSync è un servizio gestito che utilizza GraphQL per consentire alle applicazioni di ottenere con facilità esattamente i dati di cui hanno bisogno.

Con AWS AppSync, puoi creare applicazioni scalabili, comprese quelle che richiedono aggiornamenti in tempo reale, su una vasta gamma di fonti di dati come archivi dati NoSQL, database relazionali,

APIs HTTP e sorgenti dati personalizzate con. AWS Lambda Per le app mobili e web, offre AWS AppSync inoltre l'accesso locale ai dati quando i dispositivi vanno offline e la sincronizzazione dei dati con risoluzione dei conflitti personalizzabile, quando tornano online. Per ulteriori informazioni, consulta AWS AppSync.

AWS AppSync nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS AppSync al mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli IAM al tuo account: e. `customer_appsync_service_role` `customer_appsync_author_role` Una volta effettuato il provisioning nel tuo account, devi integrare la soluzione `customer_appsync_author_role` nella tua federazione.

D: Quali sono le restrizioni all'utilizzo di? AWS AppSync

- Quando si crea una fonte di dati, AppSync il cliente deve specificare il ruolo di servizio creato in precedenza, la creazione di un nuovo ruolo non è consentita e pertanto restituirà un accesso negato
- AppSync i ruoli sono configurati per limitare le autorizzazioni alle risorse contenenti i prefissi «AMS-» o «MC-» per impedire qualsiasi modifica all'infrastruttura AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare? AWS AppSync

Il servizio consente di utilizzare più altri servizi come origine dati. Le autorizzazioni di base per utilizzarli come tali sono incluse nel ruolo del servizio (`customer_appsync_service_role`), ma è necessario selezionare manualmente il ruolo del servizio quando si utilizza il servizio.

Utilizza AMS SSP per il provisioning AWS App Mesh nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS App Mesh funzionalità direttamente nel tuo account gestito da AMS. AWS App Mesh fornisce reti a livello di applicazione per facilitare la comunicazione tra i servizi attraverso diversi tipi di infrastruttura di elaborazione. App Mesh standardizza il modo in cui i tuoi servizi comunicano, offrendoti end-to-end visibilità e garantendo un'elevata disponibilità per le tue applicazioni.

AWS App Mesh semplifica l'esecuzione dei servizi fornendo visibilità e controlli coerenti del traffico di rete per i servizi creati su diversi tipi di infrastruttura di elaborazione. App Mesh elimina la necessità di aggiornare il codice dell'applicazione per modificare il modo in cui i dati di monitoraggio vengono raccolti o il traffico viene instradato tra i servizi. App Mesh configura ogni servizio per esportare i dati di monitoraggio e implementa una logica di controllo delle comunicazioni coerente in tutta l'applicazione. In questo modo è facile individuare rapidamente la posizione esatta degli errori e reindirizzare automaticamente il traffico di rete in caso di guasti o quando è necessario implementare modifiche al codice. Per ulteriori informazioni, consulta AWS App Mesh.

AWS App Mesh nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS App Mesh al mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce il seguente ruolo IAM al tuo account:. `customer_app_mesh_console_role` Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo di? AWS App Mesh

La funzionalità completa di AWS App Mesh è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze per l'utilizzo? AWS App Mesh

Non ci sono prerequisiti o dipendenze da utilizzare AWS App Mesh nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Audit Manager nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Audit Manager direttamente nel tuo account gestito AMS. Audit Manager ti aiuta a controllare continuamente l' AWS utilizzo per semplificare la valutazione del rischio e della conformità alle normative e agli standard di settore. Audit Manager automatizza la raccolta delle prove per semplificare la valutazione dell'efficacia delle policy, delle procedure e delle attività. Quando è il momento di un audit, Audit Manager ti aiuta a gestire le revisioni dei controlli da parte delle parti interessate e ti aiuta a creare report pronti per l'audit con uno sforzo manuale significativamente inferiore. Per ulteriori informazioni, consulta Audit Manager.

AWS Audit Manager nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS Audit Manager al mio account AMS?

Puoi richiedere l'accesso inviando il servizio AWS Services RFC Management | AWS | Self-provisioned service | Add (managed automation) (ct-3qe6io8t6jtny). Questa RFC fornisce `customer-audit-manager-admin-Role` il seguente ruolo IAM nel tuo account:. Dopo aver effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo? AWS Audit Manager

Non ci sono restrizioni per l'uso AWS Audit Manager nel tuo account AMS. AWS Audit Manager Viene fornita la funzionalità completa per.

D: Quali sono i prerequisiti o le dipendenze per l'utilizzo? AWS Audit Manager

1. Devi fornire ad AMS il bucket s3 in cui desideri risiedere. reports/assessments
2. Se desideri utilizzare il servizio di crittografia, devi fornire ad AMS l'ARN CMK KMS da utilizzare.
3. Se desideri inviare una notifica SNS a un argomento, devi fornire il nome dell'argomento o dell'arn.
4. (Facoltativo) Esiste un ulteriore prerequisito se desideri abilitare Organizations come parte della tua landing zone multi-account in Audit Manager e desideri un account amministratore delegato: nel campo della descrizione di RFC (Management | AWS service | Compatible Service| Aggiungi), indica che desideri utilizzare l'account amministratore delegato come parte dell'installazione di Audit Manager e fornisci i seguenti dettagli:
   - KMS CMK ARN (utilizzato inizialmente per configurare Audit Manager)
   - ID dell'account amministratore delegato per Audit Manager da utilizzare come parte di questa landing zone con più account (può essere un account dell'applicazione MALZ)

Utilizza AMS SSP per il provisioning AWS Batch nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Batch funzionalità direttamente nel tuo account gestito da AMS. AWS Batch consente a sviluppatori, scienziati e ingegneri di eseguire in modo semplice ed efficiente centinaia di migliaia di lavori di elaborazione in batch. AWS AWS Batch fornisce dinamicamente la quantità e il tipo ottimali di risorse di elaborazione (ad esempio istanze ottimizzate per CPU o memoria) in base al volume e ai requisiti di risorse

specifici dei processi batch inviati. In questo modo non è necessario installare e gestire il software di elaborazione in batch o i cluster di server utilizzati per eseguire i processi, il che consente di concentrarsi sull'analisi dei risultati e sulla risoluzione dei problemi. AWS Batch Per ulteriori informazioni, consulta AWS Batch.

AWS Batch nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS Batch al mio account AMS?

1. Per richiedere l'accesso a AWS Batch, invia il servizio RFC Management | AWS | Self-provisioned service | Add (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli e politiche IAM nel tuo account:

Ruoli IAM:

- `customer_batch_console_role`
- `customer_batch_ecs_instance_role`
- `customer_batch_events_service_role`
- `customer_batch_service_role`
- `customer_batch_ecs_task_role`

Policy:

- `customer_batch_console_role_policy`
- `customer_batch_service_role_policy`
- `customer_batch_events_service_role_policy`

2. Dopo aver effettuato il provisioning nel tuo account, devi inserire il ruolo `customer_batch_console_role` nella tua soluzione di federazione.

D: Quali sono le restrizioni all'utilizzo? AWS Batch

Quando crei l'ambiente di calcolo, devi etichettare EC2 le istanze come «customer_batch» o «customer-batch». Se le istanze non sono contrassegnate, le istanze non verranno terminate in batch al termine del processo.

D: Quali sono i prerequisiti o le dipendenze da utilizzare? AWS Batch

Non ci sono prerequisiti o dipendenze da utilizzare AWS Batch nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Certificate Manager nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità AWS Certificate Manager (ACM) direttamente nel tuo account gestito AMS. AWS Certificate Manager è un servizio che consente di fornire, gestire e distribuire certificati Secure Layer/Transport Sockets Layer Security (SSL/TLS) pubblici e privati da utilizzare con i servizi e le risorse interne connesse. AWS SSL/TLS i certificati vengono utilizzati per proteggere le comunicazioni di rete e stabilire l'identità dei siti Web su Internet e delle risorse su reti private. AWS Certificate Manager rimuove il lungo processo manuale di acquisto, caricamento e rinnovo SSL/TLS dei certificati.

Con AWS Certificate Manager, puoi richiedere un certificato, distribuirlo su AWS risorse integrate con ACM, come Elastic Load Balancers, distribuzioni CloudFront Amazon e su APIs API Gateway, e lasciare che gestisca i rinnovi dei certificati. AWS Certificate Manager Consente inoltre di creare certificati privati per le risorse interne e gestire il ciclo di vita dei certificati in modo centralizzato. I certificati pubblici e privati forniti AWS Certificate Manager per l'utilizzo con i servizi integrati ACM sono gratuiti. Paghi solo per le AWS risorse che crei per eseguire l'applicazione. Con AWS Autorità di certificazione privata, paghi mensilmente per il funzionamento dei CA privata AWS e per i certificati privati che emetti. Per ulteriori informazioni, consulta AWS Certificate Manager - AWS Documentazione.

Domande frequenti su ACM in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS Certificate Manager al mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce il seguente ruolo IAM al tuo account:. `customer_acm_create_role` Puoi utilizzare questo ruolo per creare e gestire certificati ACM. Dopo averlo inserito nel tuo account, devi inserire il ruolo nella tua soluzione federativa.

I certificati ACM possono essere creati utilizzando i seguenti tipi di modifica, anche se non hai aggiunto il `customer_acm_create_role` ruolo IAM:

- ACM | Crea certificato pubblico

- ACM | Crea certificato privato
- Certificato ACM con ulteriore | Crea SANs

D: Quali sono le restrizioni all'utilizzo di AWS Certificate Manager?

È necessario inviare una Request for Change (RFC) ad AMS per eliminare o modificare i certificati esistenti, poiché tali azioni richiedono l'accesso amministrativo completo (utilizzate il tipo Management | Advanced stack components | ACM | Delete certificate change (ct-1q8q56cmwqj9m)). Tieni presente che la policy IAM non può escludere i diritti in base ai nomi dei tag (mc*, ams*, ecc.). I certificati non comportano costi, quindi l'eliminazione dei certificati non utilizzati non è urgente.

D: Quali sono i prerequisiti o le dipendenze per l'utilizzo di Certificate Manager?

Nome DNS pubblico esistente e accesso per creare record DNS CNAME, ma non è necessario che siano ospitati nell'account gestito.

Utilizza AMS SSP per il provisioning AWS Autorità di certificazione privata nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Autorità di certificazione privata funzionalità direttamente nel tuo account gestito da AMS. I certificati privati vengono utilizzati per identificare e proteggere le comunicazioni tra risorse connesse su reti private, come server, dispositivi mobili e applicazioni IoT. CA privata AWS è un servizio CA privato gestito che consente di gestire in modo semplice e sicuro il ciclo di vita dei certificati privati. CA privata AWS offre un servizio CA privato ad alta disponibilità senza gli investimenti iniziali e i costi di manutenzione continui legati alla gestione di una CA privata. CA privata AWS estende le funzionalità di gestione dei certificati di ACM ai certificati privati, consentendoti di creare e gestire certificati pubblici e privati in modo centralizzato. Puoi creare e distribuire facilmente certificati privati per AWS le tue risorse utilizzando la console di AWS gestione o l'API ACM. Per le istanze EC2, i contenitori, i dispositivi IoT e le risorse locali, puoi creare e tracciare facilmente certificati privati e utilizzare il tuo codice di automazione lato client per distribuirli. Hai anche la flessibilità di creare certificati privati e gestirli autonomamente per applicazioni che richiedono durate dei certificati, algoritmi chiave o nomi di risorse personalizzati. Per ulteriori informazioni, consulta. CA privata AWS

CA privata AWS nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso CA privata AWS al mio account AMS?

Richiedi l'accesso tramite l'invio dei AWS Servizi RFC (Gestione | AWS servizio | Servizio compatibile). Tramite questa RFC, nel tuo account verrà assegnato il seguente ruolo IAM:. `customer_acm_pca_role` Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo di? CA privata AWS

Attualmente, AWS Resource Access Manager (AWS RAM) non può essere utilizzato per condividere più CA privata AWS account.

D: Quali sono i prerequisiti o le dipendenze per l'utilizzo? CA privata AWS

1. Se intendi creare un CRL, hai bisogno di un bucket S3 in cui archiviarlo. CA privata AWS deposita automaticamente il CRL nel bucket Amazon S3 designato e lo aggiorna periodicamente. È necessario che il bucket S3 disponga della seguente policy relativa ai bucket prima di poter configurare un CRL. Per procedere con questa richiesta, crea un RFC con ct-0fpjlxa808sh2 (Gestione | Advanced stack components | S3 storage | Update policy) come segue:

- Fornisci il nome o l'ARN del bucket S3.
- Copia la seguente policy su RFC e sostituiscila `bucket-name` con il nome del bucket S3 desiderato.

JSON

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Effect":"Allow",
         "Principal":{
            "Service":"acm-pca.amazonaws.com"
         },
         "Action":[
            "s3:PutObject",
            "s3:PutObjectAcl",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation"
         ],
         "Resource":[
```

```
            "arn:aws:s3:::bucket-name/*",
            "arn:aws:s3:::bucket-name"
         ]
      }
   ]
}
```

2. Se il bucket S3 di cui sopra è crittografato, il Service Principal acm-pca.amazonaws.com richiede le autorizzazioni per la decrittografia. Per procedere con questa richiesta, crea un RFC con ct-3ovo7px2vsa6n (Gestione | Advanced stack components | KMS key | Update) come segue:

- Fornisci l'ARN della chiave KMS su cui deve essere aggiornata la policy.
- Copia la politica seguente su RFC e sostituiscila `bucket-name` con il nome del bucket S3 desiderato.

```
{
   "Sid":"Allow ACM-PCA use of the key",
   "Effect":"Allow",
   "Principal":{
      "Service":"acm-pca.amazonaws.com"
   },
   "Action":[
      "kms:GenerateDataKey",
      "kms:Decrypt"
   ],
   "Resource":"*",
   "Condition":{
      "StringLike":{
         "kms:EncryptionContext:aws:s3:arn":[
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key",
            "arn:aws:s3:::bucket_name/acm-pca-permission-test-key-private",
            "arn:aws:s3:::bucket_name/audit-report/*",
            "arn:aws:s3:::bucket_name/crl/*"
         ]
      }
   }
}
```

3. CA privata AWS CRLs non supportano l'impostazione S3 «Blocca l'accesso pubblico a bucket e oggetti concesso tramite nuove liste di controllo degli accessi (ACLs)». È necessario disabilitare

questa impostazione con l'account e il bucket S3 per consentire la CA privata AWS scrittura CRLs come indicato in Come creare e archiviare in modo sicuro il CRL per ACM Private CA Se desideri disabilitarlo, crea un nuovo RFC con ct-0xdawir96cy7k (Gestione | Altro | Altro | Aggiornamento) e allega un'accettazione del rischio. Se hai domande sull'accettazione del rischio, contatta il tuo Cloud Architect.

Utilizza AMS SSP per il provisioning AWS CloudEndure nel tuo account AMS

> **Note**
>
> Dopo il successo del lancio di AWS Application Migration Service, il servizio di CloudEndure migrazione è ora giunto alla fine del ciclo di vita in tutte le AWS regioni. Consigliamo ai clienti di utilizzarlo AWS Application Migration Service per le migrazioni lift-and-shift verso le GovCloud Regioni e le Regioni commerciali. Per informazioni, consulta What Is? AWS Application Migration Service.
> Se desideri utilizzarli AWS Application Migration Service, contatta il tuo CA in modo che possano guidarti.

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS CloudEndure funzionalità direttamente nel tuo account gestito da AMS. AWS CloudEndure la migrazione semplifica, accelera e automatizza le migrazioni su larga scala da infrastrutture fisiche, virtuali e basate su cloud a. AWS CloudEndure Il Disaster Recovery (DR) protegge dai tempi di inattività e dalla perdita di dati da qualsiasi minaccia, inclusi ransomware e danneggiamento dei server.

AWS CloudEndure nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso CloudEndure al mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_cloud_endure_user` seguente utente IAM al tuo account:. Dopo aver effettuato il provisioning nel tuo account, la chiave di accesso e la chiave segreta dell'utente vengono condivise in AWS Secrets Manager.

Queste politiche vengono fornite anche all'account: `customer_cloud_endure_policy` e. `customer_cloud_endure_deny_policy`

Inoltre, è necessario fornire una Risk Acceptance poiché la soluzione CloudEndure DR per l'integrazione delle applicazioni dispone di autorizzazioni che modificano l'infrastruttura. A tale scopo, collabora con il tuo cloud service delivery manager (CSDM).

D: Quali sono le restrizioni all'utilizzo CloudEndure nel mio account AMS?

Le istanze di replica e conversione endure su cloud possono essere avviate solo nella sottorete indicata.

D: Quali sono i prerequisiti o le dipendenze da utilizzare nel mio account AMS? CloudEndure Condividi quanto segue tramite corrispondenza bidirezionale RFC:

- Dettagli della sottorete VPC per le istanze di replica e conversione da avviare.
- La chiave KMS Amazon Resource Name (ARN) se i volumi EBS sono crittografati.

Utilizza AMS SSP per il provisioning AWS CloudHSM nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS CloudHSM funzionalità direttamente nel tuo account gestito da AMS. AWS CloudHSM ti aiuta a soddisfare i requisiti di conformità aziendali, contrattuali e normativi per la sicurezza dei dati utilizzando istanze Hardware Security Module (HSM) dedicate all'interno del cloud. AWS AWS, e i partner di AWS Marketplace offrono una varietà di soluzioni per proteggere i dati sensibili all'interno della AWS piattaforma, ma per alcune applicazioni e dati soggetti a mandati contrattuali o normativi per la gestione delle chiavi crittografiche, potrebbe essere necessaria una protezione aggiuntiva. AWS CloudHSM integra le soluzioni di protezione dei dati esistenti e consente di proteggere le chiavi di crittografia all'interno HSMs di esse progettate e convalidate secondo gli standard governativi per una gestione sicura delle chiavi. AWS CloudHSM consente di generare, archiviare e gestire in modo sicuro le chiavi crittografiche utilizzate per la crittografia dei dati in modo che le chiavi siano accessibili solo all'utente. Per ulteriori informazioni, consulta AWS CloudHSM.

AWS CloudHSM nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS CloudHSM al mio account AMS?

L'utilizzo di nel tuo account AMS è un processo in due fasi:

1. Richiedi un AWS CloudHSM cluster. A tale scopo, invia una RFC con il tipo di modifica Management | Other | Other | Create (ct-1e1xtak34nx76). Includi i seguenti dettagli:

- AWS Regione.
- ID/ARN. Provide a VPC ID/VPCARN VPC che si trova nello stesso account della RFC inviata.
- Specificare almeno due zone di disponibilità per il cluster.
- ID dell' EC2 istanza Amazon che si connetterà al cluster HSM.

2. Accedi alla AWS CloudHSM console. A tale scopo, invia una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Questa RFC fornisce il `customer_cloudhsm_console_role` seguente ruolo IAM al tuo account:.

Dopo aver assegnato il ruolo nel tuo account, devi inserirlo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo AWS CloudHSM nel mio account AMS?

L'accesso alla AWS CloudHSM console non ti offre la possibilità di creare, terminare o ripristinare il cluster. Per eseguire queste operazioni, invia un tipo di modifica Management | Other | Other | Create change type (ct-1e1xtak34nx76).

D: Quali sono i prerequisiti o le dipendenze da utilizzare nel mio account AMS? AWS CloudHSM

È necessario consentire il traffico TCP utilizzando la porta 2225 tramite un' EC2 istanza Amazon client all'interno di un VPC oppure utilizzare Direct Connect VPN per server locali che desiderano accedere al cluster HSM. AWS CloudHSM dipende da Amazon EC2 per i gruppi di sicurezza e le interfacce di rete. Per il monitoraggio o il controllo dei log, HSM si affida a CloudTrail (operazioni AWS API) e CloudWatch Logs per tutte le attività dei dispositivi HSM locali.

D: Chi applicherà gli aggiornamenti al AWS CloudHSM client e alle relative librerie software?

L'utente è responsabile dell'applicazione degli aggiornamenti della libreria e del client. Ti consigliamo di monitorare la pagina della cronologia delle versioni di CloudHSM per le versioni e quindi applicare gli aggiornamenti utilizzando l'aggiornamento del client CloudHSM.

> **Note**
>
> Le patch software per l'appliance HSM vengono sempre applicate automaticamente dal servizio. AWS CloudHSM

Utilizza AMS SSP per il provisioning AWS CodeBuild nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS CodeBuild funzionalità direttamente nel tuo account gestito da AMS. AWS CodeBuild è un servizio di integrazione continua completamente gestito che compila il codice sorgente, esegue test e produce pacchetti software pronti per l'implementazione. Con CodeBuild, non è necessario fornire, gestire e scalare i propri server di build. CodeBuild esegue la scalabilità continua ed elabora più build contemporaneamente, in modo che le build non restino in attesa in coda. Puoi iniziare a utilizzare CodeBuild velocemente con ambienti di compilazione predefiniti oppure puoi creare ambienti di compilazione personalizzati che utilizzano strumenti di compilazione specifici. Con CodeBuild, ti vengono addebitati al minuto per le risorse di calcolo che utilizzi. Per ulteriori informazioni, consulta AWS CodeBuild.

> **Note**
>
> Per effettuare l'onboarding CodeCommit, CodeBuild CodeDeploy, e CodePipeline con un'unica RFC, invia il tipo di modifica Management | AWS service | Self-provisioned service | Add (managed automation) (ct-3qe6io8t6jtny) e richiedi i tre servizi:, e. CodeBuild CodeDeploy CodePipeline Quindi, tutti e tre i ruoli,, e vengono assegnati nel tuo account. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Dopo aver effettuato il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione federativa.

CodeBuild nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS CodeBuild al mio account AMS?

L'utilizzo di AWS CodeBuild nel tuo account AMS è un processo in due fasi:

1. Predisponi il processo `CodeBuild Service Role` di compilazione in modo che si coordini con i bucket AWS S3, i gruppi Amazon CloudWatch e Log
2. Richiedi l'accesso alla console CodeBuild

Puoi richiedere che entrambi siano configurati nel tuo account AMS inviando una RFC al Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Dopo averlo inserito nel tuo account, devi inserire il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo AWS CodeBuild nel mio account AMS?

Per quanto riguarda l'accesso da amministratore della AWS CodeBuild console, le autorizzazioni sono limitate a livello di risorsa; ad esempio, CloudWatch le azioni sono limitate a risorse specifiche e l'`iam:PassRole`autorizzazione è controllata.

D: Quali sono i prerequisiti o le dipendenze da utilizzare CodeBuild nel mio account AMS?

Se sono necessarie autorizzazioni IAM aggiuntive per il ruolo di AWS CodeBuild servizio definito, richiedile tramite una richiesta di servizio AMS.

Utilizza AMS SSP per il provisioning AWS CodeCommit nel tuo account AMS

> **Note**
>
> AWS ha chiuso l'accesso a nuovi clienti AWS CodeCommit, a partire dal 25 luglio 2024. AWS CodeCommit i clienti esistenti possono continuare a utilizzare il servizio normalmente. AWS continua a investire in sicurezza, disponibilità e miglioramenti delle prestazioni per AWS CodeCommit, ma non abbiamo intenzione di introdurre nuove funzionalità.
> Per migrare i CodeCommit repository AWS Git verso altri provider Git, contatta il tuo architetto cloud (CA) per ricevere assistenza. Per ulteriori informazioni sulla migrazione dei tuoi repository Git, consulta Come migrare il tuo CodeCommit repository AWS verso un altro provider Git.

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS CodeCommit funzionalità direttamente nel tuo account gestito da AMS. AWS CodeCommit è un servizio di controllo del codice sorgente completamente gestito che ospita repository sicuri basati su Git. Aiuta i team a collaborare sul codice in un ecosistema sicuro e altamente scalabile. CodeCommit elimina la necessità di utilizzare il proprio sistema di controllo del codice sorgente o di preoccuparsi di scalarne l'infrastruttura. Puoi usarlo CodeCommit per archiviare in modo sicuro qualsiasi cosa, dal codice sorgente ai file binari, e funziona perfettamente con gli strumenti Git esistenti. Per ulteriori informazioni, consulta AWS CodeCommit.

> **Note**
>
> Per effettuare l'onboard CodeCommit, CodeBuild CodeDeploy, e CodePipeline con una singola RFC, invia il tipo di modifica Management | AWS service | Self-provisioned service | Add (managed automation) (ct-3qe6io8t6jtny) e richiedi i tre servizi:, e. CodeBuild CodeDeploy CodePipeline Quindi, tutti e tre i ruoli,, e vengono assegnati nel tuo account. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Dopo aver effettuato il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione federativa.

CodeCommit nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso CodeCommit al mio account AMS?

AWS CodeCommit i ruoli di console e accesso ai dati possono essere richiesti inviando due AWS Service RFCs, accesso alla console e accesso ai dati:

- Richiedi l'accesso AWS CodeCommit inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC `customer_codecommit_console_role` fornisce il seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

  L'accesso ai dati (come gli elenchi di formazione e di entità) richiede una distinzione CTs per ogni fonte di dati, specificando l'origine dati S3 (obbligatoria), il bucket di output (obbligatorio) e il KMS (opzionale). Non ci sono limitazioni alla creazione di AWS CodeCommit posti di lavoro purché a tutte le fonti di dati siano stati concessi ruoli di accesso. Per richiedere l'accesso ai dati, invia una RFC a Management | Other | Other | Create (ct-1e1xtak34nx76).

D: Quali sono le restrizioni all'utilizzo nel mio account AMS? AWS CodeCommit

La funzionalità Trigger attiva è disattivata in base CodeCommit ai diritti associati alla creazione di argomenti SNS. L'autenticazione diretta CodeCommit è limitata, gli utenti devono autenticarsi con Credential Helper. Alcuni comandi KMS sono inoltre soggetti a restrizioni:`kms:Encrypt`,,,, e`kms:Decrypt`. `kms:ReEncrypt` `kms:GenereteDataKey` `kms:GenerateDataKeyWithoutPlaintext` `kms:DescribeKey`

D: Quali sono i prerequisiti o le dipendenze da utilizzare AWS CodeCommit nel mio account AMS?

Se i bucket S3 sono crittografati con chiavi KMS, è necessario utilizzare S3 e KMS. AWS CodeCommit

Utilizza AMS SSP per il provisioning AWS CodeDeploy nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS CodeDeploy funzionalità direttamente nel tuo account gestito da AMS. AWS CodeDeploy è un servizio di distribuzione completamente gestito che automatizza le distribuzioni di software su una varietà di servizi di elaborazione come Amazon EC2 e i server locali AWS Fargate. AWS Lambda AWS CodeDeploy ti aiuta a rilasciare rapidamente nuove funzionalità, ti aiuta a evitare i tempi di inattività durante la distribuzione delle applicazioni e gestisce la complessità dell'aggiornamento delle applicazioni. È possibile utilizzarlo AWS CodeDeploy per automatizzare le distribuzioni del software, eliminando la necessità di operazioni manuali soggette a errori. Il servizio è scalabile in base alle esigenze di implementazione. Per ulteriori informazioni, consulta AWS CodeDeploy.

> **Note**
>
> Per effettuare l'onboard e CodePipeline con una singola RFC CodeCommit CodeBuild CodeDeploy, invia il tipo di modifica Management | AWS service | Self-provisioned service | Add (managed automation) (ct-3qe6io8t6jtny) e richiedi i tre servizi:, e. CodeBuild CodeDeploy CodePipeline Quindi, tutti e tre i ruoli,, e vengono assegnati nel tuo account. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Dopo aver effettuato il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione federativa.

CodeDeploy nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso CodeDeploy al mio account AMS?

Richiedi l'accesso CodeDeploy inviando una RFC con il servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli IAM al tuo account: e. `customer_codedeploy_console_role` `customer_codedeploy_service_role` Dopo aver effettuato il provisioning nel tuo account, devi inserire il `customer_codedeploy_console_role` ruolo nella tua soluzione di federazione.

D: Quali sono le restrizioni all'utilizzo CodeDeploy nel mio account AMS?

Al momento supportiamo solo Compute Platform come: Amazon EC2/on-premise. Blue/Green Le distribuzioni non sono supportate.

D: Quali sono i prerequisiti o le dipendenze da utilizzare CodeDeploy nel mio account AMS?

Non ci sono prerequisiti o dipendenze da utilizzare CodeDeploy nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS CodePipeline nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS CodePipeline funzionalità direttamente nel tuo account gestito da AMS. AWS CodePipeline è un servizio di distribuzione continua completamente gestito che consente di automatizzare le pipeline di rilascio per aggiornamenti rapidi e affidabili di applicazioni e infrastrutture. CodePipeline automatizza le fasi di compilazione, test e distribuzione del processo di rilascio ogni volta che viene apportata una modifica al codice, in base al modello di rilascio definito dall'utente. Ciò consente di fornire funzionalità e aggiornamenti in modo rapido e affidabile. Puoi integrarti facilmente AWS CodePipeline con servizi di terze parti come GitHub o con il tuo plug-in personalizzato. Con AWS CodePipeline, paghi solo per quello che usi. Non sono previste tariffe iniziali né impegni a lungo termine. Per ulteriori informazioni, consulta AWS CodePipeline.

> **Note**
>
> Per effettuare l'onboard CodeCommit, CodeBuild CodeDeploy, e CodePipeline con un'unica RFC, invia il tipo di modifica del tipo Management | AWS service | Self-provisioned service | Add (managed automation) (ct-3qe6io8t6jtny) e richiedi i tre servizi:, e. CodeBuild CodeDeploy CodePipeline Quindi, tutti e tre i ruoli,, e vengono assegnati nel tuo account. `customer_codebuild_service_role` `customer_codedeploy_service_role` `aws_code_pipeline_service_role` Dopo aver effettuato il provisioning nel tuo account, devi inserire il ruolo nella tua soluzione federativa.
> CodePipeline in AMS non supporta «Amazon CloudWatch Events» per Source Stage perché necessita di autorizzazioni elevate per creare il ruolo e la policy del servizio, che aggira il modello dei privilegi minimi e il processo di gestione delle modifiche AMS.

CodePipeline nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso CodePipeline al mio account AMS?

Richiedi l'accesso CodePipeline inviando una richiesta di servizio `customer_code_pipeline_console_role` nell'account pertinente. Dopo averlo inserito nel tuo account, devi inserire il ruolo nella tua soluzione federativa.

Al momento, AMS Operations implementerà anche questo ruolo di servizio nel tuo account:. `aws_code_pipeline_service_role_policy`

D: Quali sono le restrizioni all'utilizzo CodePipeline nel mio account AMS?

Sì. CodePipeline le funzionalità, gli stage e i provider sono limitati a quanto segue:

1. Fase di distribuzione: limitata ad Amazon S3 e AWS CodeDeploy
2. Source Stage: limitato ad Amazon S3, AWS CodeCommit, e BitBucket GitHub
3. Build Stage: Limitato a AWS CodeBuild, e Jenkins
4. Fase di approvazione: limitata ad Amazon SNS
5. Fase di test: limitata ai AWS CodeBuild test dell'interfaccia utente di Jenkins BlazeMeter, Ghost Inspector, Micro StormRunner Focus Load e Runscope API Monitoring
6. Invoke Stage: limitato a Step Functions e Lambda

> **Note**
>
> AMS Operations verrà implementato `customer_code_pipeline_lambda_policy` nel tuo account; deve essere associato al ruolo di esecuzione Lambda per la fase di invoca Lambda. Fornisci il nome del service/execution ruolo Lambda con cui desideri aggiungere questa policy. Se non esiste un service/execution ruolo Lambda personalizzato, AMS creerà un nuovo ruolo denominato`customer_code_pipeline_lambda_execution_role`, che sarà una copia di`customer_lambda_basic_execution_role`. `customer_code_pipeline_lambda_policy`

D: Quali sono i prerequisiti o le dipendenze da utilizzare CodePipeline nel mio account AMS?

AWS i servizi AWS CodeCommit supportati AWS CodeDeploy devono essere lanciati prima o insieme al lancio di. AWS CodeBuild CodePipeline

Utilizza AMS SSP per il provisioning AWS Compute Optimizer nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Compute Optimizer funzionalità direttamente nel tuo account gestito da AMS. AWS Compute Optimizer consiglia risorse di AWS calcolo ottimali per i carichi di lavoro per ridurre i costi e migliorare le prestazioni utilizzando l'apprendimento automatico per analizzare le metriche di utilizzo cronologiche. L'over-provisioning dell'elaborazione (Amazon EC2 e ASG) può comportare costi di infrastruttura non necessari, mentre un calcolo insufficiente può portare a prestazioni delle applicazioni scadenti. Compute Optimizer ti aiuta a scegliere i tipi di istanze Amazon EC2 ottimali, incluse quelle che fanno parte di un gruppo Amazon EC2 Auto Scaling, in base ai tuoi dati di utilizzo. Per ulteriori informazioni, consulta AWS Compute Optimizer.

Domande frequenti su Compute Optimizer in AWS Managed Services

D: Come posso richiedere l'accesso a Compute Optimizer nel mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_compute_optimizer_readonly_role` seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo di Compute Optimizer nel mio account AMS?

Non ci sono restrizioni. La funzionalità completa di AWS Compute Optimizer è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Compute Optimizer nel mio account AMS?

- È necessario inviare un RFC (Management | Other | Other | Update) che autorizzi AMS Ops ad abilitare il servizio nell'account. Durante l'implementazione, viene creato un ruolo collegato al servizio (SLR) per consentire la raccolta delle metriche e la generazione di report. La reflex è etichettata "». AWSService RoleForComputeOptimizer Per ulteriori informazioni, vedere Utilizzo dei ruoli collegati ai servizi per AWS Compute Optimizer
- CloudWatch le metriche devono essere abilitate per le seguenti metriche:
  - Utilizzo della CPU: la percentuale di unità di calcolo Amazon EC2 allocate in uso sull'istanza. Questa metrica identifica la potenza di elaborazione richiesta per eseguire un'applicazione su un'istanza selezionata.

- Utilizzo della memoria: la quantità di memoria che è stata utilizzata in qualche modo durante il periodo di campionamento. Questa metrica identifica la memoria richiesta per eseguire un'applicazione su un'istanza selezionata. L'utilizzo della memoria viene analizzato solo per le risorse su cui è installato l'agente CloudWatch unificato. Per ulteriori informazioni, vedere Enabling Memory Utilization with the CloudWatch Agent (p. 10).
- Rete in ingresso: il numero di byte ricevuti su tutte le interfacce di rete dall'istanza. Questa metrica identifica il volume del traffico di rete in entrata su una singola istanza.
- Rete in uscita: il numero di byte inviati su tutte le interfacce di rete dall'istanza. Questa metrica identifica il volume del traffico di rete in uscita da una singola istanza.
- Disco locale input/output (I/O): il numero di operazioni per il disco locale. input/output Questa metrica identifica le prestazioni del volume principale di un'istanza

Utilizza AMS SSP per il provisioning AWS DataSync nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS DataSync funzionalità direttamente nel tuo account gestito da AMS. AWS DataSync sposta grandi quantità di dati online tra lo storage locale e Amazon S3, Amazon Elastic File System (Amazon Elastic File System) o Amazon. FSx Le attività manuali relative ai trasferimenti di dati possono rallentare le migrazioni e appesantire le operazioni IT. DataSync elimina o gestisce automaticamente molte di queste attività, tra cui la creazione di copie di script, la pianificazione e il monitoraggio dei trasferimenti, la convalida dei dati e l'ottimizzazione dell'utilizzo della rete. L'agente DataSync software si connette allo storage Network File System (NFS) e Server Message Block (SMB), in modo da non dover modificare le applicazioni. DataSync può trasferire centinaia di terabyte e milioni di file a velocità fino a 10 volte superiori rispetto agli strumenti open source, tramite Internet o collegamenti. AWS Direct Connect Puoi utilizzarli DataSync per migrare set o archivi di dati attivi AWS, trasferire dati sul cloud per analisi ed elaborazione tempestive o replicare i dati per la continuità aziendale. AWS

Per ulteriori informazioni, consulta AWS DataSync.

DataSync nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso DataSync al mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_datasync_console_role` seguente ruolo IAM al tuo account:.

Dopo aver effettuato il provisioning nel tuo account, devi integrare i ruoli nella tua soluzione federativa.

Il gruppo di CloudWatch log da utilizzare per lo streaming dei log delle attività è «/aws/datasync».

D: Quali sono le restrizioni all'utilizzo nel mio account AMS? DataSync

La funzionalità completa di AWS DataSync è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare DataSync nel mio account AMS?

- Amazon S3 (ARNs Amazon Resource Names) sono necessari per tutti i bucket S3 associati alle DataSync attività che verranno eseguite utilizzando il ruolo di servizio. DataSync `customer_datasync_service_role`
- Gli endpoint VPC e i gruppi di sicurezza per DataSync gli agenti devono essere richiesti con una RFC con il tipo di modifica Management | Other | Other | Create (ct-1e1xtak34nx76) prima di utilizzare gli endpoint VPC.
- AWS DataSync gli agenti vengono eseguiti in AMS come appliance. L' AWS DataSync agente viene patchato e aggiornato dal servizio; per i dettagli, consulta AWS DataSync le domande frequenti.
- Per avviare un AWS DataSync agente, invia una RFC con il tipo di modifica Management | Other | Other | Create (ct-1e1xtak34nx76), richiedendo l'implementazione dell'agente. Fornisci l'ID AMI AWS DataSync Amazon EC2, il tipo di istanza, la sottorete, il gruppo di sicurezza e fai riferimento a una coppia di chiavi Amazon EC2 esistente o richiedi la creazione di una nuova coppia di chiavi.

> **Note**
>
> AMS fornisce l' AWS DataSync agente manualmente per conto del cliente e non richiede il processo di inserimento di WIGS sull'AMI Amazon EC2 AWS DataSync .

Utilizza AMS SSP per il provisioning AWS Device Farm nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Device Farm funzionalità direttamente nel tuo account gestito AMS. AWS Device Farm è un servizio di test delle applicazioni che consente di migliorare la qualità delle app Web e mobili testandole su un'ampia gamma di browser desktop e dispositivi mobili reali, senza dover fornire e gestire alcuna infrastruttura

di test. Il servizio consente di eseguire i test contemporaneamente su più browser desktop o dispositivi reali per accelerare l'esecuzione della suite di test e genera video e registri per aiutarti a identificare rapidamente i problemi con la tua app.

Per ulteriori informazioni, consulta AWS Device Farm.

AWS Device Farm nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso AWS Device Farm al mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_devicefarm_role` seguente ruolo IAM al tuo account:.

Una volta effettuato il provisioning nel tuo account, devi integrare i ruoli nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo AWS Device Farm nel mio account AMS?

L'accesso completo al AWS Device Farm servizio è fornito ad eccezione dell'utilizzo dello spazio dei nomi AMS nel tag 'Name'.

D: Quali sono i prerequisiti o le dipendenze da utilizzare AWS Device Farm nel mio account AMS?

Nessuna.

Utilizza AMS SSP per il provisioning Ripristino di emergenza di elastico di AWS nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle Ripristino di emergenza di elastico di AWS funzionalità direttamente nel tuo account gestito AMS. Ripristino di emergenza di elastico di AWS riduce al minimo i tempi di inattività e la perdita di dati con un ripristino rapido e affidabile delle applicazioni locali e basate sul cloud utilizzando storage a prezzi accessibili, elaborazione e ripristino minimi. point-in-time È possibile aumentare la resilienza IT quando si utilizzano applicazioni locali o basate sul Ripristino di emergenza di elastico di AWS cloud in esecuzione su sistemi operativi supportati. Utilizzalo Console di gestione AWS per configurare le impostazioni di replica e avvio, monitorare la replica dei dati e avviare istanze per esercitazioni o ripristino.

Per ulteriori informazioni, consulta Ripristino di emergenza di elastico di AWS.

Ripristino di emergenza di elastico di AWS nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso Ripristino di emergenza di elastico di AWS al mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_drs_console_role` seguente ruolo IAM al tuo account:.

Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo Ripristino di emergenza di elastico di AWS nel mio account AMS?

Non ci sono restrizioni d'uso Ripristino di emergenza di elastico di AWS nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare Ripristino di emergenza di elastico di AWS nel mio account AMS?

- Dopo aver avuto accesso al ruolo della console, devi inizializzare il servizio Elastic Disaster Recovery per creare i ruoli IAM necessari all'interno dell'account.
  - È necessario inviare il tipo di modifica Management | Applications | IAM instance profile | Create (managed automation) change type ct-0ixp4ch2tiu04 RFC per creare un clone del profilo dell'istanza e allegare la policy. `customer-mc-ec2-instance-profile` `AWSElasticDisasterRecoveryEc2InstancePolicy` È necessario specificare a quali macchine collegare la nuova policy.
  - Se l'istanza non utilizza il profilo di istanza predefinito, AMS può collegarsi `AWSElasticDisasterRecoveryEc2InstancePolicy` tramite automazione.
- È necessario utilizzare una chiave KMS di proprietà del cliente per il ripristino tra più account. La chiave KMS dell'account di origine deve essere aggiornata seguendo la politica per consentire l'accesso all'account di destinazione. Per ulteriori informazioni, consulta Condividere la chiave di crittografia EBS con l'account di destinazione.
- La politica della chiave KMS deve essere aggiornata `customer_drs_console_role` per consentire la visualizzazione della politica se non desideri cambiare ruolo da visualizzare.
- Per il disaster recovery tra più account e più regioni, AMS deve configurare l'account di origine e quello di destinazione come Trusted Account e utilizzare i ruoli di failback e di adattamento.AWS CloudFormation

Utilizza AMS SSP per il provisioning AWS Elemental MediaConvert nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Elemental MediaConvert funzionalità direttamente nel tuo account gestito da AMS. AWS Elemental MediaConvert è un servizio di transcodifica video basato su file con funzionalità di livello broadcast. Consente di creare contenuti video-on-demand (VOD) per la trasmissione e la distribuzione multischermo su larga scala. Il servizio combina funzionalità video e audio avanzate con una semplice interfaccia di servizi web e prezzi. pay-as-you-go Con AWS Elemental MediaConvert, puoi concentrarti sulla fornitura di esperienze multimediali coinvolgenti senza doverti preoccupare della complessità della creazione e della gestione della tua infrastruttura di elaborazione video.

Per ulteriori informazioni, consulta AWS Elemental MediaConvert.

MediaConvert nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso MediaConvert al mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_mediaconvert_author_role` seguente ruolo IAM al tuo account:. Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

Verrà fornito un secondo ruolo`customer_MediaConvert_Default_Role`, utilizzato da per leggere dal bucket S3 di origine e scrivere l'output MediaConvert nel bucket S3 di destinazione, nonché per richiamare il gateway API nel caso in cui sia necessaria la gestione dei diritti digitali (DRM).

D: Quali sono le restrizioni all'utilizzo nel mio account AMS? MediaConvert

Non ci sono restrizioni per l'uso di MediaConvert in AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare MediaConvert nel mio account AMS?

Non ci sono prerequisiti o dipendenze da utilizzare MediaConvert nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Elemental MediaLive nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Elemental MediaLive funzionalità direttamente nel tuo account gestito da AMS. AWS Elemental MediaLive è

un servizio di elaborazione video in diretta di livello broadcast. Consente di creare flussi video di alta qualità da distribuire a televisori di trasmissione e dispositivi multischermo connessi a Internet, come tablet, smartphone e set-top box connessi a Internet. TVs Il servizio funziona codificando i flussi video in diretta in tempo reale, prendendo una sorgente video live di dimensioni maggiori e comprimendola in versioni più piccole per la distribuzione ai tuoi spettatori. Con AWS Elemental MediaLive, puoi configurare facilmente streaming sia per eventi dal vivo che per canali 24 ore su 24, 7 giorni su 7, con funzionalità di trasmissione avanzate, alta disponibilità e prezzi. pay-as-you-go AWS Elemental MediaLive ti consente di concentrarti sulla creazione di esperienze video dal vivo coinvolgenti per i tuoi spettatori senza la complessità della creazione e del funzionamento di un'infrastruttura di elaborazione video di livello broadcast.

Per ulteriori informazioni, consulta AWS Elemental MediaLive.

MediaLive nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso MediaLive al mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_medialive_author_role` seguente ruolo IAM al tuo account:.

Come parte di questa RFC, viene distribuito un secondo ruolo nel tuo account; `customer_medialive_service_role` ruolo, questo ruolo può essere assegnato ai tuoi canali e input Media Live per interagire con altri servizi come Amazon S3 e Logs. MediaStore CloudWatch

Dopo aver assegnato i ruoli nel tuo account, devi incorporarli nella tua soluzione di federazione.

D: Quali sono le restrizioni all'utilizzo MediaLive nel mio account AMS?

Non ci sono restrizioni per l'uso di MediaLive in AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare MediaLive nel mio account AMS?

Non ci sono prerequisiti o dipendenze da utilizzare MediaLive nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Elemental MediaPackage nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Elemental MediaPackage funzionalità direttamente nel tuo account gestito da AMS. AWS Elemental MediaPackage prepara e protegge in modo affidabile i tuoi video per la distribuzione su Internet.

Da un singolo ingresso video, AWS Elemental MediaPackage crea flussi video formattati per la riproduzione su telefoni cellulari TVs, computer, tablet e console di gioco connessi. Semplifica l'implementazione di funzionalità video popolari per gli spettatori (riavvio, pausa, riavvolgimento e così via), come quelle comunemente disponibili su. DVRs AWS Elemental MediaPackage può anche proteggere i tuoi contenuti utilizzando Digital Rights Management (DRM). AWS Elemental MediaPackage si ridimensiona automaticamente in risposta al caricamento, in modo che i tuoi spettatori possano sempre vivere un'esperienza eccezionale senza che tu debba prevedere con precisione in anticipo la capacità di cui avrai bisogno.

Per ulteriori informazioni, consulta AWS Elemental MediaPackage.

MediaPackage nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso AWS Elemental MediaPackage al mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_mediapackage_author_role` seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

Verrà fornito un secondo ruolo`customer_mediapackage_service_role`, che può essere assegnato ai canali e agli input di Media Live per interagire con altri servizi come S3 e Secrets Manager.

D: Quali sono le restrizioni all'utilizzo MediaPackage nel mio account AMS?

Non ci sono restrizioni per l'uso di MediaPackage in AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare MediaPackage nel mio account AMS?

Non ci sono prerequisiti o dipendenze da utilizzare MediaPackage nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Elemental MediaStore nel tuo account AMS

> **Note**
>
> Dopo un'attenta valutazione, AWS ha preso la decisione di sospendere la produzione MediaStore, a decorrere dal 13 novembre 2025. Se sei un cliente attivo di MediaStore, puoi MediaStore utilizzarlo normalmente fino al 13 novembre 2025, quando il supporto per il

servizio terminerà. Dopo questa data, non sarai più in grado di utilizzare MediaStore nessuna delle funzionalità fornite da questo servizio.

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Elemental MediaStore funzionalità direttamente nel tuo account gestito da AMS. AWS Elemental MediaStore è un servizio di AWS archiviazione ottimizzato per i media. Offre le prestazioni, la coerenza e la bassa latenza necessarie per fornire contenuti video in streaming live. AWS Elemental MediaStore funge da archivio di origine nel flusso di lavoro video. Le sue funzionalità ad alte prestazioni soddisfano le esigenze dei carichi di lavoro di media delivery più impegnativi, combinate con uno storage a lungo termine a costi contenuti. Per ulteriori informazioni, consulta AWS Elemental MediaStore.

MediaStore nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso MediaStore al mio account AMS?

Richiedi l'accesso MediaStore inviando una RFC con il servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce `customer_mediastore_author_role` il seguente ruolo IAM al tuo account:. Come parte di questa RFC, nel tuo account viene distribuito un secondo ruolo; `MediaStoreAccessLogs` ruolo, che viene utilizzato dal MediaStore servizio per registrare le attività CloudWatch, se scegli di abilitare quella funzionalità. Dopo averlo inserito nel tuo account, devi inserire i ruoli nella tua soluzione federativa.

Al momento, AMS Operations implementerà anche questo ruolo di servizio nel tuo account:. `aws_code_pipeline_service_role_policy`

D: Quali sono le restrizioni all'utilizzo MediaStore nel mio account AMS?

Non ci sono restrizioni per l'uso di MediaStore in AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare MediaStore nel mio account AMS?

Non ci sono prerequisiti o dipendenze da utilizzare MediaStore nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Elemental MediaTailor nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Elemental MediaTailor funzionalità direttamente nel tuo account gestito da AMS. AWS Elemental MediaTailor

consente ai provider di video di inserire pubblicità mirata individualmente nei propri stream video senza sacrificare il livello di trasmissione. quality-of-service Inoltre AWS Elemental MediaTailor, gli spettatori dei tuoi video in diretta o su richiesta ricevono ciascuno uno streaming che combina i tuoi contenuti con annunci personalizzati per loro. Ma a differenza di altre soluzioni pubblicitarie personalizzate, AWS Elemental MediaTailor l'intero stream (video e annunci) viene fornito con una qualità video di livello broadcast per migliorare l'esperienza degli spettatori. AWS Elemental MediaTailor offre report automatizzati basati su metriche di distribuzione degli annunci sul lato client e sul lato server, per misurare con precisione le impressioni pubblicitarie e il comportamento degli spettatori. Puoi monetizzare facilmente eventi di visualizzazione imprevisti ad alta richiesta senza costi iniziali utilizzando. AWS Elemental MediaTailor Inoltre, migliora i tassi di pubblicazione degli annunci, aiutandoti a guadagnare di più da ogni video, e funziona con una più ampia varietà di reti di distribuzione dei contenuti, server di decisione pubblicitaria e dispositivi client.

Per ulteriori informazioni, consulta AWS Elemental MediaTailor.

MediaTailor nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso MediaTailor al mio account AMS?

Richiedi l'accesso MediaTailor inviando una RFC con il servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce `customer-mediatailor-role` il seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo MediaTailor nel mio account AMS?

Non ci sono restrizioni per l'uso di MediaTailor in AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare MediaTailor nel mio account AMS?

Non ci sono prerequisiti o dipendenze da utilizzare MediaTailor nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Global Accelerator nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Global Accelerator direttamente nel tuo account gestito da AMS. Global Accelerator è un servizio a livello di rete in cui si creano acceleratori per migliorare la disponibilità e le prestazioni delle applicazioni Internet utilizzate da un pubblico globale. Per ulteriori informazioni, consulta Global Accelerator.

Domande frequenti su Global Accelerator in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere la configurazione di Global Accelerator nel mio account AMS?

Richiedi l'accesso inviando il Service RFC (Management | AWS service | Self-provisioned Service). AWS Tramite questa RFC, nel tuo account verranno assegnati i seguenti ruoli IAM:. `customer_global_accelerator_console_role` Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo di console nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo di Global Accelerator nel mio account AMS?

Global Accelerator è un servizio globale che supporta gli endpoint in più AWS regioni, elencati nella tabella delle AWS regioni.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Global Accelerator nel mio account AMS?

Quando configuri l'acceleratore con Global Accelerator, associ gli indirizzi IP statici agli endpoint regionali in una o più regioni. AWS Per gli acceleratori standard, gli endpoint sono Network Load Balancer, Application Load Balancer, EC2 istanze Amazon o indirizzi IP elastici. Per gli acceleratori di routing personalizzati, gli endpoint sono sottoreti di cloud privato virtuale (VPC) con una o più istanze. EC2

Utilizza AMS SSP per il provisioning AWS Glue nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Glue funzionalità direttamente nel tuo account gestito da AMS. AWS Glue è un servizio di estrazione, trasformazione e caricamento (ETL) completamente gestito che ti aiuta a preparare e caricare i dati per l'analisi. È possibile creare ed eseguire un processo ETL con pochi clic nel. Console di gestione AWS Indicate i dati memorizzati su AWS, li AWS Glue scoprite e memorizzate i metadati associati (ad esempio la definizione e lo schema della tabella) in. AWS Glue AWS Glue Data Catalog Una volta catalogati, i dati sono immediatamente ricercabili, interrogabili e disponibili per le azioni ETL. Per ulteriori informazioni, consulta AWS Glue.

AWS Glue nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere AWS Glue di essere configurato nel mio account AMS?

Richiedi l'accesso AWS Glue inviando una RFC con il servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli IAM al tuo account:

- `customer_glue_console_role`
- `customer_glue_service_role`

I ruoli precedenti includono le seguenti politiche allegate:

- `customer_glue_secrets_manager_policy`
- `customer_glue_deny_policy`

Dopo aver assegnato i ruoli nel tuo account, devi inserirli nella tua soluzione federativa.

Per accedere a Crawler, Jobs ed endpoint di sviluppo (ruoli necessari per casi d'uso specifici), invia una RFC con Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entity or policy (ct-3dpd8mdd9jn1r).

D: AWS Glue Quali sono le restrizioni all'utilizzo nel mio account AMS?

Non ci sono restrizioni. La funzionalità completa di AWS Glue è disponibile nel tuo account AMS. Per un ambiente interattivo in cui è possibile creare e testare script ETL, utilizza Notebooks on Studio. AWS Glue AWS Glue Le sessioni interattive e i Job Notebooks sono funzionalità serverless AWS Glue che è possibile utilizzare AWS Glue e che sfruttano il ruolo di servizio. AWS Glue

AWS Glue precedenti alla 2.0: AWS Glue i notebook sono una risorsa non gestita che avvia istanze Amazon EC2 in un account. È consigliabile avviare le proprie EC2 istanze Amazon e installare il software necessario per supportare l'ambiente e lo sviluppo di un notebook. Per ulteriori informazioni, consulta Tutorial: Configurazione di un notebook Apache Zeppelin locale per testare ed eseguire il debug degli script ETL e utilizzo degli endpoint di sviluppo per lo sviluppo di script.

D: Quali sono i prerequisiti o le dipendenze da utilizzare nel mio account AMS? AWS Glue

AWS Glue dipende da Amazon S3 CloudWatch e Logs. CloudWatch Le dipendenze transitive variano in base alle fonti di dati e possono interagire con altre funzionalità del AWS Glue servizio (ad esempio: Amazon Redshift, Amazon RDS, Athena).

Utilizza AMS SSP per il provisioning AWS Lake Formation nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Lake Formation funzionalità direttamente nel tuo account gestito da AMS. AWS Lake Formation è un servizio che semplifica la configurazione di un data lake sicuro in pochi giorni. Un data lake è un repository centralizzato, curato e sicuro che archivia tutti i dati, sia nella loro forma originale che preparati per l'analisi. Un data lake consente di suddividere i silos di dati e combinare diversi tipi di analisi per ottenere informazioni dettagliate e prendere così migliori decisioni aziendali.

La creazione di un data lake con Lake Formation è semplice quanto la definizione delle origini dati e delle policy di sicurezza e accesso ai dati da applicare. Lake Formation consente di raccogliere e catalogare i dati dai database e dall'archiviazione di oggetti, spostare i dati nel nuovo data lake Amazon S3, pulire e classificare i dati utilizzando algoritmi di machine learning e proteggere l'accesso ai dati sensibili. I tuoi utenti possono accedere a un catalogo di dati centralizzato (per i dettagli, consulta le AWS Glue domande frequenti) che descrive i set di dati disponibili e il loro utilizzo appropriato. I tuoi utenti sfruttano quindi questi set di dati con la loro scelta di servizi di analisi e apprendimento automatico, come Amazon Redshift, Amazon Athena e (in versione beta) Amazon EMR per Apache Spark. Lake Formation si basa sulle funzionalità disponibili in AWS Glue.

Per ulteriori informazioni, consulta AWS Lake Formation.

Domande frequenti su Lake Formation in AWS Managed Services

D: Come posso richiedere l'accesso AWS Lake Formation al mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce il `customer_lakeformation_data_analyst_role` seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare i ruoli nella tua soluzione federativa.

Inoltre, i due ruoli seguenti sono opzionali:

- `customer_lakeformation_admin_role`
- `customer_lakeformation_workflow_role`

Per `customer_lakeformation_admin_role` quanto riguarda le autorizzazioni di amministratore, puoi scegliere di inserire il ruolo nell'ambito dello stesso tipo di modifica SSPS (ct-3qe6io8t6jtny).

Se desideri creare blueprint nella AWS Lake Formation console, devi inviare un tipo di modifica Management | AWS service | Self-provisioned service | Add (managed automation) (ct-3qe6io8t6jtny) e aggiungerlo esplicitamente per distribuire il. `customer_lakeformation_workflow_role` Nella RFC, devi fornire il nome del bucket S3 se il bucket è una fonte al momento della creazione dei Blueprint. Il bucket S3 è applicabile se il tipo di Blueprint è Classic Load Balancer AWS CloudTrail Logs o Application Load Balancer Logs.

D: Quali sono le restrizioni all'utilizzo nel mio account AMS? AWS Lake Formation

Tutte le funzionalità di Lake Formation sono disponibili in AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare AWS Lake Formation nel mio account AMS?

Lake Formation si integra con il AWS Glue servizio, pertanto AWS Glue gli utenti possono accedere solo ai database e alle tabelle su cui dispongono delle autorizzazioni Lake Formation. Inoltre, gli utenti di AWS Athena e Amazon Redshift possono eseguire query solo sui database e sulle tabelle su cui dispongono AWS Glue delle autorizzazioni Lake Formation.

Utilizza AMS SSP per il provisioning AWS Lambda nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Lambda funzionalità direttamente nel tuo account gestito da AMS. AWS Lambda consente di eseguire il codice senza effettuare il provisioning o la gestione dei server. Paghi solo per il tempo di elaborazione che utilizzi, non ci sono costi quando il codice non è in esecuzione. Con Lambda, puoi eseguire codice praticamente per qualsiasi tipo di applicazione o servizio di back-end, il tutto senza alcuna amministrazione. Carica il codice e Lambda si occuperà di tutto il necessario per eseguire e scalare il codice con un'elevata disponibilità. Puoi configurare il codice in modo che venga attivato automaticamente da altri AWS servizi o chiamarlo direttamente da qualsiasi app Web o mobile. Per ulteriori informazioni, consulta AWS Lambda.

Domande frequenti su Lambda in AWS Managed Services

D: Come posso richiedere l'accesso AWS Lambda al mio account AMS?

Richiedi l'accesso inviando un tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (automazione gestita) (ct-3qe6io8t6jtny). Questa RFC fornisce i seguenti `customer_lambda_admin_role` ruoli IAM al tuo account: e. `customer_lambda_basic_execution_role` Dopo averlo inserito nel tuo account, devi inserire i ruoli nella tua soluzione di federazione.

D: Quali sono le restrizioni all'utilizzo AWS Lambda nel mio account AMS?

- Una funzione Lambda è progettata per essere richiamata dalle sorgenti di eventi. Per un elenco di servizi che possono essere utilizzati come origine di eventi Lambda, consulta Utilizzo AWS Lambda con altri servizi. Al momento non tutti questi servizi sono disponibili negli account AMS. Se hai bisogno di un servizio che non è disponibile, collabora con il tuo CSDM AMS per presentare un'eccezione.
- Per impostazione predefinita, AMS fornisce un ruolo di iniziazione Lambda di base contenente i `AWSXrayWriteOnlyAccess` permessi `AWSLambdaBasicExecutionRole` e; per informazioni, vedere Ruolo di iniziazione.AWS Lambda Se hai bisogno di autorizzazioni aggiuntive, come la possibilità di fornire funzioni Lambda all'interno del tuo VPC AMS, invia una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Add (managed automation) (ct-3qe6io8t6jtny).

D: Quali sono AWS Lambda i prerequisiti o le dipendenze da utilizzare nel mio account AMS?

Non ci sono prerequisiti o dipendenze con cui iniziare AWS Lambda; tuttavia, a seconda del caso d'uso specifico, potresti aver bisogno dell'accesso ad altri AWS servizi per creare fonti di eventi o autorizzazioni aggiuntive per consentire alla funzione di eseguire varie azioni. Se sono necessarie autorizzazioni aggiuntive, invia una RFC al servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (automazione gestita) (ct-3qe6io8t6jtny).

D: Cosa devo fare per eseguire una funzione Lambda in uno dei miei account?

Per implementare una funzione Lambda in un account principale, utilizza le seguenti linee guida:

- Assicurati che SSPS for sia integrato. AWS Lambda
- Non esistono restrizioni specifiche che vietino questa implementazione nell'ambito delle responsabilità di AMS, purché le risorse AMS siano protette e conformi.
- Se desideri che AMS crei la funzione Lambda, devi prima utilizzare il ruolo SSPS previsto. AWS Lambda Quindi, se desideri comunque l'assistenza di AMS per implementare o supportare la funzione, contatta la tua CA e avvia il processo out of scope (OOS).

Utilizza AMS SSP per il provisioning AWS License Manager nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS License Manager funzionalità direttamente nel tuo account gestito da AMS. AWS License Manager si integra con AWS i servizi per semplificare la gestione delle licenze su più AWS account, cataloghi IT e locali, tramite

un unico account. AWS AWS License Manager consente agli amministratori di creare regole di licenza personalizzate che emulano i termini dei loro contratti di licenza e quindi applica queste regole quando viene lanciata un'istanza di Amazon. EC2 Le regole AWS License Manager consentono di limitare una violazione della licenza bloccando fisicamente l'avvio dell'istanza o notificando agli amministratori la violazione. Per ulteriori informazioni, consulta AWS License Manager.

Domande frequenti su License Manager in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere AWS License Manager di essere configurato nel mio account AMS?

Richiedi l'accesso AWS License Manager inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC `customer_license_manager_role` fornisce il seguente ruolo IAM al tuo account:. Una volta assegnato il ruolo IAM di License Manager nel tuo account, devi inserire il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo AWS License Manager nel mio account AMS?

Puoi associare AWS License Manager le regole alle tue (AMIs filtrate nella sezione «Di mia proprietà»). Se scegli di imporre un'associazione limite a un'AMI (esempio: può supportare solo 100 vCPU di questa AMI) e esaurisci il limite, i lanci futuri con quell'AMI vengono bloccati e restituisce un errore che indica «Nessuna licenza disponibile». Questo è il comportamento previsto da questo servizio (non consente l'esaurimento della licenza). Nel caso in cui si esaurisca il limite ma sia necessario avviare nuovamente l'AMI, è necessario modificare la regola configurata in. AWS License Manager

D: Quali sono i prerequisiti o le dipendenze da utilizzare AWS License Manager nel mio account AMS?

Non ci sono prerequisiti o dipendenze da utilizzare AWS License Manager nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Migration Hub nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Migration Hub funzionalità direttamente nel tuo account gestito da AMS. AWS Migration Hub fornisce un'unica posizione in cui è possibile monitorare l'avanzamento delle migrazioni delle applicazioni tra più AWS soluzioni e partner. L'utilizzo di Migration Hub ti consente di scegliere gli strumenti di migrazione AWS

e i partner più adatti alle tue esigenze, fornendo al contempo visibilità sullo stato delle migrazioni in tutto il tuo portafoglio di applicazioni. Migration Hub fornisce anche metriche chiave e progressi per le singole applicazioni, indipendentemente dagli strumenti utilizzati per la migrazione. Ciò consente di ottenere rapidamente aggiornamenti sullo stato di avanzamento di tutte le migrazioni, identificare e risolvere facilmente eventuali problemi e ridurre il tempo e l'impegno complessivi spesi per i progetti di migrazione. Per ulteriori informazioni, consulta AWS Migration Hub.

Domande frequenti su Migration Hub in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso a Migration Hub nel mio account AMS?

Richiedi l'accesso a Migration Hub inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC fornisce `customer_migrationhub_author_role` il seguente ruolo IAM al tuo account:. Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni per Migration Hub?

Nessuna.

D: Quali sono i prerequisiti per abilitare Migration Hub?

Non ci sono prerequisiti per iniziare a utilizzare Migration Hub nel tuo account AMS. Tuttavia, durante la gestione del servizio potrebbero essere necessarie autorizzazioni esterne a Migration Hub, ad esempio autorizzazioni di scrittura su Amazon S3 per caricare informazioni sul server.

Utilizza AMS SSP per il provisioning AWS Outposts nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Outposts funzionalità direttamente nel tuo account gestito da AMS. AWS Outposts è un servizio completamente gestito che estende l' AWS infrastruttura APIs, AWS i servizi e gli strumenti praticamente a qualsiasi data center, spazio di co-location o struttura locale per un'esperienza ibrida coerente. AWS Outposts è utile per carichi di lavoro che richiedono un accesso a bassa latenza ai sistemi locali, all'elaborazione locale dei dati o all'archiviazione locale dei dati. Per ulteriori informazioni, consulta AWS Outposts.

AWS Outposts nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere AWS Outposts di essere configurato nel mio account AMS?

Richiedi l'accesso AWS Outposts inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC `customer_outposts_role` fornisce il seguente ruolo IAM al tuo account:. Una volta assegnato il ruolo nel tuo account, devi inserirlo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo AWS Outposts nel mio account AMS?

Non ci sono restrizioni per l'uso AWS Outposts nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare AWS Outposts nel mio account AMS?

Non ci sono prerequisiti o dipendenze da utilizzare AWS Outposts nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Resilience Hub nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Resilience Hub funzionalità direttamente nel tuo account gestito da AMS. AWS Resilience Hub ti aiuta a preparare e proteggere in modo proattivo le tue AWS applicazioni dalle interruzioni. Resilience Hub offre valutazioni e convalide della resilienza che si integrano nel ciclo di vita dello sviluppo del software per scoprire i punti deboli della resilienza. Resilience Hub consente di stimare se le applicazioni sono in grado di soddisfare o meno gli obiettivi RTO (Recovery Time Objective) e RPO (Recovery Point Objective) e aiuta a risolvere i problemi prima che vengano rilasciati in produzione. Dopo aver distribuito un' AWS applicazione in produzione, puoi utilizzare Resilience Hub per continuare a monitorare lo stato di resilienza dell'applicazione. In caso di interruzione, Resilience Hub invia una notifica all'operatore per avviare il processo di ripristino associato.

AWS Resilience Hub nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS Resilience Hub al mio account AMS?

Richiedi l'accesso a Resilience Hub inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli e politiche IAM al tuo account:

Ruoli IAM

- `customer_resiliencehub_console_role`

- `customer_resiliencehub_service_role`

Policy

- `customer_resiliencehub_console_policy`
- `customer_resiliencehub_service_policy`

Dopo aver assegnato il ruolo nel tuo account, devi integrarlo `customer_resiliencehub_console_role` nella tua soluzione di federazione.

D: Quali sono le restrizioni all'utilizzo AWS Resilience Hub nel mio account AMS?

Non ci sono restrizioni. La funzionalità completa di Resilience Hub è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare AWS Resilience Hub nel mio account AMS?

Non ci sono prerequisiti o dipendenze per utilizzare Resilience Hub nel tuo account AMS.

Utilizza AMS SSP per il provisioning Gestione dei segreti AWS nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle Gestione dei segreti AWS funzionalità direttamente nel tuo account gestito da AMS. Gestione dei segreti AWS ti aiuta a proteggere i segreti necessari per accedere alle tue applicazioni, servizi e risorse IT. Il servizio consente di ruotare, gestire e recuperare facilmente le credenziali del database, le chiavi API e altri segreti durante il loro ciclo di vita. Gli utenti e le applicazioni recuperano i segreti con una chiamata al Secrets Manager APIs, eliminando la necessità di codificare le informazioni sensibili in testo normale. Secrets Manager offre una rotazione segreta con integrazione integrata per Amazon RDS, Amazon Redshift e Amazon DocumentDB. Inoltre, il servizio è estensibile ad altri tipi di segreti, tra cui chiavi e token API. OAuth Per ulteriori informazioni, consulta Gestione dei segreti AWS.

> **Note**
>
> Per impostazione predefinita, gli operatori AMS possono accedere ai Gestione dei segreti AWS segreti crittografati utilizzando la AWS KMS chiave predefinita dell'account (CMK). Se desideri che i tuoi segreti siano inaccessibili ad AMS Operations, utilizza una CMK personalizzata, con una policy chiave AWS Key Management Service (AWS KMS) che definisce le autorizzazioni appropriate ai dati archiviati nel segreto.

Domande frequenti su Secrets Manager in AWS Managed Services

D: Come posso richiedere l'accesso Gestione dei segreti AWS al mio account AMS?

Richiedi l'accesso a Secrets Manager inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (ct-3qe6io8t6jtny). Questa RFC fornisce i `customer-rotate-secrets-lambda-role` seguenti `customer_secrets_manager_console_role` ruoli IAM al tuo account: e. `customer_secrets_manager_console_role`Viene utilizzato come ruolo di amministratore per fornire e gestire i segreti e `customer-rotate-secrets-lambda-role` viene utilizzato come ruolo di esecuzione Lambda per le funzioni Lambda che ruotano i segreti. Dopo averlo inserito nel tuo account, devi inserire il `customer_secrets_manager_console_role` ruolo nella tua soluzione di federazione.

D: Quali sono le restrizioni all'utilizzo Gestione dei segreti AWS nel mio account AMS?

La funzionalità completa di Gestione dei segreti AWS è disponibile nel tuo account AMS, insieme alla funzionalità di rotazione automatica dei segreti. Tuttavia, tieni presente che l'impostazione della rotazione utilizzando «Crea una nuova funzione Lambda per eseguire la rotazione» non è supportata perché richiede autorizzazioni elevate per creare lo CloudFormation stack (creazione di ruoli IAM e funzioni Lambda), che ignora il processo di gestione delle modifiche. AMS Advanced supporta solo «Usa una funzione Lambda esistente per eseguire la rotazione», in cui gestisci le funzioni Lambda per ruotare i segreti utilizzando il ruolo di amministratore Lambda SSPS. AWS AMS Advanced non crea o gestisce Lambda per ruotare i segreti.

D: Quali sono i prerequisiti o le dipendenze da utilizzare Gestione dei segreti AWS nel mio account AMS?

I seguenti namespace sono riservati all'uso da parte di AMS e non sono disponibili come parte dell'accesso diretto a: Gestione dei segreti AWS

- arn:aws:secretsmanager: *:*:secret:ams-shared/*
- arn:aws:secretsmanager: *:*:secret:customer-shared/*
- arn:aws:gestore dei segreti: *:*:secret:ams/*

Condivisione delle chiavi tramite Secrets Manager (AMS SSPS)

La condivisione di segreti con AMS nel testo semplice di una RFC, di una richiesta di assistenza o di un rapporto sull'incidente genera un incidente di divulgazione delle informazioni e AMS elimina tali informazioni dal caso e richiede la rigenerazione delle chiavi.

È possibile utilizzare Gestione dei segreti AWS(Secrets Manager) in questo spazio dei nomi,. `customer-shared`

Domande frequenti sulla condivisione delle chiavi con Secrets Manager

D: Quali tipi di segreti devono essere condivisi utilizzando Secrets Manager?

Alcuni esempi sono le chiavi precondivise per la creazione di VPN, le chiavi riservate come le chiavi di autenticazione (IAM, SSH), le chiavi di licenza e le password.

D: Come posso condividere le chiavi con AMS utilizzando Secrets Manager?

1. Accedi alla console di AWS gestione utilizzando l'accesso federato e il ruolo appropriato:

   per SALZ, il `Customer_ReadOnly_Role`

   per MALZ,. `AWSManagedServicesChangeManagementRole`
2. Vai alla Gestione dei segreti AWS console e fai clic su Memorizza un nuovo segreto.
3. Seleziona Altro tipo di segreti.
4. Inserisci il valore segreto come testo semplice e utilizza la crittografia KMS predefinita. Fare clic su Avanti.
5. Inserisci il nome e la descrizione segreti, il nome inizia sempre con customer-shared/. Ad esempio customer-shared/mykey2022. Fare clic su Avanti.
6. Lascia disattivata la rotazione automatica, fai clic su Avanti.
7. Controlla e fai clic su Store per salvare il segreto.
8. Rispondi a noi con il nome segreto tramite la richiesta di servizio, la RFC o il rapporto sull'incidente, in modo che possiamo identificare e recuperare il segreto.

D: Quali autorizzazioni sono necessarie per condividere le chiavi utilizzando Secrets Manager?

SALZ: Cerca la policy IAM `customer_secrets_manager_shared_policy` gestita e verifica che il documento relativo alla policy sia lo stesso allegato nella procedura di creazione riportata di seguito. Conferma che la policy sia allegata ai seguenti ruoli IAM:`Customer_ReadOnly_Role`.

MALZ: verifica che`AMSSecretsManagerSharedPolicy`, sia associato al `AWSManagedServicesChangeManagementRole` ruolo che consente l'`GetSecretValue`azione nel namespace. `ams-shared`

Esempio:

```
{
 "Action": "secretsmanager:*",
 "Resource": [
 "arn:aws:secretsmanager:*:*:secret:ams-shared/*",
 "arn:aws:secretsmanager:*:*:secret:customer-shared/*"
 ],
 "Effect": "Allow",
 "Sid": "AllowAccessToSharedNameSpaces"
 }
```

> **Note**
>
> Le autorizzazioni necessarie vengono concesse quando si aggiunge Gestione dei segreti AWS un servizio fornito in modalità self-service.

Utilizza AMS SSP per il provisioning AWS Security Hub CSPM nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Security Hub CSPM funzionalità direttamente nel tuo account gestito da AMS. AWS Security Hub CSPM vi offre una visione completa dello stato di sicurezza interno AWS e della vostra conformità agli standard e alle best practice del settore della sicurezza. Security Hub CSPM centralizza e dà priorità ai risultati di sicurezza e conformità provenienti da AWS account, servizi e partner terzi supportati per aiutarti ad analizzare le tendenze in materia di sicurezza e identificare i problemi di sicurezza con la massima priorità. Per ulteriori informazioni, consulta AWS Security Hub CSPM.

Domande frequenti su Security Hub CSPM in AWS Managed Services

D: Come posso richiedere l'accesso al AWS Security Hub CSPM mio account AMS?

Richiedi l'accesso a Security Hub CSPM inviando una RFC con il servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce `customer_securityhub_role` il seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo di Security Hub CSPM nel mio account AMS?

La funzionalità di archiviazione è stata considerata un potenziale rischio operativo e di sicurezza ed è stata limitata nell'ambito del ruolo Security del servizio fornito autonomamente.

D: Quali sono i prerequisiti o le dipendenze da utilizzare AWS Security Hub CSPM nel mio account AMS?

Non ci sono prerequisiti o dipendenze da utilizzare AWS Security Hub CSPM nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Service Catalog AppRegistry nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AppRegistry funzionalità direttamente nel tuo account gestito da AMS. AppRegistry consente la ricerca, il reporting e le azioni di gestione delle applicazioni da una posizione centrale. I costruttori raramente creano applicazioni in un unico AWS account. In genere separano le risorse delle applicazioni in base alle fasi del ciclo di vita, come sviluppo, test e produzione. AppRegistry consente di raggruppare e visualizzare tutte le raccolte di risorse tra gli AWS account definiti dall'utente.

Con AppRegistry, è possibile archiviare AWS le applicazioni, la raccolta di risorse associate alle applicazioni e i gruppi di attributi delle applicazioni. Per ulteriori informazioni, consulta Cos'è AppRegistry.

Domande frequenti: AWS Service Catalog AppRegistry in AMS

D: Come posso richiedere l'accesso AWS Service Catalog AppRegistry al mio account AMS?

Richiedi l'accesso AppRegistry inviando una RFC con Management | AWS service | Self-provisioned service | Add (managed automation) (ct-3qe6io8t6jtny) di modifica. Questa RFC `customer-appregistry-console-role` fornisce il seguente ruolo IAM al tuo account:. Dopo aver effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo AWS Service Catalog AppRegistry nel mio account AMS?

L'accesso completo al AppRegistry servizio è fornito ad eccezione dell'utilizzo dello spazio dei nomi AMS nel `'Name'` tag.

D: Quali sono i prerequisiti o le dipendenze da utilizzare AWS Service Catalog AppRegistry nel mio account AMS?

Non ci sono prerequisiti o dipendenze da utilizzare AppRegistry nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Shield Advanced nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Shield Advanced funzionalità direttamente nel tuo account gestito da AMS. AWS Shield Advanced è un servizio gestito di protezione Distributed Denial of Service (DDoS) che protegge le applicazioni in esecuzione su. AWS Shield Advanced offre un rilevamento sempre attivo e mitigazioni automatiche in linea che riducono al minimo i tempi di inattività e la latenza delle applicazioni, quindi non è necessario coinvolgere l'assistenza AWS per beneficiare della protezione S. DDo Esistono due livelli AWS Shield : Standard e Advanced; AMS offre Shield Advanced. Per ulteriori informazioni, consulta Shield Advanced.

Tutti AWS i clienti beneficiano delle protezioni automatiche di AWS Shield Standard, senza costi aggiuntivi. AWS Shield Standard difende dagli attacchi di livello DDo S di rete e di trasporto più comuni e frequenti che prendono di mira i siti Web o le applicazioni. Se utilizzi AWS Shield Standard Amazon CloudFront e Amazon Route 53, ricevi una protezione completa della disponibilità contro tutti gli attacchi noti all'infrastruttura (Layer 3 e 4).

Per livelli di protezione più elevati contro gli attacchi diretti alle tue applicazioni in esecuzione su risorse Amazon Elastic Compute Cloud (Amazon EC2), Elastic Load Balancing (ELB), CloudFront Amazon e AWS Global Accelerator Amazon Route 53, puoi abbonarti a. AWS Shield Advanced

Oltre alle protezioni a livello di rete e trasporto fornite in dotazione AWS Shield Standard, AWS Shield Advanced offre funzionalità aggiuntive di rilevamento e mitigazione contro attacchi DDo S di grandi dimensioni e sofisticati, visibilità quasi in tempo reale degli attacchi e integrazione con AWS WAF un firewall di applicazioni web. AWS Shield Advanced offre inoltre accesso 24 ore su 24, 7 giorni su 7 al AWS Shield Response Team (SRT) e protezione contro DDo i picchi correlati a S nei costi di Amazon Elastic Compute Cloud (EC2Amazon), Elastic Load Balancing (Elastic Load Balancing) CloudFront AWS Global Accelerator, Amazon e Amazon Route 53.

Domande frequenti su Shield Advanced in AWS Managed Services

D: Come posso richiedere l'accesso a Shield Advanced nel mio account AMS?

Richiedi l'accesso a Shield Advanced inviando una RFC con il tipo di modifica Management | AWS service | Self-provisioned service | Add (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli IAM al tuo account: e. `customer_shield_role` `aws_drt_shield_role` Una volta effettuato il provisioning nel tuo account, devi integrare i ruoli nella tua soluzione di federazione.

Dopo aver distribuito i ruoli nel tuo account, puoi utilizzarli `customer_shield_role` per confermare l'iscrizione al AWS Shield Advanced tuo account.

> **Note**
>
> Tieni presente che è previsto un canone mensile e un impegno di un anno associati all'uso di. AWS Shield Advanced Inoltre, l'utilizzo AWS Shield Advanced in AMS autorizza AMS a rivolgersi a AWS Shield (SRT), che può apportare modifiche alle regole del Web Application Firewall (AWS WAF) in caso di gravi incidenti di Distributed Denial of Service (S). DDo Queste modifiche verranno apportate in collaborazione con AMS.

D: Quali sono le restrizioni all'utilizzo di Shield Advanced nel mio account AMS?

Sebbene non sia una restrizione, è necessario tenere presente che l'utilizzo di Shield Advanced implementa il`aws_drt_shield_role`, che consente ai AWS Shield team (SRT) di apportare modifiche di emergenza alle AWS WAF regole all'interno degli account AMS durante gli incidenti S più gravi. DDo Questa operazione è consigliata da AMS per la risoluzione più rapida degli attacchi DDo S e si verificherebbe dopo un'escalation di AMS verso l'SRT.

D: Quali sono i prerequisiti o le dipendenze per utilizzare Shield Advanced nel mio account AMS?

Non ci sono prerequisiti o dipendenze per utilizzare Shield Advanced nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Snowball Edge nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Snowball Edge direttamente dal tuo account gestito AMS. Snowball Edge è una soluzione di trasporto dati su scala petabyte che utilizza dispositivi progettati per essere sicuri, per trasferire grandi quantità di dati da e verso il cloud. AWS Snowball Edge affronta le sfide più comuni relative ai trasferimenti di dati su larga scala, tra cui costi di rete elevati, lunghi tempi di trasferimento e problemi di sicurezza. Puoi utilizzare Snowball Edge per migrare dati di analisi, dati genomici, librerie video, archivi di immagini, backup e per archiviare parte delle chiusure dei data center, della sostituzione dei nastri o dei progetti di migrazione delle applicazioni. Il trasferimento di dati con Snowball Edge è semplice, veloce, più sicuro e può costare solo un quinto del costo del trasferimento di dati tramite Internet ad alta velocità.

Con Snowball Edge, non è necessario scrivere codice o acquistare hardware per trasferire i dati. Inizia utilizzando la console di AWS gestione per creare un processo di importazione per Snowball

e un dispositivo Snowball ti verrà spedito automaticamente. Una volta arrivato, collega il dispositivo alla rete locale, scarica ed esegui lo Snowball Client («Client») per stabilire una connessione, quindi utilizza il Client per selezionare le directory di file che desideri trasferire sul dispositivo. Il client quindi crittografa e trasferisce i file sul dispositivo ad alta velocità. Una volta completato il trasferimento e il dispositivo è pronto per essere restituito, l'etichetta di spedizione E Ink si aggiorna automaticamente e puoi monitorare lo stato del lavoro con Amazon Simple Notification Service (Amazon SNS), messaggi di testo o direttamente nella console. Per ulteriori informazioni, consulta AWS Snowball Edge.

Domande frequenti su Snowball Edge in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS Snowball Edge al mio account AMS?

L'implementazione di Snowball Edge in AMS è un processo in due fasi:

1. Invia un Management | Altro | Altro | Crea (ct-1e1xtak34nx76) modifica tipo e richiedi un ruolo di servizio per Snowball Edge per il tuo account AMS.
2. Richiedi l'accesso utente inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce i seguenti ruoli IAM al tuo account:, e. `customer_snowball_console_role` `customer_snowball_export_role` `customer_snowball_import_role` Dopo averlo inserito nel tuo account, devi inserire il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo AWS Snowball Edge nel mio account AMS?

La funzionalità completa di AWS Snowball Edge è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare AWS Snowball Edge nel mio account AMS?

È necessario disporre dell'account del ruolo di servizio come indicato sopra.

Utilizza AMS SSP per il provisioning AWS Step Functions nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Step Functions funzionalità direttamente nel tuo account gestito da AMS. AWS Step Functions è un servizio Web

che consente di coordinare i componenti di applicazioni e microservizi distribuiti utilizzando flussi di lavoro visivi. La creazione di applicazioni a partire da componenti individuali che eseguono ciascuno una funzione discreta, detta anche task, consente di dimensionare e modificare rapidamente le applicazioni. Step Functions offre un modo affidabile per coordinare i componenti e gestire le funzioni dell'applicazione. Step Functions offre una console grafica per visualizzare i componenti dell'applicazione in una serie di passaggi. Attiva e tiene traccia automaticamente di ogni passaggio e riprova in caso di errori, in modo che l'applicazione venga eseguita sempre nell'ordine e come previsto. Step Functions registra lo stato di ogni passaggio, così quando qualcosa va storto, puoi diagnosticare ed eseguire rapidamente il debug dei problemi. Per ulteriori informazioni, consulta AWS Step Functions.

Domande frequenti su Step Functions in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS Step Functions al mio account AMS?

Richiedi l'accesso AWS Step Functions inviando una RFC al Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC `customer_step_functions_role` fornisce il seguente ruolo IAM al tuo account:. Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo AWS Step Functions nel mio account AMS?

La funzionalità completa di AWS Step Functions è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare AWS Step Functions nel mio account AMS?

In fase di esecuzione, il ruolo utilizzato da Step Functions deve avere accesso ai servizi utilizzati dalla funzione step. Ad esempio, una funzione step potrebbe dipendere dalle funzioni Lambda. È probabile che qualcuno che crea una funzione step stia creando funzioni Lambda contemporaneamente e dovrebbe richiedere anche l'accesso a quel servizio.

Usa AMS SSP per effettuare il provisioning di AWS Systems Manager Parameter Store nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di AWS Systems Manager Parameter Store direttamente nel tuo account gestito da AMS. AWS Systems Manager Parameter Store fornisce uno storage sicuro e gerarchico per la gestione dei dati di

configurazione e la gestione dei segreti. È possibile archiviare dati, ad esempio le password, le stringhe di database e i codici di licenza, come valori dei parametri. È possibile memorizzare i valori in testo semplice o crittografati. Puoi fare riferimento ai valori utilizzando il nome univoco specificato quando crei il parametro. Altamente scalabile, disponibile e durevole, Parameter Store è supportato dal cloud. AWS Per ulteriori informazioni, consulta AWS Systems Manager Parameter Store.

> **Note**
>
> Se desideri un archivio segreto dedicato con gestione del ciclo di vita, usa Utilizza AMS SSP per il provisioning Gestione dei segreti AWS nel tuo account AMS invece di Parameter Store. Secrets Manager ti aiuta a soddisfare i tuoi requisiti di sicurezza e conformità consentendoti di ruotare i segreti automaticamente. Secrets Manager offre un'integrazione integrata per MySQL, PostgreSQL e Amazon Aurora su Amazon RDS, estensibile ad altri tipi di segreti personalizzando le funzioni Lambda.

AWS Systems Manager Domande frequenti su Parameter Store in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso a Systems Manager Parameter Store nel mio account AMS?

Richiedete l'accesso a AWS Systems Manager Parameter Store inviando una RFC al Management | AWS service | Self-provisioned service | Add change type (ct-1w8z66n899dct). Questa RFC fornisce `customer_systemsmanager_parameterstore_console_role` il seguente ruolo IAM al tuo account:. Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo di AWS Systems Manager Parameter Store nel mio account AMS?

È necessario utilizzare le chiavi AWS gestite; l'accesso è limitato alla creazione di chiavi KMS personalizzate. Tuttavia, se è richiesta una chiave personalizzata, invia una RFC per creare una chiave gestita dal cliente (CMK) utilizzando Deployment | Advanced Stack Components | KMS Key | Create change type (ct-1d84keiri1jhg) con questo ruolo IAM, come valore per i parametri and. `customer_systemsmanager_parameterstore_console_role` `IAMPrincipalsRequiringDecryptPermissions`

`IAMPrincipalsRequiringEncryptPermissionsPrincipal` Dopo aver creato la chiave KMS, puoi creare una stringa sicura utilizzandola.

D: Quali sono i prerequisiti o le dipendenze per utilizzare AWS Systems Manager Parameter Store nel mio account AMS?

Non ci sono prerequisiti; tuttavia, SSM Parameter Store dipende da KMS per creare una stringa sicura in modo da poter crittografare e decrittografare i valori memorizzati in Parameter Store.

Usa AMS SSP per fornire AWS Systems Manager l'automazione nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di AWS Systems Manager automazione direttamente nel tuo account gestito AMS. AWS Systems Manager L'automazione semplifica le attività comuni di manutenzione e distribuzione delle istanze di Amazon Elastic Compute Cloud e di altre AWS risorse utilizzando runbook, azioni e quote di servizio. Ti consente di creare, eseguire e monitorare automazioni su larga scala. Un Systems Manager Automation è un tipo di documento di Systems Manager che definisce le azioni che Systems Manager esegue sulle istanze gestite. Un runbook utilizzato per eseguire attività comuni di manutenzione e distribuzione, come l'esecuzione di comandi o script di automazione all'interno delle istanze gestite. Systems Manager include funzionalità che ti aiutano a indirizzare grandi gruppi di istanze utilizzando i tag Amazon Elastic Compute Cloud e controlli di velocità che ti aiutano a implementare le modifiche in base ai limiti che definisci. I runbook sono scritti utilizzando JavaScript Object Notation (JSON) o YAML. Tuttavia, utilizzando lo strumento Document Builder (Generatore documenti) nella console del servizio di automazione di Systems Manager, è possibile creare un runbook senza doverlo creare in formato JSON o YAML nativo. In alternativa, puoi utilizzare i runbook forniti da Systems Manager con passaggi predefiniti adatti alle tue esigenze. Per ulteriori informazioni, consulta Lavorare con i runbook nella documentazione. AWS Systems Manager

> **Note**
>
> Sebbene Systems Manager Automation supporti 20 tipi di azioni che possono essere utilizzati nel runbook, è possibile utilizzare un numero limitato di azioni durante la creazione del runbook da utilizzare nel proprio account AMS Advanced. Allo stesso modo, è possibile utilizzare un numero limitato di runbook forniti da Systems Manager direttamente o dall'interno del proprio runbook. Per i dettagli, consulta le restrizioni nelle seguenti domande frequenti.

AWS Systems Manager Domande frequenti sull'automazione in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso a Systems Manager Automation nel mio account AMS?

Richiedi l'accesso all' AWS Systems Manager automazione inviando una RFC con Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce `customer_systemsmanager_automation_console_role` il seguente ruolo IAM al tuo account:. Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le limitazioni all'utilizzo dell' AWS Systems Manager automazione nel mio account AMS?

È necessario creare il runbook, con un set limitato di azioni supportate da Systems Manager per l'automazione, solo per eseguire and/or script di comandi all'interno delle istanze gestite. Le azioni disponibili e le eventuali restrizioni sono descritte di seguito.

AWS Systems Manager Limitazioni dell'automazione

Azione	Descrizione	Limitazione
aws: assertAwsResource Proprietà —	Afferma lo stato di una AWS risorsa o di un evento	Solo istanze EC2
aws:aws:branch —	Esegui passaggi di automazione condizionale	Nessuna limitazione
AWS: crea tag —	Crea tag per le risorse AWS	Solo per i runbook di automazione SSM che hai creato
AWS: esegui l'automazione —	Esegui un'altra automazione	Solo il runbook di automazione che hai creato
AWS: ExecuteScript —	Esegui uno script	Unico script che non effettua alcuna chiamata API a nessun servizio

Azione	Descrizione	Limitazione
aws:pause —	Metti in pausa un'automazione	Nessuna limitazione
AWS: runCommand —	Esegui un comando su un'istanza gestita	Utilizzando solo il documento fornito da System Manager - AWS- RunShellScript e AWS-RunPowerShellScript
aws:sleep —	Ritardare un'automazione	Nessuna limitazione
Leggi: waitForAws ResourceProperty —	Attendi la proprietà di una AWS risorsa	Solo EC2 istanze

Puoi anche scegliere di eseguire comandi o script direttamente con i runbook AWS RunShellScript e AWS forniti da Systems Manager RunPowerShellScript utilizzando la funzionalità «Run Command» dalla console Systems Manager. Puoi anche inserire questi runbook all'interno del tuo runbook che prevede ulteriori operazioni di validazione pre and/or post convalida o qualsiasi logica di automazione complessa.

Il ruolo aderisce al principio del privilegio minimo e fornisce solo le autorizzazioni necessarie per creare, eseguire e recuperare i dettagli di esecuzione dei runbook finalizzati all'esecuzione di script di comandi all'interno delle istanze gestite. and/or Non fornisce l'autorizzazione per altre funzionalità fornite dal servizio. AWS Systems Manager Sebbene la funzionalità consenta di creare runbook di automazione, l'esecuzione dei runbook non può essere indirizzata alle risorse di proprietà di AMS.

D: Quali sono i prerequisiti o le dipendenze per utilizzare AWS Systems Manager Automation nel mio account AMS?

Non ci sono prerequisiti; tuttavia, è necessario assicurarsi che i controlli di and/or conformità dei processi interni vengano rispettati durante la creazione dei runbook. Consigliamo inoltre di testare a fondo i runbook prima di eseguirli con risorse di produzione.

D: La policy Systems Manager può **`customer_systemsmanager_automation_policy`** essere associata ad altri ruoli IAM?

No, a differenza di altri servizi abilitati all'autofornitura, questa policy può essere assegnata solo al ruolo predefinito assegnato. `customer_systemsmanager_automation_console_role`

A differenza delle policy di altri ruoli SSPS, questa policy SSM SSPS non può essere condivisa con altri ruoli IAM personalizzati, poiché questo servizio AMS serve solo per l'esecuzione di comandi o script di automazione all'interno delle istanze gestite. Se si consentisse di associare queste autorizzazioni ad altri ruoli IAM personalizzati, potenzialmente alle autorizzazioni su altri servizi, l'ambito delle azioni consentite potrebbe estendersi ai servizi gestiti e potenzialmente ridurre il livello di sicurezza dell'account.

Per valutare eventuali richieste di modifica (RFCs) rispetto ai nostri standard tecnici AMS, collabora con i rispettivi Cloud Architect o Service Delivery Manager, consulta le recensioni di sicurezza RFC.

> **Note**
>
> AWS Systems Manager ti consente di utilizzare i runbook condivisi con il tuo account. Ti consigliamo di fare attenzione ed eseguire un controllo di due diligence quando usi runbook condivisi e assicurati di esaminare il contenuto per capire come command/scripts vengono eseguiti prima di eseguire i runbook. Per i dettagli, consulta le migliori pratiche per i documenti SSM condivisi.

Utilizza AMS SSP per il provisioning AWS Transfer Family nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità (Transfer AWS Transfer Family Family) direttamente nel tuo account gestito AMS. AWS Transfer Family è un AWS servizio completamente gestito che consente di trasferire file tramite Secure File Transfer Protocol (SFTP), da e verso lo storage Amazon Simple Storage Service (Amazon S3) Simple Storage Service (Amazon S3). SFTP è noto anche come Secure Shell (SSH) File Transfer Protocol. SFTP viene utilizzato in flussi di lavoro per lo scambio di dati tra settori diversi quali servizi finanziari, settore sanitario, pubblicità e vendita al dettaglio.

Con AWS SFTP, puoi accedere a un server SFTP AWS senza la necessità di eseguire alcuna infrastruttura server. È possibile utilizzare questo servizio per migrare i flussi di lavoro basati su SFTP AWS mantenendo inalterati i client e le configurazioni degli utenti finali. Per prima cosa associ il tuo hostname all'endpoint del server SFTP, quindi aggiungi gli utenti e fornisci loro il giusto livello di accesso. Dopo averlo fatto, le richieste di trasferimento degli utenti vengono gestite direttamente dall'endpoint del server SFTP. AWS Per ulteriori informazioni, consulta anche Creare un server compatibile con AWS Transfer for SFTPSFTP.

AWS Transfer for SFTP nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS Transfer for SFTP al mio account AMS?

Richiedi l'accesso AWS Transfer for SFTP inviando una RFC al Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Tramite questa RFC, nel tuo account vengono assegnati i seguenti ruoli IAM e una policy:

- `customer_transfer_author_role`. Questo ruolo è progettato per consentirti di gestire il servizio SFTP tramite la console.
- `customer_transfer_sftp_server_logging_role`. Questo ruolo è progettato per essere collegato al server SFTP. Consente al server SFTP di inserire i log. CloudWatch
- `customer_transfer_sftp_user_role`. Questo ruolo è progettato per essere associato agli utenti SFTP. Consente agli utenti SFTP di interagire con il bucket S3.
- `policy customer_transfer_scope_down_policy`. Si tratta di una politica mirata che può essere applicata all'utente SFTP per limitare l'accesso del bucket S3 alle proprie cartelle home.
- `customer_transfer_sftp_efs_user_role`. Questo ruolo è progettato per essere associato agli utenti SFTP. Consente agli utenti SFTP di interagire con il file system EFS.

Dopo aver effettuato il provisioning nel tuo account, devi inserire i ruoli nella tua soluzione di federazione.

D: Quali sono le restrizioni all'utilizzo AWS Transfer for SFTP nel mio account AMS?

AWS La configurazione Transfer for SFTP è limitata alle risorse senza prefissi «AMS-» o «MC-» per impedire qualsiasi modifica all'infrastruttura AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare nel mio account AMS? AWS Transfer for SFTP

- È necessario disporre di un bucket Amazon S3 con un nome che contenga la parola chiave «transfer» prima di creare il AWS Transfer for SFTP server e gli utenti.
- Per utilizzare un «Customer Identify Provider», devi implementare l'API Gateway, la funzione Lambda e il tuo repository utente (AD, Secrets Manager e così via). Per ulteriori informazioni, consulta Abilitare l'autenticazione tramite password per l' AWS Transfer for SFTP utilizzo Gestione dei segreti AWS e l'utilizzo dei provider di identità.

Utilizza AMS SSP per il provisioning AWS Transit Gateway nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Transit Gateway funzionalità direttamente nel tuo account gestito da AMS. AWS Transit Gateway è un servizio che ti consente di connettere Amazon Virtual Private Cloud (VPCs) e le tue reti locali a un unico gateway. Man mano che aumenti il numero di carichi di lavoro su cui esegui AWS, devi essere in grado di scalare le tue reti su più account e Amazon VPCs per stare al passo con la crescita. Oggi puoi connettere coppie di Amazon VPCs utilizzando il peering. Tuttavia, la gestione della point-to-point connettività su molti Amazon VPCs, senza la possibilità di gestire centralmente le politiche di connettività, può essere costosa e complicata dal punto di vista operativo. Per la connettività locale, devi collegare la tua AWS VPN a ogni singolo Amazon VPC. La creazione di questa soluzione può richiedere molto tempo e può essere difficile da gestire quando il numero sale VPCs a centinaia. Per ulteriori informazioni, consulta AWS Transit Gateway.

AWS Transit Gateway nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS Transit Gateway al mio account AMS?

Richiedi l'accesso AWS Transit Gateway inviando una RFC al Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC `customer_tgw_console_role` fornisce il seguente ruolo IAM al tuo account:. Una volta effettuato il provisioning nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo AWS Transit Gateway nel mio account AMS?

La funzionalità completa di AWS Transit Gateway è disponibile nel tuo account di landing zone con account singolo AMS, ad eccezione delle modifiche alla tabella delle rotte per il routing Transit Gateway. Richiedi modifiche alla tabella delle rotte inviando un tipo di modifica Gestione | Altro | Altro | Crea modifica (ct-1e1xtak34nx76).

> **Note**
>
> Questo servizio è supportato solo per la landing zone a account singolo (SALZ), non per la zona di atterraggio multi-account (MALZ).

D: Quali sono i prerequisiti o le dipendenze da utilizzare nel mio account AMS? AWS Transit Gateway

Non ci sono prerequisiti o dipendenze da utilizzare AWS Transit Gateway nel tuo account AMS.

Usa AMS SSP per il provisioning AWS WAF - Web Application Firewall nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS WAF funzionalità direttamente nel tuo account gestito da AMS. AWS WAF è un firewall per applicazioni Web (AWS WAF) che aiuta a proteggere le applicazioni Web da exploit Web comuni che potrebbero influire sulla disponibilità delle applicazioni, compromettere la sicurezza o consumare risorse eccessive. AWS WAF consente di controllare il traffico da consentire o bloccare verso le applicazioni Web definendo regole di sicurezza Web personalizzabili. È possibile AWS WAF utilizzarlo per creare regole personalizzate che bloccano i modelli di attacco più comuni, come SQL injection o cross-site scripting, e regole progettate per l'applicazione specifica.

Per ulteriori informazioni, consulta AWS WAF - Web Application Firewall.

AMS non supporta il monitoraggio (CloudWatch allarmi, eventi, avvisi MMS) per. AWS WAF A causa della natura di AWS WAF, è necessario creare regole personalizzate per le applicazioni; AMS non può quantificare e creare allarmi per voi, indipendentemente dal contesto dell'applicazione. Per ulteriori informazioni, consulta AWS WAF - Web Application Firewall.

AWS WAF nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere AWS WAF di essere configurato nel mio account AMS?

Richiedi l'accesso AWS WAF inviando una RFC con il servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce `customer_waf_role` il seguente ruolo IAM al tuo account:. Dopo aver assegnato il ruolo AWS WAF IAM nel tuo account, devi integrare il ruolo nella tua soluzione di federazione.

D: Quali sono le restrizioni all'utilizzo? AWS WAF

Dopo aver fornito le autorizzazioni, avrai la piena funzionalità di. AWS WAF

D: Quali sono i prerequisiti o le dipendenze per l'utilizzo? AWS WAF

Non ci sono prerequisiti o dipendenze da utilizzare AWS WAF nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS Well-Architected Tool nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Well-Architected Tool funzionalità direttamente nel tuo account gestito da AMS. Ti AWS Well-Architected Tool aiuta a rivedere lo stato dei tuoi carichi di lavoro e a confrontarli con le migliori pratiche architettoniche più recenti. AWS Lo strumento si basa sul AWS Well-Architected Framework, sviluppato per aiutare gli architetti del cloud a creare un'infrastruttura applicativa sicura, ad alte prestazioni, resiliente ed efficiente. Questo framework offre un approccio coerente per la valutazione delle architetture, è stato utilizzato in decine di migliaia di revisioni dei carichi di lavoro condotte dal team di architettura delle AWS soluzioni e fornisce linee guida per aiutare a implementare progetti scalabili in base alle esigenze delle applicazioni nel tempo. Per ulteriori informazioni, consulta AWS Well-Architected Tool.

AWS WA Tool nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS Well-Architected Tool al mio account AMS?

Richiedi l'accesso AWS Well-Architected Tool inviando una RFC con il servizio Management | AWS | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce `customer_well_architected_tool_console_admin_role` il seguente ruolo IAM al tuo account:. Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa.

D: Quali sono le restrizioni all'utilizzo AWS Well-Architected Tool nel mio account AMS?

La funzionalità completa di AWS Well-Architected Tool è disponibile nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare AWS Well-Architected Tool nel mio account AMS?

Non ci sono prerequisiti o dipendenze da utilizzare AWS Well-Architected Tool nel tuo account AMS.

Utilizza AMS SSP per il provisioning AWS X-Ray nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità (AWS X-Ray X-Ray) direttamente nel tuo account gestito AMS. AWS X-Ray aiuta gli sviluppatori ad analizzare ed eseguire il debug di applicazioni distribuite di produzione, come quelle create utilizzando un'architettura di microservizi. Con X-Ray, è possibile comprendere le prestazioni dell'applicazione

e dei relativi servizi sottostanti, identificare e risolvere la causa principale dei problemi e degli errori di prestazioni. X-Ray fornisce una end-to-end visualizzazione delle richieste mentre viaggiano attraverso l'applicazione e mostra una mappa dei componenti sottostanti dell'applicazione. È possibile utilizzare X-Ray per analizzare sia le applicazioni in fase di sviluppo che quelle in produzione, da semplici applicazioni a tre livelli a complesse applicazioni di microservizi composte da migliaia di servizi. Per ulteriori informazioni, consulta AWS X-Ray.

Domande frequenti su X-Ray in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso AWS X-Ray al mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce il seguente ruolo IAM al tuo account:. `customer_xray_console_role` Dopo averlo inserito nel tuo account, devi integrare il ruolo nella tua soluzione federativa. Inoltre, è necessario disporre dei dati necessari `customer_xray_daemon_write_instance_profile` per trasferire i dati dalle EC2 istanze Amazon a X-Ray. Questo profilo di istanza viene creato quando ricevi il. `customer_xray_console_role`

Puoi inviare una richiesta di servizio ad AMS Operations per assegnarla `customer_xray_daemon_write_policy` al profilo dell'istanza esistente oppure puoi utilizzare il profilo di istanza creato quando AMS Operations abilita X-Ray per te.

D: Quali sono le restrizioni all'utilizzo AWS X-Ray nel mio account AMS?

La funzionalità completa di AWS X-Ray è disponibile nel tuo account AMS ad eccezione della crittografia con chiave AWS KMS (chiave KMS). AWS X-Ray crittografa tutti i dati di traccia per impostazione predefinita. Per impostazione predefinita, X-Ray crittografa le tracce e i dati correlati a riposo. Se devi crittografare i dati inattivi con una chiave, puoi scegliere tra AWS-managed KMS key (aws/xray) o KMS Customer-Managed key. Per la chiave KMS gestita dal cliente per la crittografia a raggi X, invia un tipo di modifica Gestione | Altro | Altro | Crea modifica (ct-1e1xtak34nx76).

D: Quali sono i prerequisiti o le dipendenze da utilizzare nel mio account AMS? AWS X-Ray

AWS X-Ray dipende da Amazon S3 CloudWatch e Logs CloudWatch, che sono già implementati negli account AMS. Le dipendenze transitive variano in base alle fonti di dati e ad altri AWS servizi con AWS X-Ray cui le funzionalità possono interagire (ad esempio, Amazon Redshift, Amazon RDS, Athena).

Usa AMS SSP per effettuare il provisioning della macchina virtuale Import/Export nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alla macchina virtuale Import/Exportcapabilities direttamente dal tuo account gestito AMS. VM ti Import/Export consente di importare facilmente immagini di macchine virtuali dal tuo ambiente esistente su EC2 istanze Amazon ed esportarle nuovamente nel tuo ambiente locale. Questa offerta ti consente di sfruttare gli investimenti esistenti nelle macchine virtuali che hai creato per soddisfare i requisiti di sicurezza IT, gestione della configurazione e conformità trasferendo tali macchine virtuali in Amazon EC2 come ready-to-use istanze. Puoi anche esportare le istanze importate nella tua infrastruttura di virtualizzazione locale, consentendoti di distribuire carichi di lavoro nell'infrastruttura IT. Per saperne di più, consulta VM Import/Export.

Domande frequenti sulle macchine virtuali Import/Export in AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso alla macchina virtuale Import/Export nel mio account AMS?

Richiedi l'accesso alla macchina virtuale Import/Export inviando una RFC al Management | AWS service | Self-provisioned service | Aggiungi tipo di modifica (ct-1w8z66n899dct). Questa RFC fornisce la `customer_vmimport_policy` seguente politica IAM al tuo account:. Dopo averlo inserito nel tuo account, devi inserire il ruolo nella tua soluzione federativa.

Un ruolo aggiuntivo, il ruolo VM Import/Export Service, è necessario affinché il servizio possa eseguire azioni sull'account.

D: Quali sono le restrizioni all'uso di VM Import/Export nel mio account AMS?

- La funzionalità per importare immagini di macchine e volumi di dati personalizzati è entrambe disponibili in AMS VM Import/Export. Tuttavia, le autorizzazioni per S3 sono state ridotte per limitare le azioni ai bucket corrispondenti al nome, al fine di limitare l'accesso alle `customer-vmimport-*` informazioni all'interno dell'account.
- L'importazione di immagini e istantanee è supportata in AMS VM Import/Export. Tuttavia, la funzionalità di importazione ed esportazione delle istanze non è disponibile a causa delle misure di sicurezza.
- Inoltre, la funzionalità di esportazione è stata disattivata per ridurre il rischio di esportazione di dati riservati e sensibili.

D: Quali sono i prerequisiti o le dipendenze per utilizzare VM Import/Export nel mio account AMS?

- È necessario fornire un'immagine del disco supportata da importare nell'ambiente. AWS Per informazioni, consulta Import/Export Requisiti VM.
- La VM Import/Export non è accessibile tramite la AWS console. È necessario accedere a questo servizio tramite AWS CLI AWS Strumenti per PowerShell, o il AWS SDKs. In alternativa, puoi richiedere un profilo di istanza inviando il tipo di modifica ct-117rmp64d5mvb: Deployment | Advanced stack components | Identity and Access Management (IAM) | Create instance profile. EC2 Questo profilo di istanza consente agli strumenti di eseguire comandi da un'istanza.

Modalità gestita dal cliente

La modalità Customer Managed di AWS Managed Services (AMS) fornisce un modello di governance flessibile e adattabile alle tue esigenze. Questa può essere considerata un'opzione alternativa per servizi e applicazioni che AMS non è in grado di gestire per te. AMS non gestisce un'infrastruttura ospitata in account creati in questa modalità. Tuttavia, è possibile sfruttare la gestione centralizzata di più account in questa modalità. In questa modalità è possibile sfruttare le seguenti funzionalità Multi-Account Landing Zone:

- Distribuzione automatizzata degli account
- Connettività tramite Transit Gateway nell'account di rete
- Libreria AMS Config Rules
- Archivia copie dei log nell'account di registrazione
- Aggregazione degli avvisi Guard Duty gestiti dal cliente all'account Security
- Fatturazione consolidata
- Abilitazione di politiche di controllo del servizio personalizzate.

Ad esempio: se desideri eseguire carichi di lavoro su Ubuntu Pro, che non è un sistema operativo gestito da AMS, puoi utilizzare un account gestito dal cliente per ospitarlo. Puoi anche consolidare i carichi di lavoro tramite account gestiti dai clienti, per sfruttare lo sconto all'ingrosso sui piani Instances/Sharing riservati disponibili tramite la condivisione tra un'organizzazione AWS.

Guida introduttiva alla modalità Customer Managed

La modalità AMS Customer Managed è disponibile tramite uno speciale account applicativo multi-account landing zone.

Per i dettagli, incluso come creare un account di applicazione gestito dal cliente, consulta Account applicativi gestiti dal cliente.

AMS e AWS Service Catalog

Service Catalog in AWS Managed Services (AMS) consente alle organizzazioni di creare e gestire cataloghi di servizi IT (IT) di AWS e consente agli amministratori IT di creare, gestire e distribuire cataloghi di prodotti approvati agli utenti finali nei propri account, che possono quindi accedere ai prodotti di cui hanno bisogno in un portale di servizi personalizzato. Gli amministratori possono controllare quali utenti hanno accesso a ciascun prodotto per far rispettare la conformità alle politiche aziendali dell'organizzazione. Gli amministratori possono anche impostare ruoli in modo che gli utenti finali richiedano solo l'accesso IAM a Service Catalog per distribuire risorse approvate. Service Catalog consente alla tua organizzazione di trarre vantaggio da una maggiore agilità e da costi ridotti perché gli utenti finali possono trovare e lanciare solo i prodotti di cui hanno bisogno da un catalogo sotto il tuo controllo.

Service Catalog offre un'alternativa al processo di richiesta di modifica (RFC) di AMS per il provisioning e l'aggiornamento delle risorse nei tuoi account gestiti da AMS. AMS gestisce tutte le attività operative dell'infrastruttura necessarie per eseguire AWS su larga scala per tutte le risorse di infrastruttura fornite tramite Service Catalog, tra cui sicurezza, conformità, provisioning, disponibilità, patch, monitoraggio, avvisi, reportistica, risposta agli incidenti e ottimizzazione dei costi. L'utilizzo di Service Catalog nel tuo account gestito AMS ti offre un meccanismo per gestire centralmente i servizi IT comunemente distribuiti e ti aiuta a raggiungere una governance coerente, consentendo al contempo agli utenti di implementare rapidamente solo i servizi IT approvati di cui hanno bisogno nei loro ambienti gestiti.

Guida introduttiva a Service Catalog

Per iniziare a usare Service Catalog in AMS, invia una richiesta di servizio tramite la console AMS per richiedere l'accesso a Service Catalog. Dopo l'invio della richiesta, verranno distribuiti tre ruoli IAM nei tuoi account insieme a uno stack gestito AMS contenente la CloudFormation macro che richiama l'AMS `Transform` (descritta in precedenza) in modo da poter registrare i prodotti nei nostri sistemi ed eseguire operazioni sull'infrastruttura fornita tramite Service Catalog. I tre ruoli IAM implementati includono un ruolo per gli amministratori IT di gestire i prodotti come amministratori di Service Catalog; un ruolo per i proprietari delle applicazioni e gli utenti finali per configurare, avviare e gestire i prodotti; e un ruolo che verrà utilizzato come vincolo di lancio, che definisce le autorizzazioni che Service Catalog utilizzerà durante il lancio o l'aggiornamento del prodotto.

Service Catalog in AMS prima di iniziare

Service Catalog sostituisce il processo RFC (Request for Change) esistente di AMS?

Negli account in cui Service Catalog è abilitato, fungerà da sistema di gestione delle modifiche in cui fornisci e aggiorni i servizi IT nel tuo account AMS tramite il tuo catalogo di prodotti predefinito; AMS fornirà un portfolio/product catalogo predefinito e gli amministratori IT potranno crearne e configurarne uno personalizzato. Service Catalog riconoscerà solo gli stack forniti tramite Service Catalog. Allo stesso modo, i servizi forniti tramite Service Catalog non saranno modificabili tramite il processo RFC di AMS, poiché le modifiche esterne al Service Catalog allontaneranno lo stack dalla configurazione di prodotto approvata.

Posso vedere gli stack forniti tramite il catalogo dei servizi nella console AMS?

Sì. È possibile visualizzare tutti gli stack forniti tramite il catalogo dei servizi nella console AMS. Gli stack forniti tramite il catalogo dei servizi sono facilmente identificabili dall'ID dello stack «SC-». Sebbene gli stack siano visualizzabili nella console AMS, non sarà possibile eseguire l'aggiornamento tramite il processo AMS RFC. L'accesso al sistema di gestione delle modifiche AMS (RFCs) è limitato alla richiesta di accesso, all'orchestrazione delle patch e al backup. RFCs

Se eseguo il and/or provisioning di uno stack tramite Service Catalog, nella console AMS sarà presente una RFC corrispondente?

L'unica RFC che verrà mostrata nella console AMS è una RFC per registrare lo stack con AMS quando uno stack viene inizialmente fornito. Questa RFC viene archiviata automaticamente dal processo di convalida AMS che viene attivato all'avvio di uno stack tramite Service Catalog. Tutti gli altri provisioning e le modifiche vengono tracciati direttamente in Service Catalog e sono visualizzabili nella console Service Catalog. Inoltre, è possibile utilizzare la funzionalità Provisioned Product Plan in Service Catalog per visualizzare l'elenco delle modifiche che verranno apportate alle risorse prima del provisioning o dell'aggiornamento del prodotto.

Devo fare qualcosa di specifico per il provisioning dei prodotti nel mio account gestito da AMS?

Sì. Tutti i prodotti Service Catalog forniti negli account AMS devono contenere questa riga di codice JSON nel modello CFN che definisce quel prodotto:

```
"Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
{"Ref":"AWS::StackId"}}}
```

Questo frammento di CloudFormation codice attiva le convalide AMS necessarie prima che la risorsa possa essere fornita nell'account gestito da AMS. È responsabilità dell'utente includere

questa riga di codice come parte della definizione del prodotto. Se non è inclusa, il provisioning avrà esito negativo e verrà visualizzato il seguente messaggio di errore: «Impossibile creare il prodotto. Questo account è gestito da AMS. Tutti i prodotti negli account AMS devono avere il `Transform` codice AMS nel modello.»

Esistono funzionalità del Service Catalog non disponibili and/or solo per i clienti AMS al momento del lancio?

Sì, le seguenti funzionalità SC non sono disponibili per i clienti AMS al momento del lancio iniziale:

- Creazione di account tramite Service Catalog
- Possibilità di avviare tutti i servizi AWS tramite Service Catalog in un account gestito da AMS. La disponibilità del servizio AWS è limitata ai servizi supportati da AMS (gestiti e forniti autonomamente). Per ulteriori informazioni sui servizi supportati da AMS, consulta la descrizione del servizio AMS.
- I connettori di Service Catalog IT service manager (ITSM) non comunicheranno con i report sugli incidenti e le richieste di assistenza di AMS.
- Possibilità di sfruttare gli avvii rapidi e le architetture di riferimento di Service Catalog senza modifiche. Ricorda che i prodotti Service Catalog per gli account AMS devono contenere questa riga di codice JSON:

  ```
  "Transform":{"Name":"AmsStackTransform","Parameters":{"StackId":
  {"Ref":"AWS::StackId"}}}
  ```

  nel modello CNF. Tieni presente che questa riga non fa parte di un tipico CloudFormation modello AWS e deve essere aggiunta in modo esplicito.
- Terraform non è attualmente supportato da AMS per il provisioning dei prodotti Service Catalog.
- Gli stackset AWS CFN non sono supportati in AMS.
- Non è possibile creare ruoli IAM personalizzati.
- Le azioni di servizio sono limitate a:
  - AWS- RebootRdsInstance
  - Istanza AWS-Restart EC2
  - Istanza AWS-Start EC2
  - AWS- StartRdsInstance
  - Istanza AWS-Stop EC2
  - AWS- StopRdsInstance

- AWS- CreateImage
- AWS- CreateRdsSnapshot
- AWS- CreateSnapshot

> **Note**
>
> Quando crei azioni di servizio, puoi configurare il ruolo di esecuzione in modo che corrisponda alle autorizzazioni dell'utente finale, al ruolo di lancio o a un ruolo IAM personalizzato a tua scelta. Il ruolo di esecuzione selezionato deve disporre di autorizzazioni sufficienti per eseguire l'azione di servizio e disporre di un codice TrustPolicy che ne consenta l'assunzione da parte di Service Catalog, altrimenti l'azione di servizio avrà esito negativo al momento dell'esecuzione. Si consiglia di utilizzare AWSManagedServicesServiceCatalogLaunchRole, che dispone delle autorizzazioni e della politica di fiducia corrette da utilizzare come azione di servizio.

Per cosa dovrò ancora utilizzare il sistema RFC AMS?

In caso di disponibilità generale (GA) sarà comunque necessario utilizzare RFCS per eseguire le seguenti azioni:

- Configurazione di Patch Orchestrator
- Configurazione delle politiche di backup
- Richiesta di accesso all'istanza
- Creazione e assegnazione di gruppi di sicurezza che non rientrano nelle linee guida AMS.
- Esecuzione dell'acquisizione del carico di lavoro (WIGS)
- Creazione di ruoli IAM

Posso usare l'interfaccia a riga di comando di Service Catalog per accedere a Service Catalog nel mio account gestito da AMS?

Sì, Service Catalog APIs è disponibile e abilitato tramite la CLI. Sono disponibili azioni dalla gestione degli elementi del Service Catalog fino alla fornitura e alla chiusura di tali artefatti. Per ulteriori informazioni, consulta le risorse di AWS Service Catalog o scarica l'SDK o la CLI AWS più recenti.

Chi crea, gestisce e distribuisce i cataloghi dei prodotti approvati dei clienti?

L'amministratore del catalogo del cliente, l'amministratore and/or IT o la risorsa assegnata, è responsabile della gestione dei cataloghi del Service Catalog e dei prodotti approvati.

Posso usare AMS AMIs?

Gli AMIs AMS venduti dopo marzo 2020 possono essere distribuiti tramite AWS Service Catalog.

Come posso migrare ad AMS utilizzando Service Catalog?

Per migrare il carico di lavoro su AMS utilizzando Service Catalog, iniziate seguendo il processo Workload Ingest (WIGs) per creare un'AMI in AMS. Utilizzi l'AMI prodotta da WIGS per creare un prodotto in Service Catalog. La procedura per eseguire questa operazione è descritta in dettaglio in AWS Service Catalog - Getting Started.

Onboarding con AMS Multi-Account Landing Zone (MALZ)

Architettura di rete MALZ

Informazioni sull'architettura di rete multi-account landing zone

Prima di iniziare il processo di onboarding verso AWS Managed Services (AMS) Multi-account landing zone (MALZ), è importante comprendere l'architettura di base, o landing zone, che AMS crea per tuo conto, i suoi componenti e le sue funzioni.

La landing zone multi-account AMS è un'architettura multi-account, preconfigurata con l'infrastruttura per facilitare l'autenticazione, la sicurezza, il networking e la registrazione.

> **Note**
>
> Per le stime dei costi, consulta i componenti di base dell'ambiente di landing zone multi-account AMS.

Argomenti

- Regione del servizio
- Unità organizzative
- Policy di controllo dei servizi e AWS Organization

Il diagramma seguente illustra a grandi linee la struttura dei conti e il modo in cui l'infrastruttura è suddivisa in ciascuno dei conti:

Regione del servizio

Tutte le risorse all'interno di una landing zone con più account AMS vengono distribuite all'interno di un'unica regione AWS di tua scelta, a causa dell'attuale limitazione interregionale con Active Directory e Transit Gateway.

Unità organizzative

Una tipica landing zone con più account AMS è composta da quattro unità organizzative di primo livello ()OUs:

- L'unità organizzativa (OU) principale (utilizzata per raggruppare gli account da amministrare come unità singola)
- L'unità organizzativa delle applicazioni
- L'unità organizzativa gestita dal cliente
- Accelerano l'unità organizzativa

La landing zone multi-account gestita da AMS consente inoltre di creare account personalizzati OUs per il raggruppamento e l'organizzazione di account AWS e di associare account personalizzati SCPs ad essi; per esempi su questa operazione, consulta Account di gestione | Creazione di account personalizzati OUs e di gestione | Creazione di SCP personalizzati (automazione gestita), rispettivamente. AMS offre quattro account esistenti OUs in base ai quali è possibile richiedere nuovi account: accelerate, applications > managed, applications > development OUs e customer-managed.

- accelerare OU:

  Si tratta di un'unità organizzativa di primo livello in AMS multi-account landing zone (MALZ). Gli account di questa unità organizzativa vengono forniti da AMS con un RFC (Deployment | Managed landing zone | Management account | Create Accelerate account, change type ID: ct-2p93tyd5angmi). In questi account Accelerate Application, puoi beneficiare di servizi operativi accelerati come monitoraggio e avvisi, gestione degli incidenti, gestione della sicurezza e gestione dei backup. Per maggiori dettagli, consulta Account AMS Accelerate.

- applicazioni > unità organizzativa gestita:

  In questa unità organizzativa secondaria dell'Application OU, gli account sono completamente gestiti da AMS, comprese tutte le attività operative. Le attività operative comprendono la gestione delle richieste di assistenza, la gestione degli incidenti, la gestione della sicurezza, la gestione della continuità, la gestione delle patch, l'ottimizzazione dei costi, il monitoraggio e la gestione degli eventi. Queste attività vengono eseguite per la gestione dell'infrastruttura. OUs È possibile creare più figli in base alle esigenze, fino al raggiungimento del limite massimo di nested OUs per le organizzazioni AWS. Per i dettagli, consulta Quotas for AWS Organizations.

- applicazioni > unità organizzativa di sviluppo:

In questa unità organizzativa secondaria dell'unità organizzativa dell'applicazione nella landing zone gestita da AMS, gli account sono account in modalità sviluppatore che forniscono autorizzazioni elevate per il provisioning e l'aggiornamento di risorse AWS al di fuori del processo di gestione delle modifiche AMS. Questa unità organizzativa supporta anche la creazione di nuove unità organizzative secondarie, se necessario.

- OU gestita dal cliente:

  Si tratta di un'unità organizzativa di primo livello nella landing zone multi-account AMS. Gli account appartenenti a questa unità organizzativa vengono forniti da AMS con una RFC. In questi account, le operazioni dei carichi di lavoro e delle risorse AWS sono sotto la tua responsabilità. Questa unità organizzativa supporta anche la creazione di nuove unità organizzative secondarie, se necessario.

Come procedura ottimale, consigliamo di raggruppare gli account in queste OUs sottocategorie e in quelle richieste dall'utente in base alle relative funzionalità e politiche. OUs

Policy di controllo dei servizi e AWS Organization

AWS fornisce policy di controllo dei servizi (SCPs) per la gestione delle autorizzazioni in un'organizzazione AWS. SCPs vengono utilizzati per definire barriere aggiuntive per quali azioni gli utenti possono eseguire e quali. OUs Per impostazione predefinita, AMS fornisce una serie di account SCPs distribuiti in gestione che forniscono protezioni a diversi livelli di unità organizzative predefiniti. Per le restrizioni SCP, contattate il vostro CSDM.

Puoi anche crearne di personalizzati SCPs e allegarli a specifici. OUs Possono essere richiesti dal tuo account di gestione utilizzando il tipo di modifica ct-33ste5yc7hprs. AMS esamina quindi le personalizzazioni richieste prima di applicarle all'obiettivo. SCPs OUs Ad esempio, vedi Account di gestione | Crea account personalizzato OUs e di gestione | Crea SCP personalizzato (automazione gestita).

Scelta di MALZ singoli o multipli MALZs

La tabella seguente fornisce alcune considerazioni di alto livello sulla decisione tra una singola landing zone multiaccount (MALZ) e più zone di atterraggio multi-account (ad esempio, due landing zone multi-account, Prod e non-Prod). In generale, la scelta dipende dalle esigenze individuali, dai requisiti legali e dalle pratiche operative.

Zona di atterraggio singola con più account vs. zone di atterraggio multiple con più account

Entità	Singola landing zone AMS	Zone di atterraggio multiple (due o più)
Costo base	Inferiore, ottimizzato a circa 3.000 dollari al mese.	Più alto, un costo aggiuntivo di circa 3.000 dollari per ambiente.
Fatturazione	Fattura unica, grazie a un unico account di fatturazione/gestione.	Fattura separata per ogni landing zone con più account. Attualmente AWS Org non supporta account multigestione con un'unica fattura.
Portabilità delle istanze riservate esistenti () RIs	Bassa. Al momento, AWS RIs non è convertibile tra più account di fatturazione. Riutilizzeresti l'esistente RIs per una landing zone con più account.	Inferiore. Dovresti riutilizzare e distribuire RIs su tutte le landing zone con più account.
Sconti per livelli di prodotto	Elevato. Vedi Sconti Volume.	Basso. Vedi Sconti Volume.
Sovraccarico di configurazione iniziale (in base alle project/ migration tempistiche)	Basso. Integrazioni con Active Directory, networking e Single Sign-On (SSO) una sola volta.	Elevato. Eseguiresti Active Directory, integrazione di rete e integrazioni SSO per ogni landing zone. Ciò potrebbe causare potenziali ritardi a qualsiasi progetto di migrazione.
Configurabilità dei servizi comuni	Sforzi ridotti. Configurate common/ shared servizi come DNS, backup, monitoraggio, registrazione ecc.	Grandi sforzi. È necessaria una pianificazione aggiuntiva per stabilire dove saranno collocati l'infrastruttura o i servizi comuni. Il traffico che attraversa più gateway di transito (TGWs) in ciascuna landing zone potrebbe comportare costi aggiuntivi.

Entità	Singola landing zone AMS	Zone di atterraggio multiple (due o più)
Scalabilità	Medio. AMS ha attualmente un limite pratico di 150 account per landing zone con più account. Più team o fornitori che eseguono applicazioni sullo stesso account potrebbero avere accesso a stack di proprietà di team diversi. Questa limitazione può essere mitigata controllando l'accesso a stack specifici dell'applicazione a ServiceNo w livello (integrando l'applicazione AMS ServiceNow Connector e utilizzan do i tag). Chiedi ai responsabili della fornitura tecnica di AMS (TDMs) o agli architetti cloud () come implement arloCAs.	Elevato. Possibilità di sfruttare più landing zone multi-account per distribui re i conti ottenendo al contempo un livello di segregazione dell'account o dell'applicazione. La gestione di un numero elevato di account potrebbe comportare spese operative o di costo.
Rischio operativo	(Dipende) Basso. Integrazione operativa e prontezza una sola volta. Meno possibilità di deviazioni dei processi.	(Dipende) Basso. Molteplici attività operative e di integrazione. La deriva in più zone di atterraggio nel corso del periodo potrebbe comportare rischi operativi.
Più regioni AWS	Singola regione AWS. La landing zone multi-account AMS è limitata a una singola regione AWS. Per estendersi su più regioni AWS, utilizza più landing zone multi-account.	Più regioni AWS. Con più zone di destinazione con più account, puoi avere ogni MALZ distribuito in una regione e interconnetterli utilizzando il peering del gateway di transito (TGW).
Migrazione o portabilità dell'account	Sì. È possibile spostare account da un'unità organizzativa all'altra all'inter no della stessa AWS Organization.	No. AMS non supporta la migrazion e di un account tra zone di destinazi one, ovvero tra AWS Organizations. I carichi di lavoro possono raggiungere tutte le zone di atterraggio con Transit Gateway (TGW) o peering VPC.

Entità	Singola landing zone AMS	Zone di atterraggio multiple (due o più)
Gestione delle modifiche	Medio. Apportare modifiche distrutti ve a componenti comuni come TGW, Active Directory (AD) o in uscita (egress) può influire su tutti i carichi di lavoro in una landing zone con più account. Tuttavia, le modifiche ai componenti gestiti da AMS vengono testate internamente e inserite negli aggiornamenti periodici.	Basso. Apportare modifiche distruttive a componenti comuni come TGW, AD o Outbound (egress) può influire solo sui carichi di lavoro in quella specifica landing zone multi-account.
Controlli dei dati e degli accessi	(Dipende) Controllo ridotto se desideri connetterti a reti ADs e reti locali diverse per carichi di lavoro Prod e Non-Prod. Anche la federazio ne SAML, i domini TGW e i gruppi di sicurezza () possono aiutare a implementare i controlli richiesti. SGs	(Dipende) Controllo elevato se desideri connetterti a diverse reti ADs e locali per carichi di lavoro Prod e Non-Prod. Utilizza zone di atterraggio separate per requisiti di conformità rigorosi.
Conformità e sicurezza	(Dipende) Basso se esistono esigenze di conformità rigorose per separare completamente i carichi di lavoro materiali da quelli non materiali. Sono in atto controlli preventivi e investigativi standard AMS.	(Dipende) High As Multi-Account landing zone potrebbe contribuire a soddisfare rigorosi requisiti di conformit à separando completamente i carichi di lavoro materiali da quelli non materiali . Sono in atto controlli preventivi e investigativi standard AMS.

Raccomandazione: senza una rigorosa conformità o una necessità multiregionale, iniziare con una singola landing zone AMS multi-account consentirebbe di raggiungere un buon equilibrio tra costi, sicurezza, eccellenza operativa e complessità della migrazione. Puoi sempre configurare una landing zone aggiuntiva, in caso di vincoli relativi all'account o all'attività.

Landing zone singola con più account vs. landing zone con più account FAQs

Alcune domande frequenti quando si sceglie di configurare una singola landing zone con più account o più zone di atterraggio con più account:

D1: Posso iniziare con una sola landing zone con più account e passare a più landing zone con più account, se si incontrano limiti di account o vincoli aziendali?

R: Sì. Puoi scegliere di configurare un'altra landing zone con più account in qualsiasi momento:

- Sarà necessario configurare un nuovo account di pagamento per la fatturazione (attualmente AWS non supporta account con più paganti in una singola organizzazione AWS).
- La creazione della base Multi-Account Landing Zone richiede fino a 2 settimane di lead time una volta compilato il questionario sulla zona di atterraggio multi-account.
- Ogni landing zone con più account comporta un'aggiunta di circa 3.000 USD al mese per un costo di esercizio.
- Per creare un nuovo MALZ sarà necessaria l'integrazione di N/W, AD, DNS e SSO.
- Eventuali piani Reserved Instances (RIs) e Cost Saving dovranno essere configurati per la nuova landing zone multi-account (non RIs sono trasferibili).
- La landing zone multi-account AMS non supporta la migrazione di un account tra account di landing zone con più account, ad esempio tra AWS Orgs. Tuttavia, è possibile spostare le applicazioni da un account all'altro utilizzando metodi di migrazione standard.

Q2: Qual è l'approccio di AMS a MALZ updates/changes all' underlying/shared infrastruttura e quantifica il rischio per i clienti? Fornisci dettagli sulle garanzie incluse nel processo. In che modo i clienti si rendono conto che MALZ non updates/changes avrà alcun impatto sui clienti? Esistono misure che il Cliente deve adottare per prevenire interruzioni?

R: AMS segue una rigorosa metodologia di modifica utilizzando strumenti interni che ci consentono di definire, rivedere, pianificare ed eseguire modifiche agli ambienti dei clienti.

Il processo di rilascio degli aggiornamenti prevede revisioni del codice, test di integrazione, implementazione in ambienti gamma e beta e tempi di preparazione aggiuntivi e test in ambienti beta e gamma prima del rilascio negli ambienti dei clienti. Tutte le versioni includono procedure di rollback e sono attentamente monitorate dal team addetto ai rilasci e dal team che ha creato e richiesto la modifica. L'ambito delle versioni è limitato agli stack di proprietà e forniti da AMS. In media, eseguiamo almeno una release a settimana.

Inoltre:

- Gli SLA AMS sono applicabili. In base alla descrizione del servizio AMS, qualsiasi incidente sorto a seguito di un'attività di manutenzione a infrarossi condivisa rispetterebbe lo SLA valido per la risoluzione o i crediti.

- I Clienti non richiedono misure preventive speciali per prevenire l'interruzione dell'infrastruttura comune. I clienti dispongono di autorizzazioni di sola lettura per gli account AWS Org o Core OU, quindi non possono apportare modifiche distruttive all'ambiente principale MALZ. Tutte le richieste dei clienti all'infrastruttura Core richiedono la revisione e l'approvazione di AMS.
- I clienti possono testare determinate modifiche a livello di organizzazione, SCPs/Roles ad esempio a livello di account individuali non di produzione, prima di propagarle a livello di unità organizzativa dell'app. La roadmap di AMS prevede l'utilizzo di più APP OUs (secondo trimestre 2020), il che ridurrebbe ulteriormente il rischio di apportare alcune modifiche a livello di ORG. Il team MALZ ha già rilasciato un'unità organizzativa separata per gli account «Build Mode», per garantire una chiara separazione della proprietà del cliente e dei controlli separati.
- La maggior parte di queste sono modifiche che consentono ad AMS di gestire il carico di lavoro in modo efficace ed efficiente e non influiscono necessariamente sul carico di lavoro dei clienti. Laddove AMS ritenga che una modifica condivisa dell'infrastruttura possa avere un impatto sul carico di lavoro dei clienti, viene quindi allineata alla finestra di modifica dei clienti.

Raccomandazione di alto livello, inizia con più zone di atterraggio con più account se:

- Se ti aiuta a raggiungere una conformità specifica.
- Se è necessario utilizzare Multi-Region.
- Se disponi di carichi di lavoro locali ADs e reti diverse per carichi di lavoro diversi da Prod/Material quelli non presenti. Prod/Non-Material workloads, to clearly segregate b/w

Account Multi-Account Landing Zone

Argomenti

- Gestione dell'account
- Account di rete
- Account Shared Services
- Account Log Archive
- Account di sicurezza
- Tipi di account dell'applicazione
- Account AMS Tools (migrazione dei carichi di lavoro)

Gestione dell'account

L'account di gestione è il tuo account AWS iniziale quando inizi l'onboarding con AMS. Utilizza AWS Organizations come account di gestione (noto anche come account di pagamento che paga gli addebiti di tutti gli account dei membri), che consente all'account di creare e gestire finanziariamente gli account dei membri. Contiene il framework AWS landing zone (ALZ), i set di stack di configurazione degli account, le policy di controllo dei servizi di AWS Organization (SCPs), ecc.

Per ulteriori informazioni sull'utilizzo di un account di gestione, consulta Best practice per l'account di gestione.

Il diagramma seguente fornisce una panoramica di alto livello delle risorse contenute nell'account di gestione.

Risorse nell'account di gestione

Oltre ai servizi standard di cui sopra, durante l'onboarding non vengono create risorse AWS aggiuntive nell'account di gestione. I seguenti input sono richiesti durante l'onboarding su AMS:

- ID dell'account di gestione: ID dell'account AWS creato inizialmente da te.
- Email relative agli account principali: fornisci le e-mail da associare a ciascuno degli account principali: account di rete, servizi condivisi, registrazione e sicurezza.
- Regione di servizio: fornisci la regione AWS in cui verranno distribuite tutte le risorse della tua landing zone AMS.

Account di rete

L'account Networking funge da hub centrale per il routing di rete tra gli account di landing zone con più account AMS, la rete locale e il traffico in uscita verso Internet. Inoltre, questo account contiene bastioni DMZ pubblici che rappresentano il punto di ingresso per gli ingegneri AMS per accedere agli host nell'ambiente AMS. Per i dettagli, consultate il seguente diagramma di alto livello dell'account di rete riportato di seguito.

Architettura degli account di rete

Il diagramma seguente illustra l'ambiente di landing zone multi-account AMS, mostra i flussi di traffico di rete tra gli account ed è un esempio di configurazione ad alta disponibilità.

AMS configura per te tutti gli aspetti del networking in base ai nostri modelli standard e alle opzioni selezionate fornite durante l'onboarding. Al tuo account AWS viene applicato un design di rete AWS standard e viene creato un VPC per te e connesso ad AMS tramite VPN o Direct Connect. Per ulteriori informazioni su Direct Connect, consulta AWS Direct Connect. Lo standard VPCs include la DMZ, i servizi condivisi e una sottorete di applicazioni. Durante il processo di onboarding, VPCs potrebbero essere richiesti e creati altri dati in base alle esigenze dell'utente (ad esempio, divisioni clienti, partner). Dopo l'onboarding, viene fornito un diagramma di rete: un documento ambientale che spiega come è stata configurata la rete.

> **Note**
>
> Per informazioni sui limiti e i vincoli di servizio predefiniti per tutti i servizi attivi, consulta la documentazione di AWS Service Limits.

Il design della nostra rete si basa sul «Principio del minimo privilegio» di Amazon. A tal fine, indirizziamo tutto il traffico, in ingresso e in uscita, attraverso una DMZ, ad eccezione del traffico proveniente da una rete affidabile. L'unica rete affidabile è quella configurata tra l'ambiente locale e il VPC tramite l'uso di una and/or VPN e AWS Direct Connect (DX). L'accesso è garantito tramite l'uso di istanze bastion, impedendo così l'accesso diretto a qualsiasi risorsa di produzione. Tutte le applicazioni e le risorse risiedono all'interno di sottoreti private raggiungibili tramite sistemi di bilanciamento del carico pubblici. Il traffico pubblico in uscita attraversa i gateway NAT nel VPC in uscita (nell'account di rete) verso l'Internet Gateway e quindi verso Internet. In alternativa, il traffico può fluire attraverso la tua VPN o Direct Connect verso il tuo ambiente locale.

Connettività di rete privata all'ambiente di landing zone multi-account AMS

AWS offre connettività privata tramite connettività di rete privata virtuale (VPN) o linee dedicate con AWS Direct Connect. La connettività privata nell'ambiente con più account viene configurata utilizzando uno dei metodi descritti di seguito:

- Connettività Edge centralizzata tramite Transit Gateway
- Connessione della and/or VPN Direct Connect (DX) agli account cloud privati virtuali () VPCs

Connettività edge centralizzata tramite gateway di transito

AWS Transit Gateway è un servizio che ti consente di connettere le tue reti VPCs e quelle locali a un unico gateway. Transit gateway (TGW) può essere utilizzato per consolidare la connettività edge esistente e indirizzarla attraverso un unico punto. ingress/egress Il gateway di transito viene creato nell'account di rete dell'ambiente multi-account AMS. Per ulteriori dettagli sul gateway di transito, consulta AWS Transit Gateway.

Il gateway AWS Direct Connect (DX) viene utilizzato per connettere la connessione DX tramite un'interfaccia virtuale di transito a VPCs o VPNs che sono collegati al gateway di transito. È possibile associare un gateway Direct Connect al gateway di transito. Quindi, crea un'interfaccia virtuale di transito per la tua connessione AWS Direct Connect al gateway Direct Connect. Per informazioni sulle interfacce virtuali DX, consulta Interfacce virtuali AWS Direct Connect.

Questa configurazione offre i seguenti vantaggi. Puoi:

- Gestisci una singola connessione per più connessioni VPCs o VPNs che si trovano nella stessa regione AWS.
- Pubblicizza prefissi da locale ad AWS e da AWS a locale.

> **Note**
>
> Per informazioni sull'utilizzo di un DX con i servizi AWS, consulta la sezione Resiliency Toolkit Classic. Per ulteriori informazioni, consulta Associazioni Transit Gateway.

Per aumentare la resilienza della tua connettività, ti consigliamo di collegare almeno due interfacce virtuali di transito da diverse postazioni AWS Direct Connect al gateway Direct Connect. Per ulteriori informazioni, consulta la raccomandazione sulla resilienza di AWS Direct Connect.

Connessione di DX o VPN all'account VPCs

Con questa opzione, gli ambienti VPCs di landing zone con più account AMS sono collegati direttamente a Direct Connect o VPN. Il traffico fluisce direttamente VPCs da Direct Connect o VPN senza attraversare il gateway di transito.

Risorse nell'account di rete

Come illustrato nello schema degli account di rete, i seguenti componenti vengono creati nell'account e richiedono l'input dell'utente.

L'account Networking ne contiene due VPCs: Egress VPC e DMZ VPC, noto anche come VPC perimetrale.

Gestore di rete AWS

AWS Network Manager è un servizio che consente di visualizzare le reti di gateway di transito (TGW) senza costi aggiuntivi per AMS. Fornisce il monitoraggio centralizzato della rete sia sulle risorse AWS che sulle reti locali, un'unica visione globale della rete privata in un diagramma topologico e in una mappa geografica e metriche di utilizzo, come lo stato della connessione in byte. in/out, packets in/out, packets dropped, and alerts for changes in the topology, routing, and up/down Per informazioni, consulta AWS Network Manager.

Utilizza uno dei seguenti ruoli per accedere a questa risorsa:

- AWSManagedServicesCaseRole
- AWSManagedServicesReadOnlyRole
- AWSManagedServicesChangeManagementRole

VPC in uscita

L'Egress VPC viene utilizzato principalmente per il traffico in uscita verso Internet ed è composto da sottoreti in un massimo public/private di tre zone di disponibilità (). AZs I gateway NAT (Network Address Translation) vengono forniti nelle sottoreti pubbliche e gli allegati VPC del gateway di transito (TGW) vengono creati nelle sottoreti private. Il traffico Internet in uscita, o in uscita, proveniente da tutte le reti entra attraverso la sottorete privata tramite TGW, dove viene quindi indirizzato a un NAT tramite le tabelle di routing VPC.

Per i tuoi VPCs che contengono applicazioni rivolte al pubblico in una sottorete pubblica, il traffico proveniente da Internet è contenuto all'interno di quel VPC. Il traffico di ritorno non viene instradato al VPC TGW o Egress, ma reindirizzato attraverso il gateway Internet (IGW) nel VPC.

> **Note**
>
> Intervallo CIDR VPC di rete: quando si crea un VPC, è necessario specificare un intervallo di indirizzi IPv4 per il VPC sotto forma di blocco CIDR (Classless Inter-Domain Routing), ad esempio 10.0.16.0/24. Si tratta del blocco CIDR principale per il VPC.
> Il team di AMS multi-account landing zone consiglia l'intervallo di 24 (con più indirizzi IP) per fornire un certo margine nel caso in cui altre risorse/apparecchiature vengano utilizzate in futuro.

VPC perimetrale (DMZ)

Il VPC Perimeter, o DMZ, contiene le risorse necessarie ai tecnici operativi AMS per accedere alle reti AMS. Contiene sottoreti pubbliche su 2-3 file AZs, con host SSH Bastions in un gruppo di Auto Scaling (ASG) a cui gli ingegneri di AMS Operations possono accedere o effettuare il tunneling. I gruppi di sicurezza collegati ai bastioni DMZ contengono regole in entrata sulla porta 22 di Amazon Corp Networks.

Intervallo CIDR VPC DMZ: quando si crea un VPC, è necessario specificare un intervallo di indirizzi IPv4 per il VPC sotto forma di blocco CIDR (Classless Inter-Domain Routing), ad esempio 10.0.16.0/24. Si tratta del blocco CIDR principale per il VPC.

> **Note**
>
> Il team AMS consiglia l'intervallo di 24 (con più indirizzi IP) per fornire un buffer nel caso in cui altre risorse, come un firewall, vengano implementate in futuro.

AWS Transit Gateway

AWS Transit Gateway (TGW) è un servizio che consente di connettere Amazon Virtual Private Clouds (VPCs) e le reti locali a un unico gateway. Transit gateway è la spina dorsale di rete che gestisce il routing tra reti di account AMS e reti esterne. Per informazioni su Transit Gateway, consulta AWS Transit Gateway.

Fornisci il seguente input per creare questa risorsa:

- Numero ASN del Transit Gateway *: Fornisci l'Autonomous System Number (ASN) privato per il tuo gateway di transito. Dovrebbe essere l'ASN del lato AWS di una sessione Border Gateway Protocol (BGP). L'intervallo è compreso tra 64512 e 65534 per 16 bit. ASNs

Account Shared Services

L'account Shared Services funge da hub centrale per la maggior parte dei servizi del piano dati AMS. L'account contiene l'infrastruttura e le risorse necessarie per la gestione degli accessi (AD), la gestione della sicurezza degli endpoint (Trend Micro) e contiene i bastioni dei clienti (SSH/RDP). Una panoramica di alto livello delle risorse contenute in Shared Services Account è mostrata nel grafico seguente.

Il VPC di Shared Services è composto dalla sottorete AD, dalla sottorete EPS e dalla sottorete Customer Bastions nelle tre zone di disponibilità (). AZs Le risorse create nel VPC di Shared Services sono elencate di seguito e richiedono l'input dell'utente.

- Intervallo CIDR VPC di Shared Services: quando si crea un VPC, è necessario specificare un intervallo di indirizzi IPv4 per il VPC sotto forma di blocco CIDR (Classless Inter-Domain Routing), ad esempio 10.0.1.0/24. Questo è il blocco CIDR principale per il tuo VPC.

  > **Note**
  >
  > Il team AMS consiglia l'intervallo di /23.

- Dettagli su Active Directory: Microsoft Active Directory (AD) viene utilizzato per la user/resource gestione, l'autenticazione/autorizzazione e il DNS in tutti gli account di landing zone con più account AMS. AMS AD è inoltre configurato con un trust unidirezionale con Active Directory per l'autenticazione basata sulla fiducia. Per creare l'AD è necessario il seguente input:
  - Domain Fully Qualified Domain Name (FQDN): il nome di dominio completo per la directory AWS Managed Microsoft AD. Il dominio non deve essere un dominio esistente o un dominio figlio di un dominio esistente nella rete.
  - Nome NetBIOS di dominio: se non si specifica un nome NetBIOS, AMS imposta come impostazione predefinita il nome sulla prima parte del DNS della directory. Ad esempio, corp per la directory DNS corp.example.com.

- Trend Micro — endpoint protection security (EPS): Trend Micro endpoint protection (EPS) è il componente principale di AMS per la sicurezza del sistema operativo. Il sistema è composto da Deep Security Manager (DSM), istanze EC2, istanze EC2 relay e un agente presente in tutti i piani dati e nelle istanze EC2 dei clienti.

  È necessario assumerlo `EPSMarketplaceSubscriptionRole` nell'account Shared Services e sottoscrivere l'AMI Trend Micro Deep Security (BYOL) o Trend Micro Deep Security (Marketplace).

  Per creare EPS sono necessari i seguenti input predefiniti (se si desidera modificare i valori predefiniti):

  - Tipo di istanza di inoltro: Valore predefinito - m5.large
  - Tipo di istanza DSM: valore predefinito - m5.xlarge
  - Dimensione dell'istanza DB: valore predefinito: 200 GB
  - Tipo di istanza RDS: valore predefinito - db.m5.large

- Bastioni per i clienti: nell'account Shared Services sono disponibili i bastioni SSH o RDP (o entrambi) per accedere ad altri host nell'ambiente AMS. Per accedere alla rete AMS come utente (SSH/RDP), you must use "customer" Bastions as the entry point. The network path originates from the on-premise network, goes through DX/VPNverso il gateway di transito (TGW), quindi viene indirizzato al VPC di Shared Services. Una volta che sei in grado di accedere al bastione, puoi passare ad altri host nell'ambiente AMS, a condizione che la richiesta di accesso sia stata accolta.
  - I seguenti input sono necessari per i bastioni SSH.
    - Capacità desiderata dell'istanza SSH Bastion: valore predefinito - 2.
    - Numero massimo di istanze SSH Bastion: valore predefinito - 4.
    - Istanze minime SSH Bastion: valore predefinito -2.
    - Tipo di istanza SSH Bastion: Valore predefinito - m5.large (può essere modificato per risparmiare sui costi, ad esempio t3.medium).
    - SSH Bastion Ingress CIDRs: intervalli di indirizzi IP da cui gli utenti della rete accedono a SSH Bastions.
  - I seguenti input sono necessari per i bastioni RDP di Windows.
    - Tipo di istanza RDP Bastion: Valore predefinito - t3.medium.
    - Sessioni minime desiderate per RDP Bastion: valore predefinito - 2.
    - Sessioni massime RDP: valore predefinito -10.
    - Tipo di configurazione RDP Bastion: puoi scegliere una delle seguenti configurazioni

    - SecureStandard = Un utente riceve un bastione e solo un utente può connettersi al bastione.
    - SecureHA = Un utente riceve due bastioni in due diverse AZ a cui connettersi e solo un utente può connettersi al bastione.
    - SharedStandard = Un utente riceve un bastione a cui connettersi e due utenti possono connettersi contemporaneamente allo stesso bastione.
    - SharedHA = Un utente riceve due bastioni in due diverse AZ a cui connettersi e due utenti possono connettersi contemporaneamente allo stesso bastione.
- Customer RDP Ingress CIDRs: intervalli di indirizzi IP da cui gli utenti della rete accederanno a RDP Bastions.

Aggiornamenti ai servizi condivisi: Multi-Account Landing Zone

AMS applica i rilasci del piano dati agli account gestiti su base mensile, senza preavviso.

AMS utilizza l'unità organizzativa principale per fornire servizi condivisi come accesso, rete, EPS, archiviazione dei log e aggregazione degli avvisi nella Multi-Account Landing Zone. AMS è responsabile della risoluzione delle vulnerabilità, dell'applicazione di patch e dell'implementazione di questi servizi condivisi. AMS aggiorna regolarmente le risorse utilizzate per fornire questi servizi condivisi in modo che gli utenti abbiano accesso alle funzionalità più recenti e agli aggiornamenti di sicurezza. Gli aggiornamenti avvengono in genere su base mensile. Le risorse che fanno parte di questi aggiornamenti sono:

- Account che fanno parte dell'unità organizzativa principale.

  L'account di gestione, l'account di servizi condivisi, l'account di rete, l'account di sicurezza e l'account di archiviazione dei registri dispongono di risorse per i bastioni RDP e SSH, i proxy, gli host di gestione e la sicurezza degli endpoint (EPS), che in genere vengono aggiornati ogni mese. AMS utilizza EC2 implementazioni immutabili come parte dell'infrastruttura di servizi condivisi.
- Nuovo AMS che AMIs incorpora gli ultimi aggiornamenti.

> **Note**
>
> Gli operatori AMS utilizzano un tipo di modifica della soppressione degli allarmi (CT) interno quando eseguono modifiche al piano dati e la relativa RFC viene visualizzata nell'elenco RFC. Questo perché, quando viene implementata la versione del piano dati, diverse infrastrutture possono essere chiuse, riavviate, messe offline oppure possono

verificarsi picchi di CPU o altri effetti dell'implementazione che attivano allarmi che, durante l'implementazione del piano dati, sono estranei. Una volta completata l'implementazione, viene verificato il corretto funzionamento di tutta l'infrastruttura e gli allarmi vengono riattivati.

Account Log Archive

L'account Log Archive funge da hub centrale per l'archiviazione dei log nell'ambiente di landing zone multi-account AMS. Nell'account è presente un bucket S3 che contiene copie dei file di log di AWS CloudTrail e AWS Config da ciascuno degli account dell'ambiente di landing zone multi-account AMS. Puoi utilizzare questo account per la tua soluzione di registrazione centralizzata con AWS Firehose o Splunk e così via. L'accesso di AMS a questo account è limitato a pochi utenti; limitato ai revisori e ai team di sicurezza per la conformità e le indagini forensi relative all'attività dell'account.

Account di sicurezza

L'account Security è l'hub centrale per le operazioni relative alla sicurezza degli alloggi e il punto principale per l'inoltro di notifiche e avvisi ai servizi del piano di controllo AMS. Inoltre, l'account Security ospita l'account di gestione Amazon Guard Duty e l'aggregatore AWS Config.

Tipi di account dell'applicazione

Gli account applicativi sono account AWS all'interno dell'architettura di landing zone gestita da AMS che usi per ospitare i tuoi carichi di lavoro. AMS offre tre tipi di account applicativi:

- Account applicativi gestiti da AMS
- conti AMS Accelerate
- Account applicativi gestiti dal cliente

Gli account delle applicazioni sono raggruppati in diversi OUs in AWS Organizations a seconda del tipo di account dell'applicazione:

- Unità organizzativa root:
  1. Applicazioni OU
     - Unità organizzativa gestita: account gestiti da AMS

    - Unità organizzativa di sviluppo: account gestiti da AMS con modalità sviluppatore abilitata
2. Accelerazione dell'unità operativa: account AMS Accelerate
3. Unità organizzativa gestita dal cliente: account applicativi gestiti dal cliente

Il provisioning degli account delle applicazioni viene effettuato tramite una richiesta RFC inviata dall'account di gestione:

- Crea un account applicativo con VPC ct-1zdasmc2ewzrs
- Crea un account Accelerate ct-2p93tyd5angmi
- Crea un account applicativo gestito dal cliente ct-3pwbixz27n3tn

Account applicativi gestiti da AMS

Gli account applicativi completamente gestiti da AMS sono denominati account applicativi gestiti da AMS, in cui alcune o tutte le attività operative, come la gestione delle richieste di servizio, la gestione degli incidenti, la gestione della sicurezza, la gestione della continuità (backup), la gestione delle patch, l'ottimizzazione dei costi o il monitoraggio e la gestione degli eventi dell'infrastruttura, vengono eseguite da AMS.

La quantità di attività eseguite da AMS dipende dalla modalità di gestione delle modifiche selezionata. Gli account gestiti da AMS supportano diverse modalità di gestione delle modifiche:

- modalità RFC
- Modalità Direct Change in AMS
- AMS e AWS Service Catalog
- Modalità AMS Advanced Developer
- Modalità Self-Service Provisioning in AMS

Per ulteriori informazioni sulla gestione delle modifiche e sulle diverse modalità, consulta. Modifiche alle modalità di gestione

Esistono alcuni servizi AWS che puoi utilizzare nel tuo account gestito da AMS senza la gestione di AMS. L'elenco di questi servizi AWS e come aggiungerli al tuo account AMS sono descritti nella sezione Self-service provisioning.

conti AMS Accelerate

AMS Accelerate è il piano operativo AMS in grado di gestire l'infrastruttura AWS che supporta i carichi di lavoro. Puoi beneficiare dei servizi operativi di AMS Accelerate come il monitoraggio e gli avvisi, la gestione degli incidenti, la gestione della sicurezza e la gestione dei backup, senza dover effettuare una nuova migrazione, subire interruzioni o modificare il modo in cui utilizzi AWS. AMS Accelerate offre anche un componente aggiuntivo opzionale per carichi di lavoro EC2 basati che richiedono patch regolari.

Con AMS Accelerate hai la libertà di usare, configurare e distribuire tutti i servizi AWS in modo nativo o con i tuoi strumenti preferiti. Utilizzerai i tuoi meccanismi di accesso e modifica preferiti, mentre AMS applica costantemente pratiche collaudate che aiutano a scalare il tuo team, ottimizzare i costi, aumentare la sicurezza e l'efficienza e migliorare la resilienza.

> **Note**
>
> Gli account AMS Accelerate in AMS Advanced non dispongono di AMS change management (RFCs) o della console AMS Advanced. Dispongono invece della console e della funzionalità AMS Accelerate.

È possibile effettuare il provisioning degli account Accelerate solo dal tuo account AMS multi-account landing zone Management. Accelerate offre diverse funzionalità operative. Per ulteriori informazioni, consulta la descrizione del servizio Accelerate.

- Continuerai a usufruire di alcune delle funzionalità degli account principali multi-account landing zone (MALZ) come la registrazione centralizzata, la fatturazione singola, Config Aggregator nell'account di sicurezza e. SCPs
- AMS Accelerate non fornisce alcuni servizi AMS Advanced come EPS, gestione degli accessi, gestione delle modifiche e provisioning. Ti consigliamo di seguire i passaggi successivi per accedere e configurare il gateway di transito (TGW).

Per maggiori dettagli su Accelerate, consulta Cos'è Accelerate.

Creazione del tuo account Accelerate

Per creare un account Accelerate, segui i passaggi descritti qui Crea un account Accelerate.

Accedere al tuo account Accelerate

Dopo aver effettuato il provisioning di un account Accelerate nel tuo account multi-account landing zone (MALZ), devi assumere un ruolo con autorizzazioni di accesso amministrativo nell'account. `AccelerateDefaultAdminRole`

Per accedere al nuovo account Accelerate:

1. Accedi alla console IAM per l'account di gestione con il `CustomerDefaultAssumeRole` ruolo.
2. Nella console IAM, nella barra di navigazione, scegli il tuo nome utente.
3. Seleziona Switch Role (Cambia ruolo). Se è la prima volta che scegli questa opzione, verrà visualizzata una pagina con ulteriori informazioni. Dopo la lettura, scegli Switch Role (Passaggio di ruolo). Se si cancellano i cookie del browser, questa pagina potrebbe apparire di nuovo.
4. Nella pagina Cambia ruolo, digita l'ID dell'account Accelerate e il nome del ruolo da assumere:`AccelerateDefaultAdminRole`.

Ora che hai accesso, puoi creare nuovi ruoli IAM per continuare ad accedere al tuo ambiente. Se desideri utilizzare SAML Federation per il tuo account Accelerate, consulta Abilitare gli utenti federati SAML 2.0 ad accedere alla Console di gestione AWS.

Connessione del tuo account Accelerate con Transit Gateway

AMS non gestisce la configurazione di rete di un account Accelerate. Hai la possibilità di gestire la tua rete utilizzando AWS APIs (vedi Networking Solutions) o di connetterti alla rete MALZ gestita da AMS, utilizzando il Transit Gateway (TGW) esistente distribuito in AMS MALZ.

> **Note**
>
> Puoi avere un VPC collegato al TGW solo se l'account Accelerate si trova nella stessa regione AWS. Per ulteriori informazioni, consulta Transit gateways.

Per aggiungere il tuo account Accelerate a Transit Gateway, richiedi una nuova rotta utilizzando il tipo di modifica Deployment | Managed landing zone | Networking account | Aggiungi route statica (ct-3r2ckznmt0a59), includi queste informazioni:

- Blackhole: ha valore True per indicare che la destinazione del percorso non è disponibile. Esegui questa operazione quando il traffico per la route statica deve essere interrotto dal Transit Gateway.

Se ha valore False, indirizzerà il traffico verso l'ID dell'allegato TGW specificato. Il valore predefinito è false.

- DestinationCidrBlock: L'intervallo IPV4 CIDR utilizzato per le corrispondenze di destinazione. Le decisioni di instradamento si basano sulla corrispondenza più specifica. Esempio: 10.0.2.0/24.
- TransitGatewayAttachmentId: L'ID dell'allegato TGW che fungerà da destinazione della tabella delle rotte. Se Blackhole è false, questo parametro è obbligatorio, altrimenti lascia questo parametro vuoto. Esempio: tgw-attach-04eb40d1e14ec7272.
- TransitGatewayRouteTableId: L'ID della tabella delle rotte TGW. Esempio: tgw-rtb-06ddc751c0c0c881c.

Crea percorsi nelle tabelle delle rotte TGW per connetterti a questo VPC:

1. Per impostazione predefinita, questo VPC non sarà in grado di comunicare con nessun altro VPC VPCs nella rete MALZ.
2. Decidi con il tuo architetto di soluzioni con cosa VPCs vuoi che comunichi questo Accelerate VPC.
3. Invia una distribuzione | Managed landing zone | Account di rete | Aggiungi il tipo di modifica della route statica (ct-3r2ckznmt0a59), includi queste informazioni:
   - Blackhole: il valore True indica che la destinazione del percorso non è disponibile. Esegui questa operazione quando il traffico per la route statica deve essere interrotto dal Transit Gateway. Se ha valore False, indirizzerà il traffico verso l'ID dell'allegato TGW specificato. Il valore predefinito è false.
   - DestinationCidrBlock: L'intervallo IPV4 CIDR utilizzato per le corrispondenze di destinazione. Le decisioni di instradamento si basano sulla corrispondenza più specifica. Esempio: 10.0.2.0/24.
   - TransitGatewayAttachmentId: L'ID dell'allegato TGW che fungerà da destinazione della tabella delle rotte. Se Blackhole è false, questo parametro è obbligatorio, altrimenti lascia questo parametro vuoto. Esempio: tgw-attach-04eb40d1e14ec7272.
   - TransitGatewayRouteTableId: L'ID della tabella delle rotte TGW. Esempio: tgw-rtb-06ddc751c0c0c881c.

Collegamento di un nuovo account VPC Accelerate alla rete AMS Multi-Account Landing Zone (creazione di un allegato VPC TGW):

1. Nel tuo account di rete per landing zone multi-account, apri la console Amazon VPC.

2. Nel riquadro di navigazione, selezionare Transit Gateways (Gateway di transito). Registra l'ID TGW del gateway di transito che vedi.
3. Nel tuo account Accelerate, apri la console Amazon VPC.
4. Nel pannello di navigazione, scegli Transit Gateway Attachments > Create Transit Gateway Attachments. Effettua le seguenti scelte:
   - Per il Transit Gateway ID, scegli l'ID del gateway di transito che hai registrato nella fase 2.
   - In Attachment type (Tipo collegamento), selezionare VPC.
   - In VPC Attachment (Collegamento VPC), indicare facoltativamente un nome per il campo Attachment name tag (Tag nome collegamento).
   - Scegli se abilitare DNS Support and IPv6 Support.
   - Per VPC ID (ISD VPC), scegliere il VPC da collegare al gateway di transito. Questo VPC deve possedere almeno una sottorete associata ad esso.
   - Per Subnet IDs, seleziona una sottorete per ogni zona di disponibilità da utilizzare dal gateway di transito per instradare il traffico. È necessario selezionare almeno una sottorete. È possibile selezionare solo una sottorete per ogni zona di disponibilità.
5. Selezionare Create attachment (Crea collegamento). Registra l'ID dell'allegato TGW appena creato.

Associazione dell'allegato TGW a una tabella di routing:

1. Decidi a quale tabella di routing TGW vuoi associare il VPC. Ti consigliamo di creare una nuova tabella di routing dell'applicazione per l'account Accelerate VPCs utilizzando Deployment | Managed landing zone | Account di rete | Crea il tipo di modifica della tabella delle rotte del gateway di transito (ct-3dscwaeyi6cup).
2. Invia un RFC Management | Managed landing zone | Networking account | Associa l'allegato TGW (ct-3nmhh0qr338q6) all'account di rete per associare l'allegato VPC o TGW alla tabella di percorso selezionata.

Crea percorsi nelle tabelle delle rotte TGW per connetterti a questo VPC:

1. Per impostazione predefinita, questo VPC non sarà in grado di comunicare con nessun altro VPC VPCs nella tua rete di landing zone multi-account.
2. Decidi con il tuo architetto di soluzioni con cosa VPCs vuoi che comunichi questo account VPC di Accelerate.

3. Invia un Deployment | Managed landing zone | Account di rete | Aggiungi una route statica (ct-3r2ckznmt0a59) RFC all'account di rete per creare le rotte TGW di cui hai bisogno.

Configurazione delle tabelle di routing VPC in modo che puntino al gateway di transito multi-account AMS per le landing zone:

1. Decidi con il tuo architetto di soluzioni quale traffico inviare al gateway di transito AMS Multi-Account Landing Zone.
2. Invia un Deployment | Managed landing zone | Account di rete | Aggiungi una route statica (ct-3r2ckznmt0a59) RFC all'account di rete per creare le rotte TGW di cui hai bisogno.

Account applicativi gestiti dal cliente

Puoi creare account che AMS non gestisce nel modo standard. Questi account sono denominati account gestiti dai clienti e ti danno il pieno controllo per gestire autonomamente l'infrastruttura all'interno degli account, sfruttando al contempo i vantaggi dell'architettura centralizzata gestita da AMS.

Gli account gestiti dal cliente non hanno accesso alla console AMS o a nessuno dei servizi che forniamo (patch, backup e così via).

Gli account gestiti dai clienti possono essere forniti solo dal tuo account di gestione delle landing zone multi-account AMS.

Diverse modalità AMS funzionano con gli account delle applicazioni in modo diverso; per ulteriori informazioni sulle modalità, consulta le modalità di AWS Managed Services.

Per creare un account applicativo gestito dal cliente, consulta Account di gestione | Crea account di applicazione gestito dal cliente.

Per eliminare un account di applicazione gestito dal cliente, utilizza Account di gestione | Account applicativo offboard. (Il Confirm Offboarding CT non si applica agli account delle applicazioni gestite dal cliente.)

Accesso al tuo account gestito dai clienti

Dopo aver effettuato il provisioning di un account gestito dal cliente (CMA) in una landing zone multi-account, nell'account (MALZ) viene assegnato un ruolo di

amministratore`CustomerDefaultAdminRole`, da assumere, tramite la federazione SAML, per configurare l'account.

Per accedere al CMA:

1. Accedi alla console IAM per l'account di gestione con il CustomerDefaultAssumeRoleruolo.
2. Nella console IAM, nella barra di navigazione, scegli il tuo nome utente.
3. Seleziona Switch Role (Cambia ruolo). Se è la prima volta che scegli questa opzione, verrà visualizzata una pagina con ulteriori informazioni. Dopo la lettura, scegli Switch Role (Passaggio di ruolo). Se si cancellano i cookie del browser, questa pagina potrebbe apparire di nuovo.
4. Nella pagina Cambia ruolo, digita l'ID dell'account gestito dal cliente e il nome del ruolo da assumere: CustomerDefaultAdminRole.

Ora che hai accesso, puoi creare nuovi ruoli IAM per continuare ad accedere al tuo ambiente. Se desideri utilizzare SAML Federation per il tuo account CMA, consulta Abilitare gli utenti federati SAML 2.0 ad accedere alla Console di gestione AWS.

Connessione del CMA con Transit Gateway

AMS non gestisce la configurazione di rete degli account gestiti dal cliente (CMAs). Hai la possibilità di gestire la tua rete utilizzando AWS APIs (vedi Networking Solutions) o di connetterti alla rete di landing zone multi-account gestita da AMS, utilizzando il Transit Gateway (TGW) esistente distribuito in AMS MALZ.

> **Note**
>
> Puoi avere un VPC collegato al TGW solo se il CMA si trova nella stessa regione AWS. Per ulteriori informazioni, consulta Transit gateways.

Per aggiungere il tuo CMA a Transit Gateway, richiedi una nuova rotta con l'account di rete | Aggiungi route statica (ct-3r2ckznmt0a59) modifica il tipo e includi queste informazioni:

- Blackhole: True indica che la destinazione del percorso non è disponibile. Esegui questa operazione quando il traffico per la route statica deve essere interrotto dal Transit Gateway. Se ha valore False, indirizzerà il traffico verso l'ID dell'allegato TGW specificato. Il valore predefinito è false.

- DestinationCidrBlock: L'intervallo IPV4 CIDR utilizzato per le corrispondenze di destinazione. Le decisioni di instradamento si basano sulla corrispondenza più specifica. Esempio: `10.0.2.0/24`.
- TransitGatewayAttachmentId: L'ID allegato TGW che fungerà da destinazione della tabella di routing. Se Blackhole è false, questo parametro è obbligatorio, altrimenti lascia vuoto questo parametro. Esempio: `tgw-attach-04eb40d1e14ec7272`.
- TransitGatewayRouteTableId: L'ID della tabella delle rotte TGW. Esempio: `tgw-rtb-06ddc751c0c0c881c`.

Connessione di un nuovo VPC gestito dal cliente alla rete AMS Multi-Account Landing Zone (creazione di un allegato VPC TGW):

1. Nel tuo account di rete per landing zone multi-account, apri la console Amazon VPC.
2. Nel pannello di navigazione, scegli Transit Gateways. Registra l'ID TGW del gateway di transito che vedi.
3. Nel tuo account Customer Managed, apri la console Amazon VPC.
4. Nel pannello di navigazione, scegli Transit Gateway Attachments > Create Transit Gateway Attachments. Effettua le seguenti scelte:
    a. Per il Transit Gateway ID, scegli l'ID del gateway di transito che hai registrato nella fase 2.
    b. In Attachment type (Tipo collegamento), selezionare VPC.
    c. In VPC Attachment (Collegamento VPC), indicare facoltativamente un nome per il campo Attachment name tag (Tag nome collegamento).
    d. Scegli se abilitare DNS Support and IPv6 Support.
    e. Per VPC ID (ISD VPC), scegliere il VPC da collegare al gateway di transito. Questo VPC deve possedere almeno una sottorete associata ad esso.
    f. Per Subnet IDs, seleziona una sottorete per ogni zona di disponibilità da utilizzare dal gateway di transito per instradare il traffico. È necessario selezionare almeno una sottorete. È possibile selezionare solo una sottorete per ogni zona di disponibilità.
5. Selezionare Create attachment (Crea collegamento). Registra l'ID dell'allegato TGW appena creato.

Associazione dell'allegato TGW a una tabella di routing:

Decidi a quale tabella di routing TGW vuoi associare il VPC. Consigliamo di creare una nuova tabella di routing dell'applicazione per Customer Managed VPCs inviando un RFC Deployment | Managed landing zone | Networking account | Create transit gateway route table (ct-3dscwaeyi6cup). Per associare l'allegato VPC o TGW alla tabella di percorso selezionata, invia un RFC Deployment | Managed landing zone | Networking | Associate TGW attachment (ct-3nmhh0qr338q6) sull'account Networking.

Crea percorsi nelle tabelle delle rotte TGW per connetterti a questo VPC:

1. Per impostazione predefinita, questo VPC non sarà in grado di comunicare con nessun altro VPCs nella tua rete Multi-Account Landing Zone.
2. Decidi con il tuo architetto di soluzioni con cosa VPCs vuoi che comunichi questo VPC gestito dal cliente. Invia un Deployment | Managed landing zone | Account di rete | Aggiungi una route statica (ct-3r2ckznmt0a59) RFC all'account di rete per creare le rotte TGW di cui hai bisogno.

> **Note**
>
> Questo CT (ct-3r2ckznmt0a59) non consente l'aggiunta di route statiche alla tabella di routing principale EgressRouteDomain; se il CMA deve consentire il traffico in uscita, invia una RFC Management | Other | Other (MOO) con ct-0xdawir96cy7k.

Configurazione delle tabelle di routing VPC in modo che puntino al gateway di transito AMS Multi-Account Landing Zone:

Decidi con il tuo architetto di soluzioni quale traffico inviare al gateway di transito AMS Multi-Account Landing Zone. Aggiorna le tabelle di routing VPC per inviare traffico all'allegato TGW creato in precedenza

Ottenere assistenza operativa con i tuoi account gestiti dai clienti

AMS può aiutarti a gestire i carichi di lavoro implementati nei tuoi account Customer Managed integrando l'account in AMS Accelerate. Con AMS Accelerate puoi beneficiare di servizi operativi come monitoraggio e avvisi, gestione degli incidenti, gestione della sicurezza e gestione dei backup, senza dover effettuare una nuova migrazione, subire tempi di inattività o modificare il modo in

cui utilizzi. AWS AMS Accelerate offre anche un componente aggiuntivo opzionale per carichi di lavoro EC2 basati su patch che richiedono patch regolari. Con AMS Accelerate puoi continuare a utilizzare, configurare e implementare tutti i AWS servizi in modo nativo o con i tuoi strumenti preferiti, proprio come fai con gli account AMS Advanced Customer Managed. Utilizzi i tuoi meccanismi di accesso e modifica preferiti mentre AMS applica pratiche collaudate che aiutano a scalare il tuo team, ottimizzare i costi, aumentare la sicurezza e l'efficienza e migliorare la resilienza. Per ulteriori informazioni, consulta la descrizione del servizio Accelerate.

Per inserire il tuo account Customer Managed in Accelerate, contatta il tuo CSDM e segui la procedura descritta nella Guida introduttiva ad AMS Accelerate.

> **Note**
>
> Gli account AMS Accelerate in AMS Advanced non dispongono della gestione delle modifiche AMS (richieste di modifica o RFCs) o della console AMS Advanced. Dispongono invece della console e della funzionalità AMS Accelerate.

Account AMS Tools (migrazione dei carichi di lavoro)

Il tuo account Multi-Account Landing Zone Tools (con VPC) aiuta ad accelerare le operazioni di migrazione, aumenta la tua posizione di sicurezza, riduce costi e complessità e standardizza il modello di utilizzo.

Un account Tools offre quanto segue:

- Un limite ben definito per l'accesso alle istanze di replica per gli integratori di sistema al di fuori dei carichi di lavoro di produzione.
- Consente di creare una camera isolata per verificare la presenza di malware o percorsi di rete sconosciuti in un carico di lavoro prima di trasferirlo in un account con altri carichi di lavoro.
- Essendo una configurazione definita dell'account, offre tempi più rapidi per l'onboarding e la configurazione per la migrazione dei carichi di lavoro.
- Percorsi di rete isolati per proteggere il traffico proveniente dall'account locale -> -> Tools account CloudEndure -> AMS ingerita dall'immagine. Una volta che l'immagine è stata inserita, puoi condividerla con l'account di destinazione tramite una RFC AMS Management | Advanced stack components | AMI | Share (ct-1eiczxw8ihc18).

Diagramma di architettura di alto livello:

Usa Deployment | Managed landing zone | Management account | Create tools account (con VPC) change type (ct-2j7q1hgf26x5c), per implementare rapidamente un account di strumenti e creare un'istanza di un processo di inserimento del carico di lavoro in un ambiente Multi-Account Landing Zone. Vedi Account di gestione, Account Tools: Creazione (con VPC).

> **Note**
>
> Ti consigliamo di avere due zone di disponibilità (AZs), poiché si tratta di un hub di migrazione.
> Per impostazione predefinita, AMS crea i seguenti due gruppi di sicurezza (SGs) in ogni account. Conferma che questi due SGs siano presenti. Se non sono presenti, apri una nuova richiesta di assistenza con il team AMS per richiederli.
>
> - SentinelDefaultSecurityGroupPrivateOnlyEgressAll
> - InitialGarden-SentinelDefaultSecurityGroupPrivateOnly
>
> Assicurati che le istanze di CloudEndure replica vengano create nella sottorete privata in cui sono presenti percorsi di ritorno all'ambiente locale. Puoi confermarlo assicurandoti che le tabelle di routing per la sottorete privata abbiano una route predefinita per tornare a TGW. Tuttavia, se si esegue un cut over CloudEndure automatico, si dovrebbe passare alla sottorete privata «isolata», dove non esiste alcuna via di ritorno alla rete locale, ma è consentito solo il traffico Internet in uscita. È fondamentale garantire che si verifichi il cutover nella sottorete isolata per evitare potenziali problemi alle risorse locali.

Prerequisiti:

1. Livello di supporto Plus o Premium.
2. L'account dell'applicazione IDs per la chiave KMS in cui AMIs vengono distribuite.
3. L'account degli strumenti, creato come descritto in precedenza.

AWS Servizio di migrazione delle applicazioni (AWS MGN)

AWS Application Migration Service (AWS MGN) può essere utilizzato nel tuo account MALZ Tools tramite il ruolo `AWSManagedServicesMigrationRole` IAM che viene creato automaticamente

durante il provisioning dell'account Tools. È possibile utilizzare AWS MGN per migrare applicazioni e database eseguiti su versioni supportate dei sistemi operativi Windows e Linux.

Per la maggior parte delle up-to-date informazioni sull' Regione AWS assistenza, consulta l'elenco dei servizi AWS regionali.

Se il tuo preferito non Regione AWS è attualmente supportato da AWS MGN o il sistema operativo su cui vengono eseguite le tue applicazioni non è attualmente supportato da AWS MGN, prendi in considerazione l'utilizzo di CloudEndure Migration nel tuo account Tools.

Richiedere l'inizializzazione AWS di MGN

AWS MGN deve essere inizializzato da AMS prima del primo utilizzo. Per richiederlo per un nuovo account Tools, invia una richiesta RFC Management | Other | Other dall'account Tools con questi dettagli:

```
RFC Subject=Please initialize AWS MGN in this account
RFC Comment=Please click 'Get started' on the MGN welcome page here:

    https://console.aws.amazon.com/mgn/home?region=MALZ_PRIMARY_REGION#/welcome using
 all default values
    to 'Create template' and complete the initialization process.
```

Una volta che AMS avrà completato con successo la RFC e inizializzato AWS MGN nel tuo account Tools, potrai utilizzarlo `AWSManagedServicesMigrationRole` per modificare il modello predefinito in base alle tue esigenze.

Abilita l'accesso al nuovo account AMS Tools

Una volta creato l'account Tools, AMS ti fornisce un ID account. Il passaggio successivo consiste nel configurare l'accesso al nuovo account. Segui questa procedura.

1. Aggiorna i gruppi Active Directory appropriati con l'account appropriato IDs.

   Ai nuovi account creati con AMS vengono assegnati i criteri relativi ai ReadOnly ruoli e un ruolo che consente agli utenti di archiviare i file. RFCs

   L'account Tools dispone anche di un ruolo e di un utente IAM aggiuntivi:

   - Ruolo IAM: `AWSManagedServicesMigrationRole`
   - Utente IAM: `customer_cloud_endure_user`

2. Richiedi politiche e ruoli per consentire ai membri del team di integrazione dei servizi di configurare il livello successivo di strumenti.

   Vai alla console AMS e archivia quanto segue RFCs:

   a. Crea una chiave KMS. Utilizza Crea chiave KMS (auto) o Crea chiave KMS (automazione gestita).

      Poiché utilizzi KMS per crittografare le risorse acquisite, l'utilizzo di una singola chiave KMS condivisa con il resto degli account dell'applicazione Multi-Account Landing Zone garantisce la sicurezza delle immagini importate, in modo che possano essere decrittografate nell'account di destinazione.

   b. Condividi la chiave KMS.

      Utilizza Management | Advanced stack components | KMS key | Share (managed automation) change type (ct-05yb337abq3x5) per richiedere che la nuova chiave KMS venga condivisa con gli account dell'applicazione in cui risiederà quella acquisita. AMIs

Grafico di esempio della configurazione finale dell'account:

Esempio di politica IAM CloudEndure preapprovata da AMS

Per visualizzare una CloudEndure policy IAM preapprovata da AMS: decomprimi il file di esempio WIGS Cloud Endure Landing Zone e apri il. `customer_cloud_endure_policy.json`

Test della connettività e della end-to-end configurazione dell'account AMS Tools

1. Inizia con la configurazione CloudEndure e l'installazione dell' CloudEndure agente su un server che si replicherà su AMS.
2. Crea un progetto in. CloudEndure
3. Inserisci le AWS credenziali condivise quando hai eseguito i prerequisiti, tramite Secrets Manager.
4. Nelle impostazioni di replica:
   a. Seleziona entrambi i gruppi di sicurezza AMS «Sentinel» (solo privati e EgressAll) per l'opzione Scegli i gruppi di sicurezza da applicare ai server di replica.
   b. Definite le opzioni di cutover per le macchine (istanze). Per informazioni, consultate la Fase 5. Tagliare
   c. Sottorete: sottorete privata.

5. Gruppo di sicurezza:
   a. Seleziona entrambi i gruppi di sicurezza AMS «Sentinel» (solo privato e EgressAll).
   b. Le istanze Cutover devono comunicare con l'Active Directory (MAD) gestito da AMS e con gli endpoint pubblici: AWS
      i. IP elastico: nessuno
      ii. IP pubblico: no
      iii. Ruolo IAM: profilo a customer-mc-ec 2 istanze
   c. Imposta i tag secondo la tua convenzione di etichettatura interna.
6. Installa l' CloudEndure agente sulla macchina e cerca l'istanza di replica da visualizzare nel tuo account AMS nella console EC2.

Il processo di ingestione di AMS:

Igiene dell'account AMS Tools

Ti consigliamo di ripulire l'account dopo aver condiviso l'AMI e non avrai più bisogno delle istanze replicate:

- Dopo l'ingestione dell'istanza WIGs :
  - Istanza Cutover: come minimo, interrompi o termina questa istanza, una volta completato il lavoro, tramite la console AWS
  - Backup AMI pre-incorporazione: rimuovi una volta che l'istanza è stata inserita e l'istanza locale terminata
  - Istanze inserite da AMS: disattivate lo stack o terminate una volta che l'AMI è stata condivisa
  - AMS-Ingested: elimina una volta completata la condivisione con l'account di destinazione AMIs
- Pulizia alla fine della migrazione: documenta le risorse distribuite tramite la modalità Sviluppatore per garantire che la pulizia avvenga regolarmente, ad esempio:
  - Gruppi di sicurezza
  - Risorse create tramite Cloud-formation
  - Rete ACK
  - Sottorete
  - VPC
  - Tabella di routing

- Ruoli
- Utenti e account

Migrazione su larga scala - Migration Factory

Vedi Presentazione della soluzione AWS CloudEndure Migration Factory.

MALZ: onboarding dell'account principale

Le attività chiave che dovrai svolgere durante l'onboarding su un account principale di AWS landing zone multiaccount sono le seguenti:.

Argomenti

- Crea un AWS account principale per la landing zone con più account in AMS
- Crea un ruolo IAM per AMS per accedere al tuo account
- Proteggi il nuovo account con l'autenticazione a più fattori (MFA) per l'utente root in AMS
- Iscriviti a Marketplace AWS Trend Micro Endpoint Protection (EPS)
- Configurazione della rete
- Configurare la gestione degli accessi

Per domande sull'onboarding, contatta il tuo Cloud Architect.

Crea un AWS account principale per la landing zone con più account in AMS

La landing zone con più account AMS richiede il provisioning di un nuovo account Amazon Web Services (AWS) che funga da account di gestione nell'ambiente di landing zone multi-account AMS. Per creare un account Account AWS, segui queste step-by-step istruzioni: Come posso creare e attivare un nuovo account Amazon Web Services?

I semplici passaggi sono: vai su Crea account, fai clic su Registrati ora e, nella pagina che si apre, fai clic su Crea un nuovo Account AWS. Segui le istruzioni sullo schermo, che includono la ricezione di una telefonata e l'immissione di un PIN utilizzando la tastiera del telefono. Dovrai anche inserire una carta di credito. AMS utilizza questo account come account di gestione, o account di pagamento, per la tua nuova landing zone con più account.

Note

Una volta effettuato l'onboarding, parlate con il vostro cloud service delivery manager (CSDM) per trasferire la fatturazione dalla carta di credito a un sistema di fatturazione. Saranno richieste le seguenti informazioni:

- Nome della società di fatturazione
- Nome del contatto di fatturazione
- Numero di telefono di contatto per la fatturazione
- Email di contatto per la fatturazione
- Indirizzo di fatturazione

Il tuo CSDM ti aiuterà con questo aggiornamento. Una volta completato, e per modificare il metodo di pagamento, consulta Gestione dei metodi AWS di pagamento.

Note

Non collegare il nuovo account a un account di gestione o a un account di pagamento esistente.
Assicurati che il tuo account non faccia parte di un account esistente AWS Organizations; per informazioni, consulta Cos'è AWS Organizations?

Important

È molto importante assicurarsi che all'account siano associati un indirizzo e-mail (una lista di distribuzione, non l'indirizzo e-mail di una persona) e un numero di telefono in modo da ricevere risposte a potenziali incidenti di sicurezza. Il numero di telefono e l'indirizzo e-mail dell'account non possono essere modificati senza reimpostare la password dell'account, il che rappresenta un impegno importante per un account root AMS. Per garantire che questi valori siano stabili, è fondamentale selezionare informazioni di contatto non associate a singoli individui, che possono cambiare. Scegli un alias email che possa puntare a un gruppo. Segui la stessa procedura per selezionare un numero di telefono: scegli un numero che possa indirizzare a un gruppo o a un numero di proprietà dell'azienda e non a un individuo.

Per i dettagli sulle domande che ti verranno poste per effettuare l'onboarding del tuo account Core nella landing zone multi-account AMS, consulta. Appendice: lista di considerazioni relative all'onboarding zone di atterraggio multi-account (MALZ)

Crea un ruolo IAM per AMS per accedere al tuo account

Ora che hai creato con successo il tuo nuovo account Account AWS, il passaggio successivo del processo consiste nel consentire ad AMS di accedere al nuovo account per creare e configurare il tuo ambiente AMS e soddisfare le continue richieste di modifica e provisioning. Per i dettagli, consulta Delegare l'accesso tra AWS account utilizzando i ruoli IAM.

AWS Identity and Access Management (IAM) è un servizio web che ti aiuta a controllare in modo sicuro l'accesso alle AWS risorse per i tuoi utenti. Utilizzi IAM per controllare chi può utilizzare AWS le tue risorse (autenticazione), quali risorse possono utilizzare e in che modo (autorizzazione).

Attiva l'accesso IAM alla AWS console

1. Accedi alla console di AWS gestione con le credenziali del tuo account root (l'email e la password che hai usato per creare il tuo Account AWS). Non accedere con altre credenziali IAM. Viene visualizzata la home page della console di AWS gestione.
2. Nella barra di navigazione in alto, apri il menu a discesa relativo al nome dell'account, quindi scegli Account. Si apre la home page di Fatturazione.
3. Scorri verso il basso fino all'accesso di utenti e ruoli IAM alle informazioni di fatturazione e scegli Modifica. Si apre l'area di accesso Activate IAM.
4. Seleziona la casella di controllo, quindi scegli Aggiorna. Ora puoi utilizzare le policy IAM per controllare le pagine alle quali un utente può accedere.

Crea un ruolo IAM da utilizzare con AMS

1. Ottieni un file JSON o YAML che definisca un ruolo IAM per AMS da utilizzare per creare la tua infrastruttura. Una delle seguenti opzioni:
   - Il tuo architetto cloud AMS (CA) ti fornisce un file JSON o YAML.
   - Puoi scaricare onboarding_iam_roles.zip e scegliere una delle seguenti opzioni:
     - onboarding_role_admin.json (più breve, garantisce l'accesso amministrativo completo)
     - onboarding_role_minimal.json (più lungo, concede il minimo privilegio)

2. Accedi e Console di gestione AWS apri la console all'indirizzo /cloudformazione. CloudFormation https://console.aws.amazon.com

3. Scegli Crea stack. Viene visualizzata la pagina seguente.

4. Scegli Carica un file modello, carica il file JSON o YAML del ruolo IAM, quindi scegli Avanti. Viene visualizzata la pagina seguente.

5. Entra **`ams-onboarding-role`** nella sezione Stack name e continua a scorrere verso il basso e a selezionare Avanti fino a raggiungere questa pagina.

6. Assicurati che la casella di controllo sia selezionata, quindi seleziona Crea pila.
7. Assicurati che lo stack sia stato creato correttamente.

Proteggi il nuovo account con l'autenticazione a più fattori (MFA) per l'utente root in AMS

Questa sezione è stata redatta perché contiene informazioni sensibili relative alla sicurezza di AMS. Queste informazioni sono disponibili nella documentazione della console AMS. Per accedere ad AWS Artifact, puoi contattare il tuo CSDM per ricevere istruzioni o andare alla pagina Getting Started with AWS Artifact.

Iscriviti a Marketplace AWS Trend Micro Endpoint Protection (EPS)

Trend Micro Endpoint Protection (EPS) è il componente principale di AMS per la sicurezza del sistema operativo. Per configurare EPS una volta avviata la creazione della landing zone AMS, è necessario accedere all'account principale dei servizi condivisi e abbonarsi all'AMI Trend Micro Deep Security Marketplace AWS. Il tuo CSDM o CA ti consiglieranno.

1. Accedi alla AWS console utilizzando il ruolo o l'utente specificato nel questionario di onboarding per `CustomerEPSSubscriptionIAMRoleOrUser`
2. Vai alla schermata Cambia ruolo.

- Account: fornito da AMS
- Ruolo: `EPSMarketplaceSubscriptionRole`
- Nome visualizzato: sessione di abbonamento EPS

  Per abbonarti a Trend Micro Deep Security in Marketplace AWS, segui questi passaggi dopo aver cambiato ruolo nella console:

  1. Accedi ad AWS Marketplace.
  2. In Trova Marketplace AWS i prodotti che soddisfano le tue esigenze, seleziona le seguenti opzioni:
     a. Fornitori: Trend Micro
     b. Piano tariffario: Bring Your Own License se disponi di una licenza o By Hosts Billing
     c. Metodi di consegna: Amazon Machine Image
  3. Fai clic su Continua per iscriverti nel pannello a destra.
  4. Leggi i Termini e condizioni e fai clic su Accetta i termini nell'angolo in alto a destra.
  5. Esci dall'account e conferma con Cloud Architect che la procedura è stata completata.

A questo punto AMS implementa l'infrastruttura nel tuo ambiente AMS e l'ambiente è pronto per l'uso dopo aver connesso la rete e configurato l'accesso.

Configurazione della rete

Il networking nell'ambiente AMS viene gestito principalmente nell'account di rete principale.

Esistono diversi processi che devono essere completati per configurare il networking per AWS Managed Services (AMS):

- Allocazione dello spazio IP per l'ambiente AMS
- Stabilire una connettività di rete privata a AWS
- Configurazione del firewall per consentire le operazioni AMS

Allocazione dello spazio IP per l'ambiente AMS

Dovresti aver già collaborato con il tuo Cloud Architect per definire lo spazio IP per il tuo ambiente AMS durante la compilazione del questionario di onboarding.

Stabilire la connettività di rete privata verso AWS AMS

AWS offre connettività privata utilizzando la connettività VPN e linee dedicate tramite AWS Direct Connect. La connettività privata può essere configurata in due modi:

- Connettività Edge centralizzata tramite Transit Gateway
- Connessione di Direct Connect and/or VPN all'account VPCs

Connettività edge centralizzata tramite Transit Gateway

AWS Transit Gateway è un servizio che consente di connettere Amazon Virtual Private Clouds (VPCs) e le reti locali a un unico gateway. Transit Gateway può essere utilizzato per consolidare la connettività edge esistente e instradarla attraverso un unico ingress/egress punto. Per ulteriori dettagli, consulta AWS Transit Gateway.

Connessione di Direct Connect a Transit Gateway

Puoi utilizzare la tua connessione Direct Connect esistente o creare una nuova connessione Direct Connect in uno dei tuoi AWS account esistenti. La connessione Direct Connect deve essere una connessione dedicata o ospitata con una velocità pari o superiore a 1 Gbps.

> **Note**
>
> Per informazioni sull'utilizzo di Direct Connect con AWS i servizi, consulta Guida introduttiva da una posizione AWS Direct Connect.

Per utilizzare una connessione dedicata Direct Connect esistente, sulla connessione non devono essere create più di 3 interfacce virtuali di transito. Questo perché le connessioni Direct Connect dedicate hanno un limite di 4 interfacce virtuali di transito per connessione.

Per ulteriori informazioni sui limiti di Direct Connect, consulta AWS Direct Connect Limits.

Una volta che la connessione Direct Connect è disponibile, si verifica quanto segue:

1. AMS crea un gateway Direct Connect nell'account di rete. È necessario fornire un numero ASN (Autonomous System Number) per il gateway Direct Connect e i prefissi che devono essere pubblicizzati dal gateway Direct Connect. Questo ASN viene utilizzato come Amazon ASN.
2. Crei un nuovo Transit VIF e imposti il proprietario dell'interfaccia virtuale come account di rete.
3. AMS accede all'account di rete e accetta la proposta di connessione.
4. AMS associa il gateway di transito al gateway Direct Connect.
5. AMS associa l'allegato alla tabella di routing Transit Gateway locale.

> **Note**
>
> L'ASN fornito per il gateway Direct Connect e il Transit Gateway deve essere diverso.

Per aumentare la resilienza della connettività, è consigliabile collegare almeno 2 interfacce virtuali di transito, da diverse postazioni AWS Direct Connect, al gateway Direct Connect. Per ulteriori informazioni, consulta i consigli sulla Direct Connect resilienza.

Connessione della VPN al Transit Gateway

Per collegare una connessione VPN a un gateway di transito è necessario specificare il gateway del cliente. Per ulteriori informazioni sui requisiti per un gateway per i clienti, consulta Requirements for Your Customer Gateway nella Amazon VPC Network Administrator Guide.

È necessario fornire il numero ASN BGP, l'indirizzo IP pubblico statico e l'opzione di routing (statica o dinamica). Una volta forniti questi dettagli, AMS creerà l'allegato VPN e lo assocerà alla tabella di routing Transit Gateway locale.

Per maggiori dettagli sugli allegati Transit Gateway, consulta Allegati VPN Transit Gateway.

Connessione di Direct Connect and/or VPN all'account VPCs

Puoi anche connetterti direttamente VPCs a Direct Connect o VPN. Il traffico fluisce direttamente VPCs da Direct Connect o VPN senza attraversare il gateway di transito.

> **Note**
>
> Il VPC dei servizi condivisi e l'account dell'applicazione VPCs devono essere collegati a una connessione Direct Connect o VPN per stabilire una connettività privata.

Direct Connect configurazione in AMS

Configura un account Direct Connect per comunicare tra il tuo VPC gestito da AMS e la tua rete interna.

> **Note**
>
> Per informazioni sull'utilizzo di Direct Connect con AWS i servizi, consulta Guida introduttiva da una Direct Connect postazione.

Per configurare una connessione Direct Connect, completa i seguenti passaggi:

1. Registrazione ad Amazon Web Services (AWS)
2. Invia una richiesta di Direct Connect connessione.
3. Completa il Cross Connect.
4. (Facoltativo) Configura connessioni ridondanti con. Direct Connect
5. Eseguita da AMS: crea un'interfaccia virtuale.
6. Eseguita da AMS: scarica la configurazione del router.
7. Verifica la tua interfaccia virtuale.

Configurazione VPN

I passaggi di base seguiti da AMS per configurare una VPN per comunicare tra il tuo VPC gestito da AMS e la tua rete interna.

> **Note**
>
> Per una comprensione generale dell'utilizzo di una VPN con AWS servizi, consulta What is AWS Site-to-Site VPN and Your Customer Gateway (il tuo dispositivo VPN).

Seguiamo le sezioni Guida per l'utente AWS VPN Guida introduttiva e Test della connessione Site-to-Site VPN per completare i seguenti passaggi:

1. Crea un Customer Gateway nel tuo AWS VPC.

2. Nel tuo AWS VPC, crea un gateway privato virtuale.
3. Nel tuo AWS VPC, abilita la propagazione delle rotte nella tabella delle rotte.
4. Nel tuo AWS VPC, aggiorna il tuo gruppo di sicurezza per abilitare l'accesso SSH, RDP e ICMP in entrata.
5. Nella tua rete interna, crea una connessione VPN e configura il Customer Gateway.
6. Prova la connettività VPN tra il VPC e la tua rete interna.

Configurare la gestione degli accessi

Utilizzare una rete gestita da AWS Managed Services (AMS) significa concedere ad AMS l'accesso per gestire la tua infrastruttura cloud. Dovrai configurare un mezzo per connetterti in modo sicuro tra la tua rete privata e AMS. Questo inizia con alcune decisioni:

- Accesso ad AMS API/CLI e console: ti consigliamo di installare l'AMS CLI (le istruzioni sono fornite in questo documento). Utilizzi l'API di gestione delle modifiche AMS per effettuare richieste di modifica ad AMS e l'API AMS SKMS per conoscere le tue risorse gestite da AMS. Utilizzando Active Directory Federation Services (AD FS), puoi accedere alla console AMS.
- Accesso utente: è necessario stabilire la connettività tra AD sul lato AMS (tramite Directory Services) e la directory utilizzata per gestire gli utenti.
- Accesso all'istanza: l'accesso a livello di istanza viene ottenuto tramite una configurazione di trust unidirezionale. Directory Services considera affidabili le credenziali contenute in CORP AD, permettendo agli stack all'interno del lato AMS di consentire l'accesso con credenziali CORP.

> **Note**
>
> L'Active Directory (AD) su cui AMS imposta il trust deve essere la directory che contiene gli account degli utenti da te autorizzati ad accedere alle tue risorse AWS.

Stabilire un trust per Active Directory

Per impostare un trust, AMS richiede il controller di dominio Local Policies -> Security Options -> Network Access: Named Pipes a cui è possibile accedere in modo anonimo, riporta le pipe Netlogon e lsarpc elencate. Queste pipe sono elencate di default, ma a volte vengono rimosse per motivi di sicurezza. Una volta stabilita la fiducia, possono essere nuovamente rimosse dall'elenco.

Configurare lo spedizioniere condizionale

1. In AD DNS Manager -> Crea un nuovo inoltro condizionale, in Dominio DNS: utilizza il nome di dominio che AMS ti ha fornito; ad esempio, A523434123.amazonaws.com (cambialo con il nome di dominio selezionato nel questionario di onboarding).
2. In Indirizzi IP dei server master: aggiungi gli indirizzi IP forniti da AMS. Assicurati che non ci siano problemi di connessione convalidando entrambi gli indirizzi.
3. Seleziona Archivia questo server d'inoltro condizionale in Active Directory e replica come segue: Tutti i server DNS in questo dominio e premi OK.

Configurare l'AD trust

Segui questo articolo di Microsoft AD Crea un trust unidirezionale, in entrata e forestale per un lato del trust, utilizzando le impostazioni e le scelte descritte in questa sezione.

1. Aprire la finestra di dialogo Start -> Strumenti di amministrazione -> Domini e trust di Active Directory. Fate clic con il pulsante destro del mouse sul nodo del dominio con cui desiderate stabilire un trust, quindi fate clic su Proprietà -> Trust -> New Trust per aprire la procedura guidata New Trust. Inserisci il nome di dominio fornito da AMS per il Trust Name e premi Avanti.
2. In Tipo di fiducia, seleziona il livello di fiducia appropriato (ad esempio Forest Trust). Premi Avanti.
3. In Direction of Trust, seleziona Unidirezionale: in arrivo. Premere Next (Successivo).
4. In Sides of Trust, seleziona Solo questo dominio. Premere Next (Successivo).
5. In Trust Password, digita una password a tua scelta. Premere Next (Successivo).
6. Per Trust Selections Completed e Trust Creation Complete, basta premere Avanti.
7. In Conferma fiducia in entrata, seleziona No, non confermare l'attendibilità in entrata. Premere Next (Successivo).
8. In Completato il New Trust Wizard, seleziona Fine, quindi OK per chiudere.
9. Fornisci la password affidabile (contattaci tramite il numero di telefono del tuo CSDM per motivi di sicurezza). AMS completerà la configurazione di fiducia.

Siti e servizi Active Directory

Per ridurre la latenza di accesso, aggiungi l'intervallo VPC CIDR ai tuoi siti e servizi Active Directory (Start -> Strumenti di amministrazione -> Siti e servizi di Active Directory). Aggiungi l'intervallo VPC CIDR a un sito di Active Directory che contiene i controller di dominio più vicini ad AWS.

Fornisci il nome del sito AD del sito che hai dedicato ad AMS al tuo CSDM. AMS rinominerà il sito predefinito sul lato AMS di AD in modo che corrisponda al nome fornito.

Routing dei suffissi dei nomi di Active Directory

Dopo aver stabilito l'attendibilità unidirezionale della foresta, completa i seguenti passaggi per convalidare il routing dei suffissi:

1. In Start > Tutti i programmi > Strumenti di amministrazione, fate clic su Domini e trust di Active Directory.

   Si apre la console Active Directory Domains and Trust.
2. Fai clic con il pulsante destro del mouse sul dominio aziendale e scegli Proprietà

   Si apre la finestra di dialogo Proprietà relativa a quel dominio.
3. Fai clic sulla scheda Trust.

   Si apre la pagina Trust.
4. Fai clic sul nome di dominio Amazon, quindi su Proprietà.

   Si apre la pagina delle proprietà per il dominio Amazon Trust.
5. Fai clic su Name Suffix Routing e clicca su Aggiorna.

   Accertatevi che non vi siano conflitti per garantire che Service Principal Names (SPNs) possa risolversi sul trust.

Federa il tuo Active Directory con i ruoli AMS IAM

Lo scopo della federazione della directory con i ruoli AMS IAM è consentire agli utenti aziendali di utilizzare le proprie credenziali aziendali per interagire con la console AWS e AWS e APIs, quindi, la console AMS e. APIs

Esempio di processo di federazione

Questo esempio utilizza Active Directory Federation Services (ADFS); tuttavia, è supportata qualsiasi tecnologia che supporti AWS IAM Federation. Per ulteriori informazioni sulla federazione IAM supportata da AWS, consulta Partners and Identity Provider and Federation IAM. Il CSDM ti aiuterà in questo processo, che prevede uno sforzo congiunto con il tuo team AD e AMS.

Per informazioni dettagliate sull'integrazione di SAML per l'accesso alle API, consulta questo blog AWS, How to Implementation Federated API and CLI Access Using SAML 2.0 and AD FS.

Per un esempio di installazione di AMS CLI e SAML, consulta Appendice: regola di attestazione ADFS e impostazioni SAML.

Configurazione della federazione alla console AMS (MALZ)

I ruoli IAM e il provider di identità SAML (Trusted Entity) descritti nella tabella seguente sono stati forniti come parte dell'infrastruttura AMS. Questi ruoli consentono di controllare e visualizzare gli account principali di AMS.

Ruolo	Autorizzazioni
AWSManagedServicesReadOnlyRole	Consente di visualizzare l'infrastruttura AMS negli account principali.
AWSManagedServicesCaseRole	Consente di visualizzare le risorse nel nuovo account dell'applicazione e di archiviare gli incidenti e le richieste di assistenza AMS.
AWSManagedServicesChangeManagementRole	Consente di visualizzare l'infrastruttura AMS negli account principali, inviare ticket AWS Support e richiederne alcuni RFCs.

Per l'elenco completo dei ruoli disponibili con diversi account, consultaRuolo utente IAM in AMS.

Verifica l'accesso alla console

Dopo aver configurato ADFS e aver ottenuto l'URL AMS da utilizzare per l'autenticazione, segui questi passaggi.

Con una configurazione Active Directory Federated Service (ADFS), puoi seguire questi passaggi:

1. Apri una finestra del browser e vai alla pagina di accesso fornita per il tuo account. Si apre la IdpInitiatedSignOnpagina ADFS relativa al tuo account.
2. Seleziona il pulsante di opzione accanto a Accedi a uno dei seguenti siti. L'elenco di selezione del sito Accedi diventa attivo.
3. Scegli il sito signin.aws.amazon.com e fai clic su Accedi. Le opzioni per l'immissione delle credenziali sono aperte.
4. Inserisci le tue credenziali CORP e fai clic su Accedi. Le Console di gestione AWS aperture.
5. Incolla nella barra degli indirizzi l'URL della console AMS e premi Invio. La console AMS si apre.

Verifica l'accesso all'API

AMS utilizza l'API AWS, con alcune operazioni specifiche di AMS di cui puoi leggere nell'AMS API Reference.

AWS ne fornisce diversi a SDKs cui puoi accedere tramite Tools for Amazon Web Services. Se non desideri utilizzare un SDK, puoi effettuare chiamate API dirette. Per informazioni sull'autenticazione, consulta Signing AWS API Requests. Se non utilizzi un SDK o non effettui richieste API HTTP dirette, puoi utilizzare AMS CLIs for Change Management (CM) e SKMS.

Installa l'AMS CLIs

L'AWS CLI è un prerequisito per l'utilizzo di AMS CLIs (Change Management and SKMS).

1. Per installare l'AWS CLI, consulta Installazione dell'interfaccia a riga di comando AWS e segui le istruzioni appropriate. Nota che nella parte inferiore di quella pagina ci sono istruzioni per l'uso di diversi programmi di installazione, Linux, MS Windows, macOS, Virtual Environment, Bundled Installer (Linux, macOS o Unix).
2. Dopo l'installazione, esegui aws help per verificare l'installazione.
3. Una volta installata la CLI di AWS, per installare o aggiornare la CLI AMS, scarica il file zip AMS distribuables e decomprimilo. Puoi accedere ai file distribuibili dell'AMS CLI tramite il link Documentation nel menu di navigazione a sinistra della console AMS oppure chiedi al tuo cloud service delivery manager (CSDM) di inviarti il file zip.
4. Apri la directory Managed Cloud Distributables -> CLI -> Windows o la directory Managed Cloud Distributables -> CLI -> Linux /macOS, a seconda del sistema operativo in uso, e:
5. Per Windows, esegui il programma di installazione appropriato (questo metodo funziona solo su sistemi Windows a 32 o 64 bit):

- 32 bit: API_x86.msi ManagedCloud
- 64 bit: API_x64.msi ManagedCloud

6. Per Mac/Linux, esegui il file denominato: MC_CLI.sh eseguendo questo comando: sh MC_CLI.sh. Nota che le directory amscm e amsskms e il loro contenuto devono trovarsi nella stessa directory del file MC_CLI.sh.
7. Se le credenziali aziendali vengono utilizzate tramite federazione con AWS (la configurazione predefinita di AMS), è necessario installare uno strumento di gestione delle credenziali in grado di accedere al servizio di federazione. Ad esempio, puoi utilizzare questo AWS Security Blog How to Implementation Federated API and CLI Access Using SAML 2.0 e AD FS per aiutarti a configurare i tuoi strumenti di gestione delle credenziali.
8. Dopo l'installazione, esegui e visualizza i comandi `aws amscm help` e le opzioni`aws amsskms help`.

MALZ: onboarding dell'account dell'applicazione

È necessario disporre di un ambiente AWS Managed Services (AMS) multi-account configurato con account core, prima di richiedere un nuovo account applicativo. Ecco i passaggi da eseguire dopo aver configurato il tuo ambiente.

Argomenti

- Richiesta di un nuovo account per l'applicazione
- Configurazione di Active Directory per federare l'accesso ai ruoli AMS IAM
- Configurazione della rete con il nuovo account dell'applicazione
- Configurazione aggiuntiva VPCs nell'account dell'applicazione

Per domande sull'onboarding, contatta il tuo responsabile dell'erogazione dei servizi cloud (CSDM). Vedi anche Account delle applicazioni: gestiti da AMS, in modalità Dev-Mode, Gestiti dal cliente. Per informazioni generali sulle modalità, consulta Modalità AMS. Gestione dei servizi in AWS Managed Services

Per informazioni sulle diverse modalità di account delle applicazioni, consulta Account delle applicazioni: gestiti da AMS, modalità Dev, gestiti dal cliente. Per informazioni generali sulle modalità, consulta Modalità AMS.

Richiesta di un nuovo account per l'applicazione

È necessario disporre di un ambiente AWS Managed Services (AMS) multi-account configurato con account core, prima di richiedere un nuovo account applicativo. Per informazioni sulla configurazione di un ambiente multi-account con account principali, consulta. MALZ: onboarding dell'account principale

Puoi scegliere uno dei seguenti tipi di Amazon VPC per il VPC iniziale nell'account dell'applicazione:

- Privato: questo VPC non dispone di un gateway Internet collegato. È adatto per applicazioni private che non richiedono l'accesso a to/from Internet.
- Pubblico: questo VPC ha un gateway Internet collegato e dispone di sottoreti pubbliche e private. È adatto per applicazioni pubbliche che richiedono l'accesso a to/from Internet.

Puoi richiedere un nuovo account applicativo inviando un RFC Deployment | Managed landing zone | Management account | Create application account (con VPC) (ct-1zdasmc2ewzrs) e fornendo i seguenti valori nella RFC:

- Nome account: un nome personalizzato per l'account. Tieni presente che il nome dell'account ha una lunghezza massima di 50 caratteri.
- E-mail dell'account: l'e-mail della lista di distribuzione per l'account. Questo ID e-mail viene utilizzato per creare l'account AWS.
- Livello di supporto: il livello AWS Support, Premium o Plus.
- Nome VPC: un nome per il VPC.
- Numero di zone di disponibilità (AZs): 2 o 3.
- VPC CIDR: il blocco CIDR per il VPC.
- Tipo di percorso: può essere uno dei due. `routable` `isolated` `Routable`significa che l'applicazione VPCs associata alla tabella di routing dell'applicazione Transit Gateway (TGW) può connettersi a questo VPC. `Isolated`significa che l'applicazione VPCs associata alla tabella di routing dell'applicazione TGW non può connettersi a questo VPC. Il valore predefinito è `routable`.
- Tabella del percorso dell'applicazione Transit Gateway: la tabella di routing del Transit Gateway a cui deve essere associato il VPC dell'account dell'applicazione. Se non viene fornito alcun valore, `defaultAppRouteDomain` viene utilizzata quella predefinita, il che significa che questo account sarà in grado di comunicare con tutti gli altri account nella stessa tabella di routing.
- PublicSubnetAZ *<1-3>* CIDRCIDR per la sottorete pubblica in AZ 1: il CIDR per la sottorete pubblica nella zona di disponibilità 1.

- PrivateSubnet*<1-10>*AZ *<I-3>* CIDRCIDR per la sottorete pubblica in AZ 1: Il CIDR per la sottorete pubblica nella zona di disponibilità 1.

A questo punto, AMS implementa un nuovo account applicativo nell'account di gestione AMS, con la configurazione VPC specificata.

Configurazione di Active Directory per federare l'accesso ai ruoli AMS IAM

Federa la tua directory con i ruoli AMS IAM per consentire agli utenti aziendali di utilizzare le proprie credenziali aziendali per interagire con la console AWS e AWS APIs, nonché la console AMS e AMS. APIs

Esempio di processo di federazione

Questo esempio utilizza Active Directory Federation Services (ADFS). Tuttavia, è supportata qualsiasi tecnologia che supporti AWS IAM Federation. Per ulteriori informazioni sulla federazione IAM supportata da AWS, consulta IAM Partners and Identity Providers and Federation. Il CSDM ti aiuterà in questo processo, che prevede uno sforzo congiunto con il tuo team AD e AMS.

Per informazioni dettagliate sull'integrazione di SAML per l'accesso alle API, consulta questo blog AWS, How to Implementation Federated API and CLI Access Using SAML 2.0 and AD FS.

Per un esempio di installazione di AMS CLI e SAML, consulta l'Appendice: regola di attestazione ADFS e impostazioni SAML nella Guida per l'utente AMS.

Configurazione della federazione sulla console AMS

I ruoli IAM e il provider di identità SAML (Trusted Entity) descritti nella tabella seguente vengono forniti nel nuovo account dell'applicazione. Questi ruoli consentono di accedere al nuovo account e file dell'applicazione RFCs, scrivere nei bucket S3 ed eseguire altre azioni.

Ruolo	Autorizzazioni
AWSManagedServicesReadOnlyRole	Consente di visualizzare le risorse nel nuovo account dell'applicazione.
AWSManagedServicesCaseRole	Consente di visualizzare le risorse nel nuovo account dell'applicazione e di inviare i ticket AWS Support.

Ruolo	Autorizzazioni
AWSManagedServicesChangeManagementRole	Consente di visualizzare l'infrastruttura AMS negli account delle applicazioni, nei ticket di file e file RFCs di AWS Support, scrivere nei bucket S3, gestire i segreti di Secrets Manager e gestire le istanze riservate di Amazon Elastic Compute Cloud (Amazon EC2).
AWSManagedServicesSecurityOpsRole	Consente di visualizzare l'infrastruttura AMS negli account delle applicazioni, gestire i segreti di Secrets Manager, gestire le regole del Web Application Firewall, gestire i certificati e archiviare i ticket AWS Support.
AWSManagedServicesAdminRole	Consente di visualizzare l'infrastruttura AMS negli account delle applicazioni, gestire gli abbonamenti Marketplace, gestire i segreti di Secrets Manager, gestire le regole del Web Application Firewall, gestire certificati, creare RFCs, gestire EC2 istanze Amazon riservate , scrivere su bucket S3, archiviare ticket AWS Support e gestire gli accordi AWS Artifacts.

Invio della richiesta di federazione ad AMS

Se questo è il tuo primo account, collabora con i tuoi CSDM and/or Cloud Architect per fornire il file XML di metadati per il tuo provider di identità.

Se stai effettuando l'onboarding di un account o di Identity Provider aggiuntivo e hai accesso all'account di gestione o all'account dell'applicazione desiderato, segui questi passaggi.

1. Crea una richiesta di servizio dalla console AMS.

> **Note**
>
> - Se state creando un provider di identità per un account di applicazione, inviate questa richiesta dall'account dell'applicazione stesso o dall'account di gestione.

- Se stai creando un provider di identità per un account principale AMS, invia questa richiesta dall'account di gestione.
- Se stai creando un provider di identità per l'account di gestione, invia questa richiesta dall'account di gestione o contatta il tuo CSDM per ricevere assistenza.

Nella richiesta di servizio, fornisci i dettagli necessari per aggiungere il provider di identità:

- AccountId dell'account in cui verrà creato il nuovo provider di identità.
- Il nome del provider di identità desiderato, se non viene fornito, il valore predefinito sarà customer-saml; in genere, deve corrispondere alle impostazioni configurate nel provider della federazione.
- Per gli account esistenti, indica se il nuovo provider di identità deve essere propagato a tutti i ruoli di console esistenti o fornisci un elenco di ruoli che dovrebbero considerare attendibile il nuovo provider di identità.
- Allega il file XML di metadati esportato dal tuo agente federativo alla richiesta di servizio come file allegato.

2. Dallo stesso account in cui hai creato la richiesta di servizio, crea un nuovo RFC utilizzando CT-ID ct-1e1xtak34nx76 (Gestione | Altro | Altro | Crea) con le seguenti informazioni.

- <Name>Titolo: «IDP SAML integrato per account < >». AccountId
- AccountId dell'account in cui verrà creato il provider di identità.
- Nome del provider di identità.
- Per gli account esistenti: indica se il provider di identità deve essere propagato a tutti i ruoli di console esistenti o l'elenco dei ruoli che devono considerare attendibile il nuovo provider di identità.
- ID del caso della richiesta di servizio creata nel passaggio 1, in cui è allegato il file XML di metadati.

Verifica dell'accesso alla console

Dopo aver configurato ADFS e aver ottenuto l'URL AMS da utilizzare per l'autenticazione, è possibile eseguire la procedura seguente.

Con una configurazione Active Directory Federated Service (AD FS), puoi seguire questi passaggi:

1. Apri una finestra del browser e vai alla pagina di accesso fornita per il tuo account. Si apre la IdpInitiatedSignOn pagina AD FS relativa al tuo account.
2. Seleziona il pulsante di opzione accanto a Accedi a uno dei seguenti siti. L'elenco dei siti di accesso diventa attivo.
3. Scegli il sito signin.aws.amazon.com e scegli Accedi. Le opzioni per l'immissione delle credenziali sono aperte.
4. Inserisci le tue credenziali CORP e scegli Accedi. Si apre la Console di gestione AWS.
5. Incolla nella barra degli indirizzi l'URL della console AMS e premi Invio. La console AMS si apre.

Verifica dell'accesso all'API

AMS utilizza l'API AWS, con alcune operazioni specifiche di AMS di cui puoi leggere nell'AMS API Reference.

AWS ne fornisce diversi a SDKs cui puoi accedere tramite Tools for Amazon Web Services. Se non desideri utilizzare un SDK, puoi effettuare chiamate API dirette. Per informazioni sull'autenticazione, consulta Signing AWS API Requests. . Se non utilizzi un SDK o non effettui richieste API HTTP dirette, puoi utilizzare AMS CLIs for Change Management (CM) e SKMS.

Configurazione della rete con il nuovo account dell'applicazione

La configurazione della rete per l'account dell'applicazione include la configurazione delle regole del firewall e, potenzialmente, la configurazione di tabelle di routing Transit Gateway (TGW) aggiuntive.

Configurazione del firewall

Per utilizzare le applicazioni distribuite nell'ambiente AMS, è necessario creare alcune regole firewall. Non hai bisogno di queste regole per accedere alle tue istanze, ma puoi scavalcare i bastioni per entrare nelle tue istanze.

Regole firewall per l'accesso alle applicazioni

È necessario aprire le seguenti porte per il traffico attraverso il firewall:

- Dalla rete locale al VPC della nuova applicazione CIDRs in entrambe le direzioni di ingresso e uscita.

- Dal VPC della nuova applicazione CIDRs alla rete locale in entrambe le direzioni di ingresso e uscita (se le applicazioni cloud devono raggiungere le applicazioni locali).

Porta	Protocollo	Servizio	Da/a	Da/per
80	TCP	Accesso Web HTTP	Rete locale	VPC dell'applicazione AMS
443	TCP	Accesso Web HTTPS	Rete locale	VPC dell'applicazione AMS

Configurazione di tabelle di routing delle applicazioni Transit Gateway aggiuntive

La rete AWS Managed Services (AMS) è flessibile e supporta una varietà di casi d'uso di rete.

- Comunicazione tra applicazioni VPCs nello stesso account.
- Comunicazione tra applicazioni VPCs in diversi account.
- Isolamento tra applicazioni VPCs in diversi account.
- Isolamento tra applicazioni VPCs negli stessi account.

Se hai unique/special dei requisiti per il networking, contatta il tuo AMS Cloud Architect che svilupperà un piano per far sì che i tuoi requisiti siano soddisfatti dall'architettura di rete AMS.

In base alla decisione di rete presa per l'account dell'applicazione VPCs, è possibile creare più tabelle di routing delle applicazioni Transit Gateway (TGW) inviando un RFC Deployment | Managed landing zone | Networking account | Create transit gateway route table (ct-3dscwaeyi6cup).

Il tipo di modifica richiede di specificare `TransitGatewayRouteTableName` (un nome significativo per la tabella delle rotte TGW), e. `TransitGatewayId` `TGWRouteTableType`

> **Note**
>
> Se si seleziona createCustomRoute Dominio per TGWRouteTableType, la tabella delle rotte creata è vuota. È necessario presentare una RFC con il tipo di modifica Deployment | Managed landing zone | Networking account | Aggiungi route statica (ct-3r2ckznmt0a59).

Configurazione aggiuntiva VPCs nell'account dell'applicazione

Puoi richiedere un account applicativo aggiuntivo VPC inviando un RFC Deployment | Managed landing zone | Application account | Create VPC (ct-1j3503fres5a5).

Funziona allo stesso modo della configurazione di un VPC per un nuovo account dell'applicazione. Per informazioni dettagliate, vedi Richiesta di un nuovo account per l'applicazione.

Appendice: lista di considerazioni relative all'onboarding zone di atterraggio multi-account (MALZ)

Ci sono una serie di considerazioni chiave a cui devi pensare quando pianifichi l'implementazione di una landing zone con più account AMS. Le tue scelte forniranno ad AMS le informazioni necessarie per determinare i componenti dell'infrastruttura di cui avrai bisogno. Il tuo Cloud Architect (CA) ti fornirà un questionario per aiutarti in questo lavoro.

Argomenti

- Configurazione dell'account AMS multi-account landing zone
- Avvisi di monitoraggio delle landing zone multi-account AMS
- Configurazione di rete
- Configurazione di Active Directory
- Protezione degli endpoint Trend Micro (EPS)
- Accesso: Bastions, SSH e RDP
- Federazione

> **Note**
>
> Per ulteriori informazioni sui tipi di istanze, consulta Amazon EC2 Instance Types.
> Per ulteriori informazioni sui tipi di istanze di database, consulta Tipi di istanze di Amazon RDS.
> Se hai bisogno di Direct Connect, consulta la AMS single-account landing zone Onboarding Guide per creare una connessione Direct Connect.

Riceverai un questionario di onboarding dal tuo Cloud Service Delivery Manager (CSDM) contenente domande sulle impostazioni di configurazione desiderate per il tuo account. Collabora con il tuo CSDM per completare il questionario prima di procedere.

Configurazione dell'account AMS multi-account landing zone

- Nuovo ID account

  L' Account AWS ID che hai creato per la landing zone multi-account AMS. Non dovrebbe far parte di un' AWS organizzazione.

- Regione di servizio

  La regione principale in cui verrà implementato l'ambiente di landing zone multi-account AMS.

- Le e-mail dell'account principale per le notifiche. (dovrebbero essere tutte nello stesso dominio). Fornisci un indirizzo email per ciascuno:
  - Account Shared Services
  - Account di rete
  - Account di registrazione
  - Account di sicurezza
- Il tuo tipo di servizio, Premium o Plus

  Ciò determina gli accordi sul livello di servizio (SLAs) per la risoluzione dei problemi nell'ambiente in uso

Avvisi di monitoraggio delle landing zone multi-account AMS

AMS offre un modo per ricevere avvisi diretti (anziché ricevere notifiche del servizio AMS) per determinati avvisi di monitoraggio. Per iscriverti, assicurati che il tuo Cloud Architect (CA) o Cloud Service Delivery Manager (CSDM) riceva queste informazioni:

Direct Alerts Email: questi sono gli indirizzi e-mail a cui desideri che AMS invii determinati avvisi basati sulle risorse. Per i dettagli su quali avvisi vengono inviati direttamente via e-mail, consulta Alerts from Baseline Monitoring in AMS nella AMS Advanced User Guide. Per ulteriori informazioni sul monitoraggio AMS, consulta Monitoring Management nella AMS User Guide for Single-Account Landing Zone.

Configurazione di rete

- Numero ASN del Transit Gateway

  Si tratta dell'Autonomous System Number (ASN) per il lato AWS di una sessione Border Gateway Protocol (BGP), deve essere univoco e non può essere lo stesso utilizzato per Direct Connect o VPN. L'intervallo è compreso tra 64512 e 65534 (incluso) per 16 bit. ASNs
- Le gamme VPC CIDR dell'infrastruttura di landing zone multi-account AMS.

  Questi intervalli CIDR non possono sovrapporsi alla rete locale

  Puoi includere un intervallo CIDR /22 o fornire ogni VPC CIDR singolarmente. Nota che sono consentiti solo questi intervalli CIDR:

  - 10.0.0.0 - 10.255.255.255 (prefisso 10/8)
  - 172.16.0.0 - 172.31.255.255 (prefisso 172.16/12)
  - 192.168.0.0 - 192.168.255.255 (prefisso 192.168/16)

  Tieni presente che l'intervallo IP 198.18.0.0/15 non può essere utilizzato (è riservato da AWS Directory Service).

  - Intervallo CIDR VPC dell'infrastruttura principale (intervallo /22 consigliato)
  - Intervallo VPC CIDR di rete (intervallo /24 consigliato)
  - Intervallo CIDR VPC di Shared Services (intervallo consigliato /23)
  - Intervallo DMZ VPC CIDR (intervallo consigliato /25)
- VPN ECMP (abilita o disabilita)

  In VPN ECMP support (Supporto VPN ECMP), selezionare enable (abilita) se è necessario disporre del supporto per l'instradamento Equal Cost Multipath (ECMP) tra le connessioni VPN. Se le connessioni pubblicizzano lo stesso messaggio CIDRs, il traffico viene distribuito equamente tra di loro.

Elenco di controllo degli accessi alla rete (NACL)

Una lista di controllo degli accessi alla rete (NACL) è un livello di sicurezza opzionale per il tuo VPC che funge da firewall per controllare il traffico in entrata e in uscita da una o più sottoreti. Potresti configurare una rete ACLs con regole simili ai tuoi gruppi di sicurezza per aggiungere un ulteriore

livello di sicurezza al tuo VPC. Per ulteriori informazioni sulle differenze tra gruppi di sicurezza e rete ACLs, consulta Confronto tra gruppi di sicurezza e rete ACLs.

Tuttavia, nella landing zone multi-account AMS, per consentire ad AMS di gestire e monitorare efficacemente l'infrastruttura, l'uso di NACLs è limitato al seguente ambito:

- NACLs non sono supportati negli account principali della landing zone multi-account: Management, Networking, Shared-services, Logging e Security.
- NACLs sono supportati negli account delle applicazioni con più account di landing zone, a condizione che vengano utilizzati solo come elenco «Deny». Inoltre, devono avere la configurazione «Allow All» configurata per garantire le operazioni di monitoraggio e gestione di AMS.

In ambienti con più account su larga scala, puoi anche sfruttare funzionalità come i firewall di uscita centralizzati per controllare il traffico in uscita e/o le tabelle di routing Transit AWS Gateway nella landing zone multi-account AMS per separare il traffico di rete. VPCs

Configurazione di Active Directory

Nome di dominio completo per Active Directory gestito da AMS

Protezione degli endpoint Trend Micro (EPS)

- Dimensioni delle istanze per le EC2 istanze e i gruppi di Auto Scaling

  Trend Micro Endpoint Protection (EPS) è il componente principale di AMS per la sicurezza del sistema operativo. Il sistema è composto da istanze Deep Security Manager (DSM), EC2 istanze relay e un agente presente in tutto il piano dati AMS e nelle tue EC2 istanze. EC2

  - Tipo di istanza Relay (il minimo supportato da AMS è m5.large)
  - Dimensione dell'istanza DB (consigliati 200 GB)
  - Tipo di istanza RDS (sono consentiti solo db.m5.large o db.m5.xlarge)
- Tipo di licenza DSM (Marketplace o BYOL)

  Se hai già una licenza, scegli BYOL (bring your own license). AMS ti contatterà per ottenere le informazioni necessarie sulla licenza.
- AWS Utente o ruolo IAM Amazon resource name (ARN) per Trend Micro Deep Security Subscription (Role ARN: arn:aws:iam: ::role/) *ACCOUNT_ID ROLE_NAME*

Forniscici un ruolo IAM; ARN o un ARN utente IAM da uno dei tuoi ruoli esistenti Account AWS a cui hai accesso. AMS crea un ruolo IAM; nel tuo account Shared Services della landing zone multi-account AMS e aggiunge il ruolo o l'utente fornito nel trust di un ruolo IAM in Shared Services in modo che il ruolo possa essere assunto dall'utente per abbonarsi a Trend Micro Deep Security in Marketplace AWS.

Accesso: Bastions, SSH e RDP

- Impostazioni SSH Bastion

  AMS fornisce bastioni SSH nell'account Shared Services per accedere agli host nell'ambiente AMS. Per accedere alla rete AMS come utente SSH, è necessario utilizzare SSH Bastions come punto di ingresso. Il percorso di rete proviene dalla rete On-Prem, passa DX/VPN al gateway di transito (TGW) e quindi viene indirizzato al VPC di Shared Services. Una volta che sarai in grado di accedere al bastione, potrai passare ad altri host del tuo ambiente AMS, a condizione che sia stata concessa la richiesta di accesso appropriata.

  - Numero di istanze desiderato (consigliato 2)
  - Numero massimo di istanze (4 consigliate)
  - Numero minimo di istanze (2 consigliate)
  - Tipo di istanza (consigliato m5.large)
  - Ingresso CIDRs: intervalli di indirizzi IP da cui gli utenti della rete accederanno a SSH Bastions (intervallo IP 1, intervallo IP 2, intervallo IP 3,... ecc.)
- Impostazioni RDP Bastion

  AMS fornisce opzionalmente bastioni RDP nell'account Shared Services per accedere agli host nell'ambiente AMS. Per accedere alla rete AMS come utente RDP, è necessario utilizzare RDP Bastions come punto di ingresso. Il percorso di rete proviene dalla rete On-Prem, passa DX/VPN al TGW e quindi viene indirizzato a Shared Services VPC. Una volta che sei in grado di accedere al bastione, puoi passare ad altri host nell'ambiente AMS, a condizione che sia stata concessa la richiesta di accesso appropriata.

  - Tipo di istanza (consigliato t3.medium)
  - Sessioni minime desiderate (2 consigliate)
  - Numero massimo di sessioni desiderate (10 consigliate)

- Tipo di configurazione RDP Bastion, Shared Standard o Shared HA (l'impostazione predefinita è Shared Standard)

  SecureStandard = Un utente riceve un bastione e solo un utente può connettersi al bastione.

  SecureHA = Un utente riceve due bastioni in due diverse AZ a cui connettersi e solo un utente può connettersi al bastione.

  SharedStandard = Un utente riceve un bastione a cui connettersi e due utenti possono connettersi contemporaneamente allo stesso bastione.

  SharedHA = Un utente riceve due bastioni in due diverse AZ a cui connettersi e due utenti possono connettersi contemporaneamente allo stesso bastione.

Federazione

Nome dell'Identity Provider (IDP)

L'impostazione predefinita è `customer-saml`

Onboarding con AMS Single Account Landing Zone (SALZ)

Procedura di onboarding con AMS SALZ

Per effettuare l'onboarding degli account AMS single-account landing zone (SALZ), devi seguire i seguenti passaggi:

1. Crea un nuovo account AWS che AMS configura come account di rete per ospitare il firewall. Crea il nuovo account all'interno della tua organizzazione AWS, se ne hai uno. AMS seguirà la procedura di creazione di un normale account AMS, quindi è necessario raccogliere tutte le informazioni richieste (ad esempio CIDR, licenze EPS e utenti). Nota: un'allocazione CIDR di /24 è buona.
2. Specificate se desiderate rimuovere o meno i gateway Internet (IGWs) dagli account del traffico in uscita.
3. Determina i tuoi domini approvati. AMS consente il filtraggio delle destinazioni mantenendo un elenco di domini approvati; l'elenco può essere modificato in un secondo momento.
4. Conferma la dimensione dell'istanza che desideri utilizzare in base al throughput previsto. Per impostazione predefinita, l'istanza viene creata in un'istanza m4.xlarge in cui abbiamo rilevato che il throughput del firewall è di 350 Mbps. AMS può aumentare le dimensioni fino a un'istanza C4.8xLarge in cui il throughput previsto è di 1,25 Gbps.
5. Configura la rete tra AMS e la tua rete privata. Sono incluse diverse attività:
    a. Alloca lo spazio IP
    b. Stabilisci la connettività di rete privata con AWS
    c. Configura il tuo firewall
    d. Configura la gestione degli accessi
    e. Pianifica i backup
6. Fornisci l'accesso all'account creato ad AMS.
7. Verifica che il servizio AMS funzioni correttamente.

AMS sarà in grado di eseguire la creazione (onboarding) dell'account entro 2 settimane (10 giorni lavorativi) dalla data iniziale della richiesta. Qualsiasi attività di follow-up può essere eseguita utilizzando AMS Planned Event Management (PEM).

Note

- Stati Uniti orientali (Virginia)
- Stati Uniti occidentali (California settentrionale)
- US West (Oregon)
- Stati Uniti orientali (Ohio)
- Canada (Centrale)
- Sud America (San Paolo)
- UE (Irlanda)
- UE (Francoforte)
- UE (Londra)
- EU West (Parigi)
- Asia Pacifico (Mumbai)
- Asia Pacifico (Seoul)
- Asia Pacifico (Singapore)
- Asia Pacifico (Sydney)
- Asia Pacifico (Tokyo)

Nuove regioni vengono aggiunte frequentemente. Per l'elenco più aggiornato, consulta Regioni e zone di disponibilità AWS.

Architettura di rete SALZ

Il diagramma seguente illustra il layout della rete VPC VPC con account singolo di AWS Managed Services (AMS) single-account landing zone (SALZ) ed è un esempio di configurazione ad alta disponibilità.

AMS configura per te tutti gli aspetti del networking in base ai nostri modelli standard e alle opzioni selezionate fornite durante l'onboarding. Al tuo account AWS viene applicato un design di rete AWS standard e viene creato per te un cloud privato virtuale (VPC) collegato ad AMS tramite VPN o Direct

Connect. Scopri di più su Direct Connect su AWS Direct Connect. Lo standard VPCs include la DMZ, i servizi condivisi e una sottorete di applicazioni. Durante il processo di onboarding, VPCs potrebbero essere richiesti e creati altri dati in base alle esigenze dell'utente (ad esempio, divisioni clienti, partner). Dopo l'onboarding, ti viene fornito un diagramma di rete, un documento ambientale che spiega come è stata configurata la tua rete.

> **Note**
>
> Per informazioni sui limiti e i vincoli di servizio predefiniti per tutti i servizi attivi, consulta la documentazione di AWS Service Limits.

Il design della nostra rete si basa sul «Principio del minimo privilegio» di Amazon. A tal fine, indirizziamo tutto il traffico, in entrata e in uscita, attraverso i gateway, ad eccezione del traffico proveniente da una rete affidabile. L'unica rete affidabile è quella configurata tra l'ambiente locale e il VPC tramite l'uso di una and/or VPN e AWS Direct Connect (DX). L'accesso è garantito tramite l'uso di istanze bastion, impedendo così l'accesso diretto a qualsiasi risorsa di produzione. Tutte le applicazioni e le risorse risiedono all'interno di sottoreti private raggiungibili tramite sistemi di bilanciamento del carico pubblici. Il traffico pubblico in uscita fluisce attraverso i nostri proxy di inoltro verso l'Internet Gateway e quindi verso Internet. In alternativa, il traffico può fluire attraverso la tua VPN o Direct Connect verso il tuo ambiente locale.

Servizi condivisi di landing zone con account singolo AMS

Le sottoreti di servizi condivisi contengono AMS Directory Services, l'host di gestione che automatizza il provisioning e le attività comuni, il server di gestione antivirus () TrendMicro e gli host bastion interni:

- AMS Directory Services = AD Domain Controller

  Crea un Active Directory negli account AMS, crea il dominio AMS, unisce gli stack gestiti al dominio all'avvio.
- Host di gestione = AMS Management Host (automatizza il provisioning e le attività comuni)

  Funge da endpoint API per modificare e interagire con Directory Service i Directory Service controller di dominio.
- Servizi di sicurezza: server di gestione Antivirus (TrendMicro) = EPS DSM + EPS Relay

Sfrutta il software Trend Micro™ Deep Security (DSM), opera in un modello client-server e dispone di un database di back-end, include gestori, agenti e relè di Deep Security.

- Bastioni host interni = bastioni per i clienti

  Server per scopi speciali progettati per essere il punto di accesso principale da Internet e fungere da proxy per le altre istanze Amazon EC2.

SALZ: crea un nuovo AWS account per AMS

I cinque passaggi per creare un nuovo AWS account per AWS Managed Services (AMS) sono:

1. Crea un Account AWS
2. Configura la fatturazione consolidata: collega il nuovo account all'account Payer
3. Configura il tuo accesso Account AWS per AMS
4. Proteggi il nuovo account con l'autenticazione a più fattori (MFA) per l'utente root in AMS
5. Iscriviti a Marketplace AWS for EPS

Contatta il tuo responsabile della fornitura del servizio clienti (CSDM) in caso di domande.

Crea un Account AWS

Il programma AMS richiede il provisioning di un nuovo account Amazon Web Services (AWS). Le istruzioni dettagliate sono disponibili nel seguente video: Come posso creare e attivare un nuovo account Amazon Web Services? I semplici passaggi sono:

Iscriviti a un Account AWS

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

Per iscriverti a un Account AWS

1. Apri la https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

Nel corso della procedura di registrazione riceverai una telefonata o un messaggio di testo e ti verrà chiesto di inserire un codice di verifica attraverso la tastiera del telefono.

Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

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

Proteggi i tuoi Utente root dell'account AWS

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

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Accedere come utente root nella Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

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

Crea un utente con accesso amministrativo

1. Abilita il Centro identità IAM.

   Per istruzioni, consulta Abilitazione del AWS IAM Identity Center nella Guida per l'utente di AWS IAM Identity Center .
2. Nel Centro identità IAM, assegna l'accesso amministrativo a un utente.

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

Accesso come utente amministratore

- Per accedere come utente del Centro identità IAM, utilizza l'URL di accesso che è stato inviato al tuo indirizzo e-mail quando hai creato l'utente del Centro identità IAM.

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

Assegnazione dell'accesso ad altri utenti

1. Nel Centro identità IAM, crea un set di autorizzazioni conforme alla best practice per l'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .
2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

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

> **Note**
>
> Se hai già un account, puoi andare alla pagina dei AWS prezzi e fare clic su Crea un account gratuito. Assicurati di iscriverti almeno al servizio EC2. La registrazione a un servizio ti consente di accedere a tutti i servizi in AWS. Ti vengono addebitati solo i servizi che utilizzi. Se prevedi di collegare il tuo nuovo account a un conto di pagamento ai fini della fatturazione consolidata, non è necessario inserire le informazioni sul metodo di pagamento quando richiesto. Invece, una volta raggiunta la schermata per inserire i dati della carta di credito, è sufficiente allontanarsi. Avrai bisogno dell'indirizzo email associato all'account del pagatore per inviare una richiesta di billing/linked account consolidato, descritta in dettaglio nella sezione successiva.

Important

È fondamentale assicurarsi che un indirizzo e-mail e un numero di telefono siano associati all'account in modo da ricevere risposte a potenziali incidenti di sicurezza. Il numero di telefono e l'indirizzo e-mail dell'account non possono essere modificati senza reimpostare la password dell'account, il che rappresenta un impegno importante per un account root AMS. Per garantire che questi valori siano stabili, è fondamentale selezionare informazioni di contatto non associate a singoli individui, che possono cambiare. Scegli un alias email che possa puntare a un gruppo. Segui la stessa procedura consigliata per la selezione di un numero di telefono: scegli un numero che possa indirizzare a un gruppo o a un numero di proprietà dell'azienda e non a un individuo.

Configura la fatturazione consolidata: collega il nuovo account all'account Payer

Se desideri che la tua nuova Account AWS fattura gestita da AMS venga aggiunta a un pagamento per un account di AWS Organizations gestione esistente, devi configurare la fatturazione consolidata e collegare gli account. Per ulteriori informazioni su questa operazione, consulta

- Fatturazione consolidata AWS Organizations e strategia di fatturazione AWS multiaccount.
- Invitare un uomo a entrare a far parte della tua organizzazione Account AWS

Note

Puoi eseguire questi passaggi prima di passare la consegna dell'account ad AMS. Dopo il passaggio di consegne, i passaggi per entrare a far parte dell'organizzazione (indicati sopra) possono essere eseguiti tramite il processo di gestione delle modifiche. Se hai bisogno di assistenza, rivolgiti al tuo cloud service delivery manager (CSDM) o al cloud architect (CA).

Per informazioni generali sulla fatturazione, inclusa la gestione della fatturazione consolidata, consulta Cos'è la fatturazione. AWS Per AWS Organizations informazioni generali su come gli account possono lavorare insieme, vedi Cos'è. AWS Organizations Per indicazioni prescrittive sugli account di AWS Organizations gestione, consulta L'account di gestione, l'accesso affidabile e gli amministratori delegati

Configura il tuo accesso Account AWS per AMS

Una volta completati i passaggi precedenti, hai assicurato con successo che i nuovi Account AWS costi associati vengano fatturati in modo appropriato. La fase finale del processo consiste nel consentire ad AMS l'accesso al nuovo account per la configurazione iniziale dello stack e per soddisfare le continue richieste di modifica e provisioning. Per i dettagli, leggi Accesso delegato tra AWS account utilizzando ruoli IAM. I passaggi di base sono descritti in questa sezione.

Attiva l'accesso al AWS sito

Per consentire agli utenti IAM di accedere alle informazioni e agli strumenti di fatturazione del tuo account, devi attivare la funzionalità.

Completare la procedura riportata di seguito.

1. Accedi a Console di gestione AWS con le credenziali del tuo account root (l'email e la password che hai usato per creare il tuo Account AWS). Non accedere con le tue credenziali utente IAM.

   Si apre la Console di gestione AWS home page.
2. Nella barra di navigazione in alto, apri il menu a discesa relativo al nome del tuo account, quindi scegli Il mio account.

   Si apre la home page di Fatturazione.
3. Scorri verso il basso fino all'area IAM User Access to Billing Information e fai clic su Modifica sul lato destro. *`The area does not appear unless you are logged in with root credentials`*.

   Si apre un'area di accesso Activate IAM.
4. Seleziona la casella di controllo e fai clic su Aggiorna.

   Ora puoi utilizzare le policy IAM per controllare le pagine alle quali un utente può accedere.

Per maggiori dettagli su questo processo in AWS, consulta Panoramica sulla gestione delle autorizzazioni di accesso.

Creare un ruolo IAM con accesso al AWS sito Web

AWS Identity and Access Management (IAM) è un servizio web che ti aiuta a controllare in modo sicuro l'accesso alle AWS risorse per i tuoi utenti. Utilizzi IAM per controllare chi può utilizzare AWS le tue risorse (autenticazione), quali risorse possono utilizzare e in che modo (autorizzazione).

1. Vai alla console di gestione IAM, fai clic su Ruoli nel riquadro di navigazione a sinistra.

   La pagina di gestione dei ruoli si apre con informazioni sui ruoli IAM, un'opzione Create role e un elenco di ruoli esistenti.

2. Fai clic su Crea ruolo.

   Viene visualizzata la pagina Crea ruolo Seleziona il tipo di entità affidabile. Fai clic su Altro Account AWS per aprire un'area delle impostazioni in basso.

   Inserisci l'ID dell'account affidabile AMS che ti è stato fornito da AMS.
   Lascia deselezionate le opzioni Richiedi ID esterno e Richiedi MFA.

3. Fare clic su Next: Permissions (Successivo: Autorizzazioni).

   Viene visualizzata la pagina Crea ruolo Allega criteri di autorizzazione con le opzioni per la creazione di una nuova politica, l'aggiornamento della pagina e la ricerca delle politiche esistenti. Viene fornito un elenco di politiche esistenti.

4. Seleziona la AdministratorAccesspolitica, quindi fai clic su Avanti: revisione.

   Viene visualizzata la pagina Crea ruolo: revisione.

5. Assegna un nome al nuovo ruolo aws_managedservices_onboarding_role e digita «AMS Onboarding Role» per la descrizione del ruolo. Rivedi le impostazioni per il nuovo ruolo e, se sei soddisfatto, fai clic su Crea ruolo.

   Si apre la pagina di gestione dei ruoli con il nuovo ruolo elencato.

Iscriviti a Marketplace AWS for EPS

Le recenti modifiche alla sicurezza degli endpoint di AMS (EPS) richiedono l'iscrizione a TrendMicro Deep Security tramite Marketplace AWS e l'accettazione dei termini del software.

TrendMicro offre due modelli di licenza: Per Protected Instance Hour e Bring your own License (BYOL).

- BYOL:
  1. Utilizzi la tua licenza che hai acquistato tramite canali esterni.
  2. È necessario fornire tutte le chiavi di licenza ad AMS per creare l'infrastruttura EPS. È possibile fornire un codice di attivazione che concede in licenza tutti i moduli o codici di attivazione individuali che autorizzano un determinato set di moduli. AMS crea solo i file di licenza che corrispondono ai codici di attivazione forniti. Poiché l'attivazione della licenza avviene durante l'onboarding, in presenza di un ingegnere capo AMS e del CSDM, puoi quindi condividere tali informazioni.
  3. Inoltre, è necessario abbonarsi all'abbonamento BYOL TrendMicro Market Place AMI. Vedi Trend Micro Deep Security (BYOL).
- Per ora di istanza protetta:
  1. In questo abbonamento, non è necessario disporre di alcuna licenza Trend acquistata in precedenza.
  2. Tuttavia, è necessario abbonarsi all'abbonamento Marketplace.
  3. In questo modello non è richiesta la condivisione delle chiavi di licenza con AMS, poiché l'utilizzo di Trend viene misurato automaticamente, incluso l'utilizzo della licenza software e EC2 dell'infrastruttura. Vedi Trend Micro Deep Security.

Per abbonarti a Trend Micro, segui questi passaggi:

1. Accedi al tuo Account AWS.
2. Vai alla pagina del prodotto Trend Micro Deep Security (BYOL o Per Protected Instance Hour).
3. Fai clic su Continua per iscriverti nel pannello a destra.
4. Fai clic su Accetta i termini nell'angolo in alto a destra.

Abilita IDS e IPS in Trend Micro Deep Security

Puoi richiedere che AMS abiliti Trend Micro Intrusion Detection System (IDS) e Intrusion Protection Systems (IPS), funzionalità non predefinite, per il tuo account.

A tale scopo, invia una richiesta di aggiornamento (Gestione | Altro | Altro | Aggiornamento) e includi un elenco di indirizzi e-mail per ricevere le notifiche IDS e IPS. Questi indirizzi vengono aggiunti a un argomento SNS del tuo account, che AMS crea per te.

> **Note**
>
> AMS non può aggiungere alcun servizio Trend Micro che possa interferire con la nostra capacità di fornire altri servizi AMS.

Fase successiva: Proteggi il nuovo account con l'autenticazione a più fattori (MFA) per l'utente root in AMS

Abbonati Marketplace AWS a CentOS 7.6

AMS ora fornisce CentOS 7 (x86_64), con Updates HVM venduto da CentOS.org, come AMI AMS. Per utilizzare questa AMI, devi sottoscrivere la licenza GRATUITA Cent OS e accettarla su tutti i tuoi account AMS.

Per iscriverti, vai Marketplace AWSe segui le istruzioni per l'iscrizione.

Non dovrai sostenere costi software per l'utilizzo di questo prodotto, ma sei comunque responsabile per gli altri AWS costi, incluso l'utilizzo. EC2 Se si tratta di un prodotto «Bring Your Own License», è necessario disporre di una licenza software valida per poterlo utilizzare.

È possibile consultare le informazioni per questo software su CentOS 7 (x86_64), con Updates HVM.

Proteggi il nuovo account con l'autenticazione a più fattori (MFA) per l'utente root in AMS

Questa sezione è stata redatta perché contiene informazioni sensibili relative alla sicurezza di AMS. Queste informazioni sono disponibili nella documentazione della console AMS. Per accedere ad AWS Artifact, puoi contattare il tuo CSDM per ricevere istruzioni o andare alla pagina Getting Started with AWS Artifact.

SALZ: configura la rete

Esistono diversi processi che devono essere completati per configurare il networking per AWS Managed Services (AMS):

1. Allocazione dello spazio IP per l'ambiente AMS
2. Stabilire la connettività di rete privata con AWS
3. Configurazione del firewall per consentire le operazioni AMS

Alloca lo spazio IP per il tuo ambiente AMS

AMS è stato progettato e testato utilizzando un blocco CIDR /16 come allocazione di rete consigliata. È importante che la rete affidabile connessa ad AMS utilizzi un blocco CIDR che non si sovrapponga al blocco CIDR assegnato ad AMS. Questi indirizzi sono necessari per configurare il cloud privato virtuale (VPC) e le sottoreti. Per ulteriori informazioni su AWS VPCs, consulta Amazon VPC Limits e Amazon VPC. FAQs

Sebbene un blocco CIDR /16 possa sembrare un sacco di indirizzi IP, un VPC, una volta creato, non può essere espanso. Quindi questa allocazione garantisce che il VPC gestito da AMS possa funzionare per un periodo considerevole. All'interno del blocco CIDR, è necessario allocare intervalli di indirizzi IP per almeno due sottoreti private e due sottoreti pubbliche.

AWS accetta la connettività all'ambiente AMS tramite funzionalità di rete privata virtuale (VPN) nativa di AWS. Da parte tua, ciò può essere ottenuto tramite AWS Direct Connect (DX), una VPN hardware o una VPN software. Per quanto riguarda AMS, utilizziamo la funzionalità Virtual Gateway di VPCs.

Componenti ambientali di base

Opzioni di Network-to-Amazon connettività VPC utente	
VPN hardware	Stabilisce una connessione VPN hardware dalle apparecchiature di rete su una rete remota alle apparecchiature di rete gestite da AMS collegate al VPC.
AWS Direct Connect (DX)	Stabilisce una connessione privata, logica (o crittografata se utilizzata con una VPN) dalla

Opzioni di Network-to-Amazon connettività VPC utente	
	rete remota ad Amazon VPC, sfruttando AWS Direct Connect.
Software VPN	Stabilisce una connessione VPN dalle apparecchiature su una rete remota a un'applia nce VPN software gestita dall'utente in esecuzione all'interno di un Amazon VPC.

> **Note**
>
> AMS consiglia connessioni private ridondanti da VPN a DX. Il tuo responsabile della fornitura del servizio clienti (CSDM) ti aiuterà a configurare questa configurazione al momento dell'onboarding del tuo account.

Stabilisci la connettività di rete privata con AWS

Aggiungi AMS all'Active Directory aziendale per stabilire la connettività. Potresti voler eseguire azioni amministrative o l'accesso degli utenti tramite una connessione di rete privata. AWS offre sia connettività VPN che linee dedicate tramite Direct Connect. I passaggi seguenti spiegano come lavorare con AMS per stabilire uno (o entrambi) i mezzi di connettività.

Configurazione VPN

Questa sezione descrive i passaggi di base per configurare una VPN per comunicare tra il VPC gestito da AMS e la rete interna.

> **Note**
>
> Per informazioni generali sull'utilizzo di una VPN con i servizi AWS, consulta What is AWS Site-to-Site VPN and all about Your Customer Gateway (il tuo dispositivo VPN).

Segui le sezioni Getting Started and Testing the Site-to-Site VPN Connection della AWS VPN User Guide per completare i seguenti passaggi.

- Fase 1: Nel tuo VPC AWS, crea un Customer Gateway
- Fase 2: Nel tuo VPC AWS, crea un gateway privato virtuale
- Fase 3: Nel tuo VPC AWS, abilita la propagazione delle rotte nella tabella delle rotte
- Fase 4: Nel tuo AWS VPC, aggiorna il tuo gruppo di sicurezza per abilitare l'accesso SSH, RDP e ICMP in entrata
- Fase 5: Nella rete interna, crea una connessione VPN e configura il Customer Gateway
- Passaggio 6: verifica la connettività VPN tra il VPC e la rete interna

Direct Connect Configurazione

Questa sezione descrive i passaggi di base per configurare un Direct Connect (DX) per comunicare tra il VPC gestito da AMS e la rete interna.

> **Note**
>
> Per informazioni sull'utilizzo di un DX con i servizi AWS, consulta Getting Started at an Direct Connect Location.

Per configurare una connessione DX, devi completare i seguenti passaggi:

1. Iscriviti ad Amazon Web Services
2. Invia una richiesta di connessione AWS Direct Connect
3. Completa il Cross Connect
4. (Facoltativo) Configurazione di connessioni ridondanti con AWS Direct Connect
5. Eseguita da AMS: creazione di un'interfaccia virtuale
6. Eseguita da AMS: scarica la configurazione del router
7. Verifica la tua interfaccia virtuale

Configura il tuo firewall

Questa sezione è stata redatta perché contiene informazioni sensibili relative alla sicurezza di AMS. Queste informazioni sono disponibili nella documentazione della console AMS. Per accedere ad AWS

Artifact, puoi contattare il tuo CSDM per ricevere istruzioni o andare alla pagina Getting Started with AWS Artifact.

Opzioni AMS Bastion durante le migrazioni e l'onboarding delle applicazioni

Per offrirti la migliore esperienza durante le operazioni di migrazione, di seguito sono elencate le potenziali opzioni che AMS potrebbe attualmente sfruttare:

- Opzione 1: bypass Bastions solo per motivi di migrazione (è necessario sottoscrivere questa opzione per motivi di sicurezza come misura temporanea).

  Nota: le funzionalità di controllo continueranno a essere disponibili per garantire che AMS abbia visibilità su ogni richiesta.
- Opzione 2: tunneling SSH con uno strumento a scelta, ad esempio PuTTy, come illustrato.

  I componenti ambientali descritti dovrebbero già essere presenti per questa opzione.

  AMS fornirebbe note e istruzioni aggiuntive.

Fasi di tunneling SSH con Pu: TTy

All'interno di PuTTY, è necessario creare una sessione SSH, con l'IP pubblico dell'host bastion, fornire la chiave PEM nella sezione AUTH e quindi creare un tunnel. La porta di origine del tunnel dovrebbe essere una porta locale inutilizzata (ad esempio 5000) e l'IP dovrebbe essere l'IP dell'host di destinazione (la casella di Windows che stai cercando di raggiungere) con la porta RDP aggiunta (3389). Assicurati di salvare la configurazione, in quanto non vorrai doverla fare ogni volta che accedi alla casella. Connect al bastion host ed effettua il login. Quindi, avvia una sessione RDP per localhost:5000 (o qualsiasi porta tu scelga).

1. Imposta il nome host o l'IP pubblico dell'host bastion

2. In SSH ->Auth, imposta il file della chiave privata in formato.ppk

3. In SSH ->Tunnels, aggiungi la nuova porta inoltrata. La porta di origine dovrebbe essere la porta arbitraria non utilizzata e la destinazione dovrebbe essere l'IP del server di destinazione dietro l'host bastion, con la porta RDP aggiunta.

4. Connect all'host bastion tramite PuTTY e accedi.

5. Avvia una sessione RDP su localhost:5000 per raggiungere il server di destinazione.

SALZ: configura la gestione degli accessi

Utilizzare una rete gestita da AWS Managed Services (AMS) significa concedere ad AMS l'accesso per gestire la tua infrastruttura cloud. Dovrai configurare un mezzo per connetterti in modo sicuro tra la tua rete privata e AMS. Questo inizia con alcune decisioni sui tipi di accesso che desideri fornire:

- Per l'accesso ad AMS API/CLI e console: ti consigliamo di installare l'AMS CLI (le istruzioni sono fornite in questo documento). Utilizzi l'API di gestione delle modifiche AMS per effettuare richieste di modifica ad AMS e l'API AMS SKMS per conoscere le tue risorse gestite da AMS. Utilizzando Active Directory Federation Services (AD FS), puoi accedere alla console AMS.

  > **Note**
  >
  > Se stai configurando il tuo ITSM, dovrai utilizzare l'API AWS Support (SAPI) per le richieste di servizio e i report sugli incidenti. SAPI è documentato nel AWS Support API Reference.

- Per l'accesso degli utenti: indipendentemente dal fatto che gestiate gli utenti con Windows Active Directory (AD) o una Linux/LDAP soluzione, è necessario stabilire la connettività tra AD sul lato AMS (tramite Directory Services) e la directory.
- Ad esempio, accesso: l'accesso a livello di istanza viene ottenuto tramite una configurazione Forest Trust unidirezionale. Directory Services considera affidabili le credenziali presenti nel proprio programma CORP AD, permettendo agli stack presenti sul lato AMS di consentire l'accesso con credenziali CORP.

  Tieni presente che l'Active Directory (AD) su cui AMS imposta il trust deve essere la directory che contiene gli account degli utenti da te autorizzati ad accedere alle tue risorse AWS.

> **Important**
>
> Per configurare un Forest Trust, AMS richiede il controller di dominio Local Policies -> Security Options -> Network Access: Named Pipes a cui è possibile accedere in modo anonimo, con le pipe Netlogon e lsarpc elencate. Queste pipe sono elencate di default, ma a

volte vengono rimosse per motivi di sicurezza. Una volta stabilita la fiducia, possono essere nuovamente rimosse dall'elenco.

Stabilire un trust Active Directory (AD)

Prima di iniziare a stabilire un trust Active Directory (AD) per il tuo account AWS Managed Services (AMS), assicurati che le porte firewall appropriate siano aperte.

La fiducia offerta dall'Active Directory gestito da AMS e dal servizio di directory aziendale consente di utilizzare le credenziali gestite dall'azienda per accedere alle istanze gestite da AMS per eseguire funzioni di sviluppo, test o amministrative.

La creazione di una connessione affidabile è un esercizio in due parti:

Innanzitutto, configura un inoltro condizionale, una configurazione DNS in modo che le query DNS sappiano a quale server DNS rivolgersi.

In secondo luogo, configura un trust, un costrutto di Active Directory (AD) per consentire l'accesso degli utenti di un dominio all'utilizzo delle risorse di un altro dominio.

Configurare lo spedizioniere condizionale

Segui questo articolo di Microsoft AD Assegna un server d'inoltro condizionale per un nome di dominio e usa queste impostazioni e scelte:

1. In AD DNS Manager -> Crea un nuovo spedizioniere condizionale, in Dominio DNS: utilizza il nome di dominio che AMS ti ha fornito; ad esempio,. *A523434123.amazonaws.com*
2. In Indirizzi IP dei server master: aggiungi gli indirizzi IP forniti da AMS. Assicurati che non ci siano problemi di connessione convalidando entrambi gli indirizzi.
3. Seleziona Archivia questo server d'inoltro condizionale in Active Directory e replica come segue: Tutti i server DNS in questo dominio e premi OK.

Configura la fiducia

Per configurare la fiducia per il tuo account AWS Managed Services (AMS), segui questo articolo di MicroSoft AD Crea un trust forestale unidirezionale, in entrata per un lato del trust, utilizzando le impostazioni e le scelte descritte in questa sezione.

1. Apri la finestra di dialogo Start -> Strumenti di amministrazione -> Active Directory Domains and Trust. Fate clic con il pulsante destro del mouse sul nodo del dominio con cui desiderate stabilire un trust, quindi fate clic su Proprietà -> Trust -> New Trust per aprire la procedura guidata New Trust. Inserisci il nome di dominio fornito da AMS per il Trust Name e premi Avanti.
2. In Tipo di fiducia, seleziona Forest Trust. Premere Next (Successivo).
3. In Direction of Trust, seleziona Unidirezionale: in arrivo. Premere Next (Successivo).
4. In Sides of Trust, seleziona Solo questo dominio. Premere Next (Successivo).
5. In Trust Password, digita una password a tua scelta. Premere Next (Successivo).
6. Per Trust Selections Completed e Trust Creation Complete, basta premere Avanti.
7. In Conferma l'attendibilità in entrata, seleziona No, non confermare l'attendibilità in entrata. Premere Next (Successivo).
8. In Completato il New Trust Wizard, seleziona Fine, quindi OK per chiudere.
9. Fornisci la password affidabile (contattaci tramite il numero di telefono del tuo CSDM per motivi di sicurezza). AMS completerà la configurazione di fiducia.

Siti e servizi Active Directory

Per ridurre la latenza di accesso, aggiungi l'intervallo VPC CIDR ai tuoi siti e servizi di Active Directory (Start -> Strumenti di amministrazione -> Siti e servizi di Active Directory). Aggiungi l'intervallo VPC CIDR a un sito di Active Directory che contiene i controller di dominio più vicini ad AWS.

Routing dei suffissi dei nomi di Active Directory

Dopo aver istituito il trust forestale unidirezionale, completa i passaggi aggiuntivi.

1. In Start > Tutti i programmi > Strumenti di amministrazione, fai clic su Domini e trust di Active Directory.

   Si apre la console Active Directory Domains and Trust.
2. Fai clic con il pulsante destro del mouse sul dominio aziendale e scegli Proprietà

   Si apre la finestra di dialogo Proprietà relativa a quel dominio.
3. Fai clic sulla scheda Trust.

   Si apre la pagina Trust.

4. Fai clic sul nome di dominio Amazon, quindi su Proprietà.

   Si apre la pagina delle proprietà per il dominio Amazon Trust.
5. Fai clic su Name Suffix Routing e clicca su Aggiorna.

   Questi passaggi assicurano che Service Principal Names (SPNs) possa prevalere sul trust.

Risoluzione dei problemi

Alcune cose da provare in caso di problemi:

- È necessario consentire la connessione al gruppo di sicurezza in uscita di Active Directory gestito da AMS tramite il blocco CIDR (ad esempio 10.27.0.0/16) al controller di dominio.
- Traccia il percorso nella console AWS da controller di dominio a controller di dominio controllando tutti i gruppi di sicurezza lungo il percorso.
- Assicurati di poter eseguire il ping dei controller di dominio Active Directory gestiti da AMS se Internet Control Message Protocol (ICMP) è consentito.
- Assicurati che il tuo controller di dominio sia in grado di comunicare con AWS Directory Services.
- Assicurati che i server d'inoltro condizionali si risolvano e siano convalidati.
- Se non vedi Forest Trust nella procedura guidata New Trust, è possibile che i tuoi inoltratori condizionali non funzionino correttamente:
  - Usa nslookup per testare la risoluzione
  - Prova a riavviare il controller di dominio

Active Directory gestita da AMS

AMS offre ora un nuovo servizio chiamato Managed Active Directory (aka Managed AD) che consente ad AMS di occuparsi delle operazioni dell'infrastruttura Active Directory (AD), mantenendo al contempo il controllo dell'amministrazione di Active Directory.

Il supporto AMS per Managed AD è simile al supporto AMS per Amazon Relational Database Service (Amazon RDS). In entrambi i casi, AWS (incluso AMS) supporta la creazione e la gestione dell'infrastruttura che esegue il servizio, mentre tu esegui il controllo degli accessi e tutte le funzioni di amministrazione. Questo modello presenta i seguenti vantaggi:

- Limita i rischi per la sicurezza: AWS e AMS non necessita di privilegi amministrativi per il tuo dominio.

- Integrazioni dirette: puoi utilizzare il tuo modello di autorizzazione attuale e integrarlo con AD senza bisogno di interfacciarti con AMS.

Note:

- Né AMS né l'utente avranno accesso ai controller di dominio Managed AD, quindi nessun software può essere installato sui controller di dominio. Questo è importante perché non sono consentite soluzioni di terze parti che richiedono l'installazione di software sui controller di dominio.

  Access funziona in questo modo:

  - AWS Team di Directory Service: ha accesso ai controller di dominio.
  - AMS: ha accesso al Directory Service APIs per eseguire determinate azioni sul dominio. Queste azioni includono l'acquisizione di istantanee AD, la modifica dello schema AD e altre azioni.
  - Tu: hai accesso al dominio (AD) per creare utenti, gruppi e così via.
- Si consiglia di eseguire una prova di fattibilità su Managed AD prima di migrare l'AD aziendale, poiché non tutte le funzionalità di un ambiente AD tradizionale sono disponibili in un ambiente AD gestito.
- AMS non gestirà né fornirà indicazioni sulla gestione di AD. Ad esempio, AMS non fornirà indicazioni sulla struttura delle unità organizzative, sulla struttura delle politiche di gruppo, sulle convenzioni di denominazione degli utenti di AD e così via.

Funziona così:

1. AMS integra Account AWS per te un nuovo account AMS, separato e in aggiunta al tuo account AMS, e fornisce un ambiente Active Directory (AD) tramite AWS Directory Service (vedi anche What Is AWS Directory Service?).

   Di seguito sono riportate le informazioni che un integratore di sistemi dovrebbe raccogliere dall'utente per consentire ad AMS di entrare a far parte di Managed AD:

   - Informazioni sull'account
     - ID dell'account creato per Account AWS il tuo AD gestito da AMS: numero Account AWS
     - Regione in cui effettuare l'onboarding del tuo AD gestito per: Regione AWS
   - Informazioni gestite su Active Directory:
     - Edizione Microsoft AD: Standard/Enterprise. AWS Microsoft AD (Standard Edition) include 1 GB di storage di oggetti di directory. Questa capacità può supportare fino a 5.000 utenti o

30.000 oggetti di directory, inclusi utenti, gruppi e computer. AWS Microsoft AD (Enterprise Edition) include 17 GB di storage di oggetti di directory, in grado di supportare fino a 100.000 utenti o 500.000 oggetti.

Per ulteriori informazioni, consulta AWS Directory Service FAQs.

- Nome di dominio completo: il nome di dominio completo per il dominio AMS Managed AD.
- Nome NetBIOS del dominio: il nome NetBIOS per il dominio AMS Managed AD.
- Numeri di account degli account AMS-Standard in cui desideri l'integrazione con Managed AD (AMS configura un trust unidirezionale dall'AD dell'account AMS-Standard a Managed AD)
- Sono necessarie modifiche allo schema di Active Directory e, in caso affermativo, quali modifiche?
- Per impostazione predefinita, vengono forniti due controller di dominio. Ne hai bisogno di più? In caso affermativo, quanti ne servono e per quale motivo?

- Informazioni sulla rete per Managed Active Directory:
  - CIDR AD VPC gestito per controller di dominio (un CIDR nell'intervallo di sottoreti privato per i controller di dominio AD gestiti):
    - Subnet CIDR 1 per controller di dominio: [il tuo CIDR, deve far parte di AMS Managed AD VPC CIDR]
    - Subnet CIDR 2 per controller di dominio: [il tuo CIDR, deve far parte di AMS Managed AD VPC CIDR]

    Ad esempio:

    - CIDR AD VPC gestito: 192.168.0.0/16
    - CIDR 1 per controller di dominio: 192.168.1.0/24
    - CIDR 2 per controller di dominio: 192.168.2.0/24

    Per evitare conflitti di indirizzi IP, assicurati che il CIDR VPC AD gestito che hai specificato non sia in conflitto con nessun'altra sottorete privata CIDR che stai utilizzando nella tua rete aziendale.
  - Tecnologia VPN (opzionale): [Direct Connect/Direct Connect e VPN]
    - Numero di sistema autonomo (ASN) BGP del gateway: [ASN fornito dal cliente]
    - L'indirizzo IP indirizzabile su Internet per l'interfaccia esterna del gateway, l'indirizzo deve essere statico: [Indirizzo IP fornito dal cliente]

- Indipendentemente dal fatto che la connessione VPN richieda o meno percorsi statici: [sì/no]

2. AMS ti fornisce la password dell'account amministratore per l'ambiente AD e ti chiede di reimpostare la password in modo che i tecnici AMS non possano più accedere al tuo ambiente AD.
3. Per reimpostare la password dell'account Admin, connettiti all'ambiente Active Directory utilizzando Active Directory Users and Computers (ADUC). ADUC e altri strumenti di amministrazione remota del server (RSAT) devono essere installati ed eseguiti su host amministrativi forniti dall'utente su un'infrastruttura non AMS. Microsoft utilizza le best practice per proteggere tali host amministrativi. Per informazioni, vedi Implementazione di host amministrativi sicuri. È possibile gestire l'ambiente Active Directory utilizzando questi host amministrativi.
4. Nelle operazioni quotidiane, AMS gestisce il Account AWS lato più completo dei AWS Directory Service, ad esempio la configurazione VPC, i backup AD, la creazione e l'eliminazione di trust AD e così via. L'utente utilizza e gestisce l'ambiente AD, ad esempio la creazione di utenti, la creazione di gruppi, la creazione di policy di gruppo e così via.

Per la tabella RACI più recente, vedere la sezione «Ruoli e responsabilità» nella descrizione del servizio.

Federa il tuo Active Directory con i ruoli AMS AWS Identity and Access Management

Lo scopo della federazione della directory con i ruoli AMS IAM è consentire agli utenti aziendali di utilizzare le proprie credenziali aziendali per interagire con la Console di gestione AWS e, quindi AWS APIs, la console AMS e. APIs

Esempio di processo di federazione

Questo esempio utilizza Active Directory Federation Services (AD FS); tuttavia, è supportata qualsiasi tecnologia che supporti AWS Identity and Access Management Federation. Per ulteriori informazioni sulla federazione IAM AWS supportata, consulta IAM Partners and Identity Providers and Federation. Il CSDM ti aiuterà in questo processo, che prevede uno sforzo congiunto con il tuo team AD e AMS.

Per informazioni dettagliate sull'integrazione di SAML per l'accesso alle API, consulta questo AWS blog, How to Implementated Federated API and CLI Access Using SAML 2.0 e AD FS.

> **Note**
>
> Per un esempio che installa AMS CLI e SAML, vedi. Appendice: Regola di reclamo di ActiveDirectory Federation Services (ADFS) e impostazioni SAML

Configurazione della federazione sulla console AMS (SALZ)

I ruoli IAM e il provider di identità SAML (Trusted Entity) descritti nella tabella seguente sono stati forniti come parte dell'onboarding dell'account. Questi ruoli ti consentono di inviare e monitorare RFCs richieste di assistenza e segnalazioni di incidenti, nonché di ottenere informazioni sui tuoi stack e sugli stack. VPCs

Ruolo	Provider di identità	Autorizzazioni
Cliente_ _Ruolo ReadOnly	SAML	Per account AMS standard. Consente di inviare o apportare modifiche RFCs all'infrastruttura gestita da AMS, nonché di creare richieste di servizio e incidenti.
customer_managed_ad_user_role	SAML	Per gli account AMS Managed Active Directory. Consente di accedere alla console AMS per creare richieste di servizio e incidenti (no RFCs).

Per l'elenco completo dei ruoli disponibili con diversi account, consultaRuolo utente IAM in AMS.

Un membro del team di onboarding carica il file di metadati dalla soluzione di federazione al provider di identità preconfigurato. Utilizzi un provider di identità SAML quando desideri stabilire un rapporto di fiducia tra un IdP (provider di identità) compatibile con SAML come Shibboleth o Active Directory Federation Services, in modo che gli utenti della tua organizzazione possano accedere alle risorse AWS. I provider di identità SAML in IAM vengono utilizzati come principali in una policy di fiducia IAM con i ruoli sopra indicati.

Mentre altre soluzioni di federazione forniscono istruzioni di integrazione per AWS, AMS fornisce istruzioni separate. Utilizzando il seguente post di blog, Enabling Federation to AWS Using Windows

Active Directory, AD FS e SAML 2.0, insieme alle modifiche riportate di seguito, consentirai agli utenti aziendali di accedere a più account AWS da un unico browser.

Dopo aver creato il relying party trust come indicato nel post del blog, configura le regole relative ai reclami nel modo seguente:

- NameId: Segui il post del blog.
- RoleSessionName: Utilizza i seguenti valori:
  - Nome della regola di rivendicazione: RoleSessionName
  - Archivio attributi: Active Directory
  - Attributo LDAP: SAM-Account-Name
  - Tipo di reclamo in uscita: Attributi/ https://aws.amazon.com/SAML/ RoleSessionName
- Ottieni gruppi di annunci: segui il post del blog.
- Dichiarazione di ruolo: segui il post del blog, ma per la regola personalizzata, usa questo:

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
 => issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-",
 "arn:aws:iam::$1:saml-provider/customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Quando utilizzi AD FS, devi creare gruppi di sicurezza Active Directory per ogni ruolo nel formato mostrato nella tabella seguente (customer_managed_ad_user_role è solo per gli account AMS Managed AD):

Group (Gruppo)	Ruolo
AWS- [AccountNo] ReadOnly -Customer_ _Ruolo	Cliente_ _Ruolo ReadOnly
AWS- [AccountNo] -customer_managed_ ad_user_role	customer_managed_ad_user_role

Per ulteriori informazioni, consulta Configurazione delle asserzioni SAML per la risposta di autenticazione.

> **Tip**
>
> Per facilitare la risoluzione dei problemi, scarica il plug-in SAML tracer per il tuo browser.

Invio della richiesta di federazione ad AMS

Se questo è il tuo primo account, collabora con i tuoi CSDM and/or Cloud Architect per fornire il file XML di metadati per il tuo provider di identità.

Se stai effettuando l'onboarding di un account o di Identity Provider aggiuntivo e hai accesso all'account di gestione o all'account dell'applicazione desiderato, segui questi passaggi.

1. Crea una richiesta di servizio dalla console AMS, fornisci i dettagli necessari per aggiungere il provider di identità:
   - AccountId dell'account in cui verrà creato il nuovo provider di identità.
   - Il nome del provider di identità desiderato, se non viene fornito, il valore predefinito sarà customer-saml; in genere, deve corrispondere alle impostazioni configurate nel provider della federazione.
   - Per gli account esistenti, indica se il nuovo provider di identità deve essere propagato a tutti i ruoli di console esistenti o fornisci un elenco di ruoli che dovrebbero considerare attendibile il nuovo provider di identità.
   - Allega il file XML di metadati esportato dal tuo agente federativo alla richiesta di servizio come file allegato.
2. Dallo stesso account in cui hai creato la richiesta di servizio, crea un nuovo RFC utilizzando CT-ID ct-1e1xtak34nx76 (Gestione | Altro | Altro | Crea) con le seguenti informazioni.
   - <Name>Titolo: «IDP SAML integrato per account < >». AccountId
   - AccountId dell'account in cui verrà creato il provider di identità.
   - Nome del provider di identità.
   - Per gli account esistenti: indica se il provider di identità deve essere propagato a tutti i ruoli di console esistenti o l'elenco dei ruoli che devono considerare attendibile il nuovo provider di identità.
   - ID del caso della richiesta di servizio creata nel passaggio 1, in cui è allegato il file XML di metadati.

Verifica l'accesso alla console

Dopo aver configurato ADFS e aver ottenuto l'URL AMS da utilizzare per l'autenticazione, segui questi passaggi.

Con una configurazione Active Directory Federated Service (ADFS), puoi seguire questi passaggi:

1. Apri una finestra del browser e vai alla pagina di accesso fornita per il tuo account. Si apre la IdpInitiatedSignOnpagina ADFS relativa al tuo account.
2. Seleziona il pulsante di opzione accanto a Accedi a uno dei seguenti siti. L'elenco di selezione del sito Accedi diventa attivo.
3. Scegli il sito signin.aws.amazon.com e fai clic su Accedi. Le opzioni per l'immissione delle credenziali sono aperte.
4. Inserisci le tue credenziali CORP e fai clic su Accedi. Le Console di gestione AWS aperture.
5. Incolla nella barra degli indirizzi l'URL della console AMS e premi Invio. La console AMS si apre.

Verifica l'accesso all'API

AMS utilizza l'API AWS, con alcune operazioni specifiche di AMS di cui puoi leggere nell'AMS API Reference.

AWS ne fornisce diversi a SDKs cui puoi accedere tramite Tools for Amazon Web Services. Se non desideri utilizzare un SDK, puoi effettuare chiamate API dirette. Per informazioni sull'autenticazione, consulta Signing AWS API Requests. Se non utilizzi un SDK o non effettui richieste API HTTP dirette, puoi utilizzare AMS CLIs for Change Management (CM) e SKMS.

Installa l'AMS CLIs

Per un esempio di installazione della CLI AWS Managed Services (AMS) da utilizzare con SAML, consulta. Appendice: Regola di reclamo di ActiveDirectory Federation Services (ADFS) e impostazioni SAML

Se hai bisogno di un accesso temporaneo, per ottenere e installare AWS Managed Services (AMS) SDKs, consulta Accesso temporaneo alla console AMS.

> **Note**
>
> È necessario disporre delle credenziali di amministratore per questa procedura.

L'AWS CLI è un prerequisito per l'utilizzo di AWS Managed Services (AMS) CLIs (Change Management and SKMS).

1. Per installare l'AWS CLI, consulta Installazione dell'interfaccia a riga di comando AWS e segui le istruzioni appropriate. Nota che nella parte inferiore di quella pagina ci sono istruzioni per l'uso di diversi programmi di installazione, Linux, MS Windows, macOS, Virtual Environment, Bundled Installer (Linux, macOS o Unix).

   Dopo l'installazione, esegui per verificare l'installazione. `aws help`
2. Una volta installata la CLI di AWS, per installare o aggiornare la CLI di AMS, scarica il file zip distribuibile AMS AMS CLI o AMS SDK distribuibile e decomprimilo. Puoi accedere ai file distribuibili della CLI AMS tramite il link Risorse per sviluppatori nel menu di navigazione a sinistra della console AMS.
3. Il file README fornisce istruzioni per qualsiasi installazione.

   Apri uno dei due:

   - CLI zip: fornisce solo la CLI AMS.
   - SDK zip: fornisce tutto l'AMS APIs e la CLI AMS.

   Per Windows, esegui il programma di installazione appropriato (solo sistemi a 32 o 64 bit):

   - 32 bit: API_x86.msi ManagedCloud
   - 64 bit: API_x64.msi ManagedCloud

   Per Mac/Linux, esegui il file denominato: AWSManagedServices_InstallCLI.sh eseguendo questo comando:. `sh AWSManagedServices_InstallCLI.sh` Nota che le directory amscm e amsskms e il loro contenuto devono trovarsi nella stessa directory del file.sh. AWSManagedServices_InstallCLI
4. Se le credenziali aziendali vengono utilizzate tramite la federazione con AWS (la configurazione predefinita di AMS), è necessario installare uno strumento di gestione delle credenziali in grado di accedere al servizio di federazione. Ad esempio, puoi utilizzare questo AWS Security Blog How to Implementation Federated API and CLI Access Using SAML 2.0 e AD FS per aiutarti a configurare i tuoi strumenti di gestione delle credenziali.
5. Dopo l'installazione, esegui e visualizza i comandi `aws amscm help` e le opzioni`aws amsskms help`.

> **Note**
>
> Affinché questi comandi funzionino, è necessario installare l'AMS CLI. Per installare l'API o la CLI AMS, vai alla pagina Risorse per gli sviluppatori della console AMS. Per materiale di riferimento sull'API AMS CM o sull'API AMS SKMS, consulta la sezione AMS Information Resources nella Guida per l'utente. Potrebbe essere necessario aggiungere un'`--profile`opzione per l'autenticazione, `aws amsskms` *`ams-cli-command`* `--profile SAML` ad esempio. Potrebbe essere necessario aggiungere l'`--region`opzione anche perché tutti i comandi AMS non utilizzano us-east-1, ad esempio. `aws amscm` *`ams-cli-command`* `--region=us-east-1`

Pianificazione dei backup AMS a livello di VPC

La pianificazione del backup di AWS Managed Services (AMS) nel VPC, dove vengono allocate le istanze di destinazione, viene creata durante l'onboarding dell'account con un tag predefinito nello schema di creazione del VPC. Il sistema di backup pianifica l'esecuzione delle istantanee in base al tag VPC. La modifica della pianificazione può essere effettuata creando una richiesta di servizio. Per ulteriori informazioni, consulta Tag e impostazioni predefinite VPC.

Per le impostazioni predefinite di backup, consulta Understanding AMS Defaults

SALZ: impostazioni predefinite

La tua rete AWS Managed Services (AMS) è configurata in modo standardizzato con impostazioni predefinite per la maggior parte dei servizi.

Questa sezione descrive le impostazioni predefinite utilizzate da AMS per la sicurezza, l'accesso, il monitoraggio, la registrazione, la continuità, l'applicazione di patch e la gestione.

Per un esempio dei costi dell'infrastruttura, consulta Componenti di base.

Le regole del firewall sono disponibili in Configura il tuo firewall

Sicurezza degli endpoint (EPS)

Le risorse fornite nell'ambiente AMS Advanced includono automaticamente l'installazione di un client di monitoraggio della sicurezza degli endpoint (EPS). Questo processo garantisce che le risorse

gestite da AMS Advanced siano monitorate e supportate 24 ore su 24, 7 giorni su 7. Inoltre, AMS Advanced monitora tutte le attività degli agenti e, se viene rilevato un evento di sicurezza, si crea un incidente.

> **Note**
>
> Gli incidenti di sicurezza vengono gestiti come incidenti; per ulteriori informazioni, consulta Risposta agli incidenti.

La sicurezza degli endpoint fornisce una protezione antimalware, in particolare sono supportate le seguenti azioni:

- EC2 le istanze vengono registrate con EPS
- EC2 le istanze vengono annullate dalla registrazione di EPS
- EC2 istanze di protezione antimalware in tempo reale
- battito cardiaco avviato dall'agente EPS
- EPS ripristina il file in quarantena
- Notifica degli eventi EPS
- Reportistica EPS

AMS Advanced utilizza Trend Micro per la sicurezza degli endpoint (EPS). Queste sono le impostazioni EPS predefinite. Per ulteriori informazioni su Trend Micro, consulta il Trend Micro Deep Security Help Center; tieni presente che i link non Amazon possono cambiare senza preavviso.

Le impostazioni predefinite di AMS Advanced Multi-Account Landing Zone (MALZ) sono descritte nelle seguenti sezioni; per le impostazioni EPS non predefinite di AMS Multi-Account Landing Zone EPS, vedere Impostazioni non predefinite di AMS Advanced Multi-Account Landing Zone EPS.

> **Note**
>
> Puoi portare il tuo EPS, vedi AMS porta il tuo EPS.

Impostazioni generali EPS

Impostazioni generali di rete per la sicurezza degli endpoint.

Impostazioni predefinite EPS

Impostazione	Default
Porte firewall (gruppo di sicurezza delle istanze)	Gli agenti EPS Deep Security Manager (DSMs) devono avere la porta 4120 aperta Agent/Relay per la comunicazione con Manager e la porta 4119 per la console di gestione. I relè EPS devono avere la porta 4122 aperta per la Manager/Agent comunicazione verso Relay. Nessuna porta specifica deve essere aperta per le comunicazioni in entrata dell'istanza del cliente, poiché gli agenti avviano tutte le richieste.
Direzione della comunicazione	Agente/dispositivo avviato
Intervallo del battito cardiaco	Dieci minuti
Numero di battiti cardiaci mancati prima di un avviso	Due
Deriva massima consentita (differenza) tra gli orari del server	Illimitato
Genera errori offline per le macchine virtuali inattive (registrate, ma non online)	No
Politica predefinita	Politica di base (descritta di seguito)
Attivazione di più computer con lo stesso nome host	È consentita
Vengono generati avvisi per gli aggiornamenti in sospeso	Dopo sette giorni
Pianificazione dell'aggiornamento	AMS prevede un ciclo di rilascio mensile per gli aggiornamenti software Trend Micro Deep Security Manager (DSM) /Deep Security Agent (DSA). Tuttavia, AMS non mantiene uno

Impostazione	Default
	SLA per gli aggiornamenti. Gli aggiornamenti vengono eseguiti a livello di flotta dai team di sviluppatori AMS durante l'implementazione. Gli aggiornamenti DSA/DSA vengono registrati negli eventi del sistema Trend Micro DSM che AMS conserva localmente per impostazione predefinita per 13 settimane. Per la documentazione del fornitore, consulta Eventi di sistema nel Trend Micro Deep Security Help Center. I log vengono inoltre esportati nel gruppo di log aws/ams/eps/var/log/DSM /.log in Amazon. CloudWatch
Fonte dell'aggiornamento	Server di aggiornamento Trend Micro (https://ipv6-iaus.trendmicro.com/iau_server.dll/)
Eliminazione dei dati relativi a eventi o registri	Gli eventi e i registri vengono eliminati dal database DSM dopo sette giorni.
Le versioni del software Agent sono conservate	Fino a cinque
Vengono mantenuti gli aggiornamenti più recenti delle regole	Fino a dieci
Archiviazione dei registri	Per impostazione predefinita, i file di log vengono archiviati in modo sicuro in Amazon S3, ma puoi anche archiviarli su Amazon Glacier per soddisfare i requisiti di audit e conformità.

Politica di base

Impostazioni predefinite della policy di base per la sicurezza degli endpoint.

Politica di base EPS

Impostazione	Default
Moduli abilitati	Anti-malware
Moduli disabilitati	Reputazione Web
	Firewall
	Protezione dalle intrusioni
	Monitoraggio dell'integrità
	Ispezione dei registri
	Controllo delle applicazioni

Anti-malware

Impostazioni antimalware per la sicurezza degli endpoint.

Impostazioni predefinite anti-malware EPS

Impostazione	Default	Note
Scansione in tempo reale	Scansiona tutto	Metti in quarantena tutti i virus sospetti. Attivazione IntelliTrap e protezione. spyware/grayware Spyware e Grayware attivano Anti-Malware e mettono in quarantena l'articolo.
	Ogni giorno (24 ore) Day/All	
Scansione manuale	Scansiona tutto	Deve essere richiesto, quindi segue la configurazione di

Impostazione	Default	Note
		scansione in tempo reale predefinita.
Scansione pianificata	Scansiona tutto	Impostato per l'ultima domenica di ogni mese, alle 6 del mattino.
Protezione intelligente	Disabilitato	N/D
File in quarantena	Trend Micro Deep Security Manager (DSM)	Circa 1 GB di disco riservato per la quarantena.
Limitazione della scansione	Trend Micro DSM	Scansiona file di tutte le dimensioni.
Spyware o grayware consentiti	Nessuno	N/D
Notifica di eventi locali	Sì	N/D

Gruppi di sicurezza

In AWS VPCs, i gruppi di sicurezza AWS agiscono come firewall virtuali, controllando il traffico per uno o più stack (un'istanza o un insieme di istanze). Quando uno stack viene lanciato, viene associato a uno o più gruppi di sicurezza, che determinano a quale traffico è consentito raggiungerlo:

- Per gli stack nelle sottoreti pubbliche, i gruppi di sicurezza predefiniti accettano il traffico proveniente da HTTP (80) e HTTPS (443) da tutte le posizioni (Internet). Gli stack accettano anche traffico SSH e RDP interno dalla rete aziendale e dai bastioni AWS. Questi stack possono quindi uscire attraverso qualsiasi porta verso Internet. Possono inoltre accedere alle sottoreti private e ad altri stack della sottorete pubblica.
- Gli stack delle sottoreti private possono passare a qualsiasi altro stack della sottorete privata e le istanze all'interno di uno stack possono comunicare completamente tra loro tramite qualsiasi protocollo.

> **Important**
>
> Il gruppo di sicurezza predefinito per gli stack nelle sottoreti private consente a tutti gli stack della sottorete privata di comunicare con altri stack in quella sottorete privata. Se si desidera limitare le comunicazioni tra gli stack all'interno di una sottorete privata, è necessario creare nuovi gruppi di sicurezza che descrivano la restrizione. Ad esempio, se desiderate limitare le comunicazioni a un server di database in modo che gli stack di quella sottorete privata possano comunicare solo da un server di applicazioni specifico tramite una porta specifica, richiedete un gruppo di sicurezza speciale. In questa sezione viene descritto come eseguire questa operazione.

Gruppi di sicurezza predefiniti

MALZ

La tabella seguente descrive le impostazioni predefinite del gruppo di sicurezza in entrata (SG) per gli stack. L'SG si chiama "SentinelDefaultSecurityGroupPrivateOnly-VPC-ID», dove è *ID* un ID VPC nel tuo account di landing zone multi-account AMS. Tutto il traffico in uscita è consentito verso "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" tramite questo gruppo di sicurezza (è consentito tutto il traffico locale all'interno delle sottoreti dello stack).

Tutto il traffico in uscita è consentito a 0.0.0.0/0 da un secondo gruppo di sicurezza "». SentinelDefaultSecurityGroupPrivateOnly

> **Tip**
>
> Se scegli un gruppo di sicurezza per un tipo di modifica AMS, ad esempio EC2 create o OpenSearch create domain, utilizzerai uno dei gruppi di sicurezza predefiniti descritti qui o un gruppo di sicurezza creato da te. Puoi trovare l'elenco dei gruppi di sicurezza, per VPC, nella console AWS EC2 o nella console VPC.

Esistono gruppi di sicurezza predefiniti aggiuntivi che vengono utilizzati per scopi AMS interni.

Gruppi di sicurezza AMS predefiniti (traffico in entrata)

Tipo	Protocollo	Intervallo porte	Origine
Tutto il traffico	Tutti	Tutti	SentinelDefaultSecurityGroupPrivateOnly (limita il traffico in uscita ai membri dello stesso gruppo di sicurezza)
Tutto il traffico	Tutti	Tutti	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (non limita il traffico in uscita)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (Fonte 0.0.0.0/0) L'accesso SSH e RDP è consentito dai bastioni	SentinelDefaultSecurityGroupPublic (non limita il traffico in uscita)
Bastioni MALZ:			
SSH	TCP	22	SharedServices VPC CIDR e DMZ VPC CIDR, oltre a soluzioni on-premise fornite dal cliente CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
Bastioni SALZ:			
SSH	TCP	22	mc-initial-garden- SG LinuxBastion
SSH	TCP	22	mc-initial-garden- LinuxBastion DMSG
RDP	TCP	3389	mc-initial-garden- WindowsBastion SG
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMSG

SALZ

La tabella seguente descrive le impostazioni predefinite del gruppo di sicurezza in entrata (SG) per gli stack. L'SG è denominato "mc-initial-garden- SentinelDefaultSecurityGroupPrivateOnly -*ID*" dove *ID* è un identificatore univoco. Tutto il traffico in uscita è consentito verso "mc-initial-garden-SentinelDefaultSecurityGroupPrivateOnly" tramite questo gruppo di sicurezza (è consentito tutto il traffico locale all'interno delle sottoreti dello stack).

Tutto il traffico in uscita è consentito a 0.0.0.0/0 da un secondo gruppo di sicurezza "- -». mc-initial-garden SentinelDefaultSecurityGroupPrivateOnlyEgressAll *ID*

> **Tip**
>
> Se scegli un gruppo di sicurezza per un tipo di modifica AMS, ad esempio EC2 create o OpenSearch create domain, utilizzerai uno dei gruppi di sicurezza predefiniti descritti qui o un gruppo di sicurezza creato da te. Puoi trovare l'elenco dei gruppi di sicurezza, per VPC, nella console AWS EC2 o nella console VPC.

Esistono gruppi di sicurezza predefiniti aggiuntivi che vengono utilizzati per scopi AMS interni.

Gruppi di sicurezza AMS predefiniti (traffico in entrata)

Tipo	Protocollo	Intervallo porte	Origine
Tutto il traffico	Tutti	Tutti	SentinelDefaultSecurityGroupPrivateOnly (limita il traffico in uscita ai membri dello stesso gruppo di sicurezza)
Tutto il traffico	Tutti	Tutti	SentinelDefaultSecurityGroupPrivateOnlyEgressAll (non limita il traffico in uscita)
HTTP, HTTPS, SSH, RDP	TCP	80/443 (Fonte 0.0.0.0/0) L'accesso SSH e RDP è consentito dai bastioni	SentinelDefaultSecurityGroupPublic (non limita il traffico in uscita)

Tipo	Protocollo	Intervallo porte	Origine
Bastioni MALZ:			
SSH	TCP	22	SharedServices VPC CIDR e DMZ VPC CIDR, oltre a soluzioni on-premise fornite dal cliente CIDRs
SSH	TCP	22	
RDP	TCP	3389	
RDP	TCP	3389	
Bastioni SALZ:			
SSH	TCP	22	mc-initial-garden- SG LinuxBastion
SSH	TCP	22	mc-initial-garden- LinuxBastion DMSG
RDP	TCP	3389	mc-initial-garden- WindowsBastion SG
RDP	TCP	3389	mc-initial-garden- WindowsBastion DMSG

Creare, modificare o eliminare gruppi di sicurezza

È possibile richiedere gruppi di sicurezza personalizzati. Nei casi in cui i gruppi di sicurezza predefiniti non soddisfano le esigenze delle applicazioni o dell'organizzazione, è possibile modificare o creare nuovi gruppi di sicurezza. Tale richiesta sarebbe considerata obbligatoria per l'approvazione e verrebbe esaminata dal team operativo AMS.

Per creare un gruppo di sicurezza al di fuori degli stack VPCs, invia una RFC utilizzando il tipo di `Deployment | Advanced stack components | Security group | Create (managed automation)` modifica (ct-1oxx2g2d7hc90).

Per le modifiche ai gruppi di sicurezza Active Directory (AD), utilizza i seguenti tipi di modifica:

- Per aggiungere un utente: invia una RFC utilizzando Management | Directory Service | Utenti e gruppi | Aggiungi utente al gruppo [ct-24pi85mjtza8k]
- Per rimuovere un utente: invia una RFC utilizzando Management | Directory Service | Utenti e gruppi | Rimuovi utente dal gruppo [ct-2019s9y3nfml4]

> **Note**
>
> Quando si utilizza la CTs modalità manuale, AMS consiglia di utilizzare l'opzione ASAP Scheduling (scegliere ASAP nella console, lasciare vuote le date di inizio e fine nell'API/CLI) in quanto CTs richiedono che un operatore AMS esamini la RFC ed eventualmente comunichi con l'utente prima che possa essere approvata ed eseguita. Se li pianifichi RFCs, assicurati di attendere almeno 24 ore. Se l'approvazione non avviene prima dell'orario di inizio programmato, la RFC viene rifiutata automaticamente.

Trova gruppi di sicurezza

Per trovare i gruppi di sicurezza collegati a uno stack o a un'istanza, usa la console EC2. Dopo aver trovato lo stack o l'istanza, puoi vedere tutti i gruppi di sicurezza ad esso collegati.

Per informazioni su come trovare i gruppi di sicurezza nella riga di comando e filtrare l'output, consulta `describe-security-groups`.

EC2 Profilo dell'istanza IAM

Un profilo di istanza è un contenitore per un ruolo IAM che puoi utilizzare per passare informazioni sul ruolo a un' EC2 istanza all'avvio dell'istanza.

MALZ

Esistono due profili di istanza AMS predefiniti `customer-mc-ec2-instance-profile` e`customer-mc-ec2-instance-profile-s3`. Questi profili di istanza forniscono le autorizzazioni descritte nella tabella seguente.

Descrizioni delle politiche

Profilo	Policy
`customer-mc-ec2-instance-profile`	`AmazonSSMManagedInstanceCore` : consente alle istanze Ec2 di utilizzare l'agente SSM.
	`AMSInstanceProfileLoggingPolicy` : Consente alle istanze Ec2 di inviare i log a S3 e. CloudWatch

Profilo	Policy
	`AMSInstanceProfileManagementPolicy` : Consente alle istanze Ec2 di eseguire azioni di avvio, come l'adesione ad Active Directory.
	`AMSInstanceProfileMonitoringPolicy` : Consente alle istanze Ec2 di riportare i risultati ai servizi di monitoraggio AMS.
	`AMSInstanceProfilePatchPolicy` : consente alle istanze Ec2 di ricevere patch.
`customer-mc-ec2-instance-profile-s3`	`AMSInstanceProfileBYOEPSPolicy` : Consente alle istanze Ec2 di utilizzare AMS bring your own EPS.
	`AMSInstanceProfileLoggingPolicy` : Consente alle istanze Ec2 di inviare i log a S3 e. CloudWatch
	`AMSInstanceProfileManagementPolicy` : Consente alle istanze Ec2 di eseguire azioni di avvio, come l'adesione ad Active Directory.
	`AMSInstanceProfileMonitoringPolicy` : Consente alle istanze Ec2 di riportare i risultati ai servizi di monitoraggio AMS.
	`AMSInstanceProfilePatchPolicy` : consente alle istanze Ec2 di ricevere patch.
	`AMSInstanceProfileS3WritePolicy` : consente alle istanze Ec2 di accedere ai read/write bucket S3 del cliente.

SALZ

Esiste un profilo di istanza AMS predefinito che concede le autorizzazioni `customer-mc-ec2-instance-profile` previste dalla policy delle istanze IAM. `customer_ec2_instance_profile_policy` Questo profilo di istanza fornisce le

autorizzazioni descritte nella tabella seguente. Il profilo concede le autorizzazioni alle applicazioni in esecuzione sull'istanza, non agli utenti che accedono all'istanza.

Le politiche spesso includono più istruzioni, in cui ogni istruzione concede autorizzazioni a un diverso set di risorse o concede autorizzazioni in base a una condizione specifica.

CW =. CloudWatch ARN = Amazon Resource Name. * = wildcard (qualsiasi).

EC2 autorizzazioni predefinite del profilo di istanza IAM

CW =. CloudWatch ARN = Amazon Resource Name. * = wildcard (qualsiasi).			
Dichiarazione delle policy	Effetto	Operazioni	Descrizione e risorse (ARN)
Amazon Elastic Compute Cloud (Amazon EC2)			
EC2 Azioni relative ai messaggi	Consens	AcknowledgeMessage, DeleteMessage, FailMessage, GetEndpoint, GetMessages, SendReply	Consente azioni di messaggistica di EC2 Systems Manager nel tuo account.
Ec2 Descrivi	Consens	* (Tutti)	Consente alla console di visualizzare i dettagli di configurazione EC2 di un account.
Iam Get Role ID	Consens	GetRole	Consente di EC2 ottenere il tuo ID IAM da `aws:iam::*:role/customer-* eaws:iam::*:role/customer_*` .
Istanza per caricare gli eventi di registro	Consens	Crea un gruppo di log	Consente la creazione di registri in: `aws:logs:*:*:log-group:i-*`

CW =. CloudWatch ARN = Amazon Resource Name. * = wildcard (qualsiasi).			
Dichiarazione delle policy	Effetto	Operazioni	Descrizione e risorse (ARN)
		Crea Log Stream	Consente lo streaming dei log su: `aws:logs:*:*:log-group:i-*`
CW per MMS	Consens	DescribeAlarms, PutMetricAlarm, PutMetricData	Consente di CloudWatch recuperare gli allarmi nel tuo account. Consente a CW di creare o aggiornare un allarme e associarlo alla metrica specificata. Consente a CW di pubblicare punti dati metrici sul tuo account.
Tag Ec2	Consens	CreateTags, DescribeTags,	Consente di aggiungere, sovrascrivere e descrivere i tag nelle istanze specificate nel tuo account.
Nega esplicitamente i registri CW	Rifiuta	DescribeLogStreams, FilterLogEvents, GetLogEvents	Non consente di elencare, filtrare o ottenere i flussi di log per: `aws:logs:*:*:log-group:/mc/*`
Amazon EC2 Simple Systems Manager (SSM)			

CW =. CloudWatch ARN = Amazon Resource Name. * = wildcard (qualsiasi).			
Dichiarazione delle policy	Effetto	Operazioni	Descrizione e risorse (ARN)
Azioni SSM	Consens	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	Consente una varietà di funzioni SSM nel tuo account.
Accesso SSM in S3	Consens	GetObject, PutObject, AbortMultipartUpload, ListMultipartUploadPorts, ListBucketMultipartUploads	Consente all'SSM di caricare e aggiornare oggetti e di interrompere il EC2 caricamento di oggetti in più parti ed elencare le porte e i bucket disponibili per i caricamenti in più parti. `aws:s3:::mc-*-internal-*/aws/ssm*`
Amazon EC2 Simple Storage Service (S3)			
Ottieni oggetti in S3	Consens	Get Elenco	Consente alle EC2 applicazioni di recuperare ed elencare gli oggetti nei bucket S3 del tuo account.
Accesso S3 al registro crittografato del cliente	Consens	PutObject	Consente EC2 alle applicazioni di aggiornare gli oggetti in `aws:s3:::mc-*-logs-*/encrypted/app/*`

CW =. CloudWatch ARN = Amazon Resource Name. * = wildcard (qualsiasi).			
Dichiarazione delle policy	Effetto	Operazioni	Descrizione e risorse (ARN)
Patch Data Put Object S3	Consens	PutObject	Consente alle EC2 applicazioni di caricare i dati di patch nei bucket S3 all'indirizzo `aws:s3:::awsms-a*-patch-data-*`
Caricamento dei propri log su S3	Consens	PutObject	Consente alle EC2 applicazioni di caricare log personalizzati su: `aws:s3:::mc-a*-logs-*/aws/instances/*/${aws:userid}/*`
Nega esplicitamente i registri di MC Namespace S3	Rifiuta	GetObject* Inserisci*	Impedisce EC2 alle applicazioni di acquisire o inserire oggetti da o verso: `aws:s3:::mc-*-logs-*/encrypted/mc*` , `aws:s3:::mc-*-logs-*/mc/*`, `aws:s3:::mc-a*-logs-*-audit/*`
Nega esplicitamente l'eliminazione di S3	Rifiuta	* (tutti)	Impedisce EC2 alle applicazioni di eseguire alcuna azione sugli oggetti in: `aws:s3:::mc-a*-logs-*/*` , `aws:s3:::mc-a*-internal-*/*` ,

CW =. CloudWatch ARN = Amazon Resource Name. * = wildcard (qualsiasi).			
Dichiarazione delle policy	Effetto	Operazioni	Descrizione e risorse (ARN)
Nega esplicita mente S3 CFN Bucket	Rifiuta	Elimina*	Impedisce alle applicazioni di eliminare oggetti EC2 da: `aws:s3:::cf-templates-*`
Nega esplicita mente List Bucket S3	Rifiuta	ListBucket	Non consente di elencare oggetti crittografati, di registro di controllo o riservati (mc) provenienti da: `aws:s3:::mc-*-logs-*`
Gestione dei segreti AWS in Amazon EC2			

CW =. CloudWatch ARN = Amazon Resource Name. * = wildcard (qualsiasi).			
Dichiarazione delle policy	Effetto	Operazioni	Descrizione e risorse (ARN)
Accesso segreto a Trend Cloud One	Consens	GetSecretValue	Consente EC2 ad Amazon di accedere ai segreti per la migrazione di Trend Cloud One: `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `arn:aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-activation-token*` , `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-id*` , `aws:secretsmanager:*:*:secret:/ams/eps/cloud-one-agent-tenant-guid*`
AWS Key Management Service in Amazon EC2			
Chiave di decrittografia Trend Cloud One	Consens	Decrypt	Consenti EC2 ad Amazon di decrittografare la AWS KMS chiave con il nome alias/-migration ams/eps/cloudone `arn:aws:kms:*:*:alias/ams/eps/cloudone-migration`

Se non conosci le politiche di Amazon IAM, consulta Panoramica delle politiche IAM per informazioni importanti.

> **Note**
>
> Le politiche spesso includono più istruzioni, in cui ogni dichiarazione concede autorizzazioni a un diverso set di risorse o concede autorizzazioni in base a una condizione specifica.

Impostazioni predefinite delle metriche monitorate

La tabella seguente mostra cosa viene monitorato e le soglie di avviso predefinite. È possibile modificare le impostazioni predefinite con una richiesta di modifica per la gestione delle modifiche (RFC).

> **Note**
>
> CloudWatch ha lanciato la conservazione estesa delle metriche il 1° novembre 2016. Per ulteriori informazioni, consulta CloudWatch Limiti.

Avvisi derivanti dal monitoraggio di base

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
Per gli avvisi contrassegnati da un asterisco (*), AMS valuta in modo proattivo l'impatto e corregge quando possibile; se la correzione non è possibile, AMS crea un incidente. Laddove l'automazione non riesca a risolvere il problema, AMS informa l'utente del caso di incidente e viene assunto un tecnico AMS. Inoltre, questi avvisi possono essere inviati direttamente alla tua e-mail (se hai scelto l'argomento Direct-Customer-Alerts SNS).			
Istanza Application Load Balancer (ALB)	No	RejectedConnectionCount somma > 0 per 1 minuto, 5 volte consecutive.	CloudWatch allarme se il numero di connessioni che sono state rifiutate perché il sistema di bilanciamento del carico ha raggiunto il suo massimo.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
Obiettivo Application Load Balancer (ALB)	No	TargetConnectionErrorCount somma > 0 per 1 minuto, 5 volte consecutive.	CloudWatch allarme se il numero di connessioni è stato stabilito senza successo tra il sistema di bilanciamento del carico e le istanze registrate.
Istanza Amazon EC2 — Windows	No	SecureChannelFailure > 0,0 per 10 degli ultimi 15 punti dati.	CloudWatch allarme sulle istanze Windows per avvisare quando la connessione Secure a Channel non è riuscita.
Istanza Aurora	No	CPUUtilization > 85% per 5 minuti, 2 volte consecutive.	CloudWatch allarme.
AWS Backup	Sì	DeleteRecoveryPoint Un ruolo principale IAM o un user principal IAM inaspettato ha eliminato un punto di AWS Backup ripristino.	CloudWatch evento. Emesso quando viene eliminato un punto di ripristino di backup.
AWS Outposts	Sì	AMSOutpostsInstanceFamilyCapacityAvailability InstanceFamilyCapacityAvailability = 80% per 5 minuti, 12 volte consecutive.	CloudWatch allarme ad esempio sulla disponibilità della capacità familiare della AWS Outposts risorsa.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
		AMSOutpostsInstanceTypeCapacityAvailability TypeCapacityAvailability = 80% per 5 minuti, 12 volte consecutive.	CloudWatch allarme sul tipo di istanza (capacità, disponibilità della AWS Outposts risorsa).
		AMSOutpostsConnectedStatusConnectedStatus < 1 per 5 minuti, 1 volta consecutiva.	CloudWatch allarme sulla connessione al AWS Outposts service link, meno di 1 conteggio è compromesso.
		AMSOutpostsCapacityExceptionCapacityExceptions 0 per 5 minuti, 1 volta consecutiva.	CloudWatch allarme in caso di capacità insufficiente, errori (ad esempio, avvio di una risorsa AWS Outposts) .
Istanza EC2: tutte OSs	No	CPUUtilization* >= 95% per 5 minuti, 6 volte consecutive, se l'istanza non risponde a un comando di polling Systems Manager.	CloudWatch allarme. L'elevato utilizzo della CPU è un indicatore di un cambiamento nello stato dell'applicazione, ad esempio deadlock, loop infiniti, attacchi dannosi e altre anomalie.
		StatusCheckFailed > 0 per 5 minuti, 3 volte consecutive.	CloudWatch allarme.
		Utilizzo del volume root >= 95% per 5 minuti, 6 volte consecutive.	

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
		Utilizzo di volumi non root > 85% per 5 minuti, 2 volte consecutive. Disattivata per impostazione predefinita; per ulteriori informazioni, vedere https://docs.aws.amazon.com/managedservices/latest/ctref/management-monitoring-cloudwatch-enable-non-root-volumes-monitoring.html#management-monitoring-cloudwatch-enable-non-root-volumes-monitoring-info.	
		Memoria liberata* MemoryFree < 5% per 5 minuti, 6 volte consecutive.	
	Sì	Malware EPS Malware rilevato su esempio.	CloudWatch evento.
Istanza Amazon EC2 - Linux	No	Utilizzo di Root Volume Inode Media >= 95% per 5 minuti, 6 volte consecutive.	CloudWatch allarme. Applicato solo alle istanze Linux.
		Swap gratuito* Memory Swap < 5% per 5 minuti, 6 volte consecutive.	

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
ElastiCache Cluster	No	CurrConnections = 65000	Questo allarme notifica ad AMS il limite massimo di connessione di un ElastiCache host. CloudWatch Allarme. Se desideri aggiornare questa soglia, contatta l'assistenza AMS.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
ElastiCache Nodo	No	CPUUtilization Media > valore predefinito per 15 minuti, 2 volte consecutive.	CloudWatch allarme. L'impostazione predefinita è 90. Se Redis, usa uno dei seguenti valori in base al tipo di istanza: • cache.t1.micro: 90% • cache.m1.small: 90% • cache.m1.medium: 90% • cache.m1.large: 45% • cache.m1.xlarge: 22,5% • cache.m2.xlarge: 45% • cache.m2.4xlarge: 11,25% • cache.c1.xlarge: 11,25% • cache.t2.micro: 90% • cache.t2.small: 90% • cache.t2.medium: 45% • cache.m3.medium: 90% • cache.m3.large: 45% • cache.m3.xlarge: 22,5% • cache.m3.2xlarge: 11,25% • cache.r3.large: 45% • cache.r3.xlarge: 22,5% • cache.r3.2xlarge: 11,25% • cache.r3.4xlarge: 5,625% • cache.r3.8xlarge: 2,8125%

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
ElastiCache Nodo: memcached	No	SwapUsage massimo > 50.000.000 di byte per 5 minuti, 5 volte consecutive.	CloudWatch allarme. Applicato solo a memcached.
OpenSearch ammasso	No	ClusterStatus.red il massimo è >= 1 per 1 minuto, 1 volta consecutiva. AMS intraprende azioni proattive per ridurre l'impatto operativo, quando viene attivato questo avviso.	CloudWatch allarme. Almeno una partizioni primaria e le relative repliche non sono assegnate a un nodo. Per saperne di più, consulta Red Cluster Status.
OpenSearch dominio	No	KMSKeyErrore >= 1 per 1 minuto, 1 volta consecutiva.	CloudWatch allarme. La chiave crittografica KMS che viene utilizzata per crittografare i dati a riposo nel tuo dominio è disabilitata. Riabilitala per ripristinare le normali operazioni. Per ulteriori informazioni, consulta Encryption of Data at Rest for OpenSearch Service.
		ClusterStatus.giallo il massimo è >= 1 per 1 minuto, 1 volta consecutiva AMS intraprende azioni proattive per ridurre l'impatto operativo, quando viene attivato questo avviso.	Almeno una partizione di replica non è allocata per un nodo. Per ulteriori informazioni, consulta Yellow Cluster Status.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
		FreeStorageSpace il minimo è <= 20480 per 1 minuto, 1 volta consecutiva AMS intraprende azioni proattive per ridurre l'impatto operativo, quando viene attivato questo avviso.	Un nodo nel cluster è legato ai 20 GiB di spazio di archiviazione gratuito. Per ulteriori informazioni, consulta Mancanza di spazio di archiviazione disponibile.
		ClusterIndexWritesBlocked >= 1 per 5 minuti, 1 volta consecutiva Quando viene attivato questo avviso, AMS intraprende azioni proattive per ridurre l'impatto operativo.	Il cluster sta bloccando le richieste di scrittura. Per ulteriori informazioni, consulta ClusterBlockException.
		Nodi il minimo è < x per 1 giorno, 1 volta consecutiva AMS intraprende azioni proattive per ridurre l'impatto operativo, quando viene attivato questo avviso.	x è il numero di nodi del cluster. Questo allarme indica che almeno un nodo nel cluster è stato irraggiungibile per un giorno. Per ulteriori informazioni, consulta Failed Cluster Nodes.
		CPUUtilization la media è >= 80% per 15 minuti, 3 volte consecutive AMS intraprende azioni proattive per ridurre l'impatto operativo, quando viene attivato questo avviso.	L'utilizzo al 100% della CPU è comune, ma medie elevate e sostenute sono problematiche. Consigliamo di utilizzare tipi di istanza più grandi o aggiungere istanze.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
		JVMMemoryPressione il massimo è >= 80% per 5 minuti, 3 volte consecutive AMS intraprende azioni proattive per ridurre l'impatto operativo, quando viene attivato questo avviso.	Sui cluster potrebbero verificar si errori di esaurimento della memoria nel caso in cui l'utilizz o aumenti. Considerare il dimensionamento verticale. Amazon ES utilizza metà della RAM di un'istanza per l'heap Java, fino a una dimensione dell'heap di 32 GiB. Puoi scalare le istanze verticalmente fino a 64 GiB di RAM e poi scalare orizzontalmente aggiungendo le istanze.
		Padrone CPUUtilization la media è >= 50% per 15 minuti, 3 volte consecutive AMS intraprende azioni proattive per ridurre l'impatto operativo, quando viene attivato questo avviso.	Prendi in considerazione l'utilizz o di tipi di istanze più grandi per i tuoi nodi master dedicati. A causa del loro ruolo nella stabilità e nelle blue/green implement azioni dei cluster, i nodi master dedicati dovrebbero avere un utilizzo medio della CPU inferiore rispetto ai nodi di dati.
		Pressione principale JVMMemory il massimo è >= 80% per 15 minuti, 1 volta consecutiva AMS intraprende azioni proattive per ridurre l'impatto operativo, quando viene attivato questo avviso.	Prendi in considerazione l'utilizz o di tipi di istanze più grandi per i tuoi nodi master dedicati. A causa del loro ruolo nella stabilità e nelle blue/green implement azioni dei cluster, i nodi master dedicati dovrebbero avere un utilizzo medio della CPU inferiore rispetto ai nodi di dati.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
OpenSearch istanza	No	AutomatedSnapshotFailure il massimo è >= 1 per 1 minuto, 1 volta consecutiva.	CloudWatch allarme. Uno snapshot automatico ha restituit o un errore. Questo errore è spesso il risultato di uno stato del cluster rosso. Vedi Red Cluster Status.
Istanza Elastic Load Balancing	No	SurgeQueueLength > 100 per 1 minuto, 15 volte consecutive.	CloudWatch allarme se un numero eccessivo di richieste è in attesa di instradamento.
		HTTPCode_ELB_5XX_Count somma > 0 per 5 minuti, 3 volte consecutive.	CloudWatch allarme relativo al numero eccessivo di codici di risposta HTTP 5XX che provengono dal load balancer.
		SpilloverCount > 1 per 1 minuto, 15 volte consecuti ve.	CloudWatch allarme se un numero eccessivo di richieste sono state rifiutate perché la coda di sovratensione è piena.
GuardDuty servizio	Sì	Non applicabile; tutti i risultati (ai fini della minaccia) vengono monitorat i. Ogni risultato corrisponde a un avviso. Modifiche nei GuardDuty risultati. Queste modifiche includono i nuovi risultati generati e le occorrenze successive dei risultati esistenti.	L'elenco dei tipi di GuardDuty ricerca supportati si trova in GuardDuty Active Finding Types.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
Integrità	Può variare	Dashboard AWS Health	Le notifiche vengono inviate quando si verificano cambiamenti nello stato degli eventi Dashboard AWS Health (AWS Health) in relazione ai servizi di base supportati da AMS che richiedono l'intervento di AMS Operations. Per ulteriori informazioni, consulta Servizi supportati.
AWS Managed Microsoft AD	No	Stato di Active Directory AWS Managed Microsoft AD l'istanza invia un evento di stato attivo.	Evento di servizio. Emesso quando la directory funziona normalmente dopo un evento.
		Stato della directory alterato AWS Managed Microsoft AD l'istanza invia un evento di stato della directory alterato.	Evento di servizio. Emesso quando la directory è in esecuzione in uno stato degradato. Uno o più problemi sono stati rilevati e non tutte le operazioni di directory potrebbero lavorare alla massima capacità operativa.
		Stato della directory non utilizzabile AWS Managed Microsoft AD l'istanza invia un evento di stato non utilizzabile.	Evento di servizio. Emesso quando la directory non è funzionante. Sono stati segnalati problemi per tutti gli endpoint della directory.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
		Eliminazione dello stato della directory AWS Managed Microsoft AD l'istanza invia un evento di eliminazi one dello stato della directory.	Evento di servizio. Emesso quando la directory viene attualmente eliminata.
		Stato della directory non riuscito AWS Managed Microsoft AD l'istanza invia un evento di stato non riuscito.	Evento di servizio. Emesso quando non è stato possibile creare la directory.
		RestoreFailed Stato della directory AWS Managed Microsoft AD l'istanza invia un evento di ripristin o non riuscito dello stato della directory.	Evento di servizio. Emesso durante il ripristino della directory da un'istantanea non riuscito.
Istanza Amazon RDS	No	L'avviso Low Storage si attiva quando lo storage allocato per l'istanza DB è esaurito.	RDS-EVENT-0007, consulta i dettagli in Utilizzo della notifica degli eventi di Amazon RDS.
		Errore dell'istanza DB L'istanza database ha avuto esito negativo a causa di una configura zione non compatibile o di un problema di storage sottostante. Inizia a point-in-time-restore per l'istanza DB.	Evento di servizio. RDS-EVENT -0031, categorie di eventi e messaggi di eventi di Amazon RDS.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
		Failover non tentato Amazon RDS non sta tentando di effettuare un failover richiesto perché di recente si è verificato un failover nell'istanza database.	Evento di servizio. RDS-EVENT -0034, categorie di eventi e messaggi di eventi di Amazon RDS.
		Parametri non validi dell'istanza DB Ad esempio, MySQL non può avviarsi perché un parametro relativo alla memoria è impostato su un valore troppo alto per questa classe di istanza, quindi l'azione del cliente consisterebbe nel modificare il parametro di memoria e riavviare l'istanza DB.	Evento di servizio. RDS-EVENT -0035, categorie di eventi e messaggi di eventi di Amazon RDS.
		Istanza DB IDs di sottorete non valida L'istanza database si trova in una rete non compatibile. Alcune delle sottoreti specificate non IDs sono valide o non esistono.	Evento di servizio. RDS-EVENT -0036, categorie di eventi e messaggi di eventi di Amazon RDS.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
		Errore di lettura della replica dell'istanza DB Si è verificato un errore interno nel processo di replica di lettura. Per ulteriori informazioni, consulta il messaggio di evento. Per informazioni sulla risoluzione degli errori di Read Replica, consulta Risoluzione di un problema di Read Replica di MySQL.	Evento di servizio. RDS-EVENT-0045, categorie di eventi e messaggi di eventi di Amazon RDS.
		La replica di lettura dell'istanza DB è terminata La replica sulla Read Replica è stata terminata.	Evento di servizio. RDS-EVENT-0057, categorie di eventi e messaggi di eventi di Amazon RDS.
		Errore durante la creazione dell'account utente statspack Errore durante la creazione dell'account utente Statspack PERFSTAT. Elimina l'account prima di aggiungere l'opzione Statspack.	Evento di servizio. RDS-EVENT-0058, categorie di eventi e messaggi di eventi di Amazon RDS.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
		Avvio del ripristino dell'istanza DB L'istanza database di SQL Server sta ristabilendo il relativo mirror. Le prestazioni subiranno un peggioramento fino al termine dell'operazione. È stato trovato un database con un modello di recupero non FULL. Il modello di ripristino è stato riportato a FULL ed è stato avviato il ripristino in mirroring. (<dbname>: <recovery model found>[,...]).	Evento di servizio. RDS-EVENT-0066, categorie di eventi e messaggi di eventi di Amazon RDS.
		Il failover del cluster di database non è riuscito.	RDS-EVENT-0069, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
		Bucket S3 di ripristino delle autorizzazioni non valide Il ruolo IAM utilizzato per accedere al bucket di Amazon S3 per il backup e ripristino nativo di SQL Server non è configurato correttamente. Per ulteriori informazioni, vedere Configurazione per il backup e il ripristino nativi.	Evento di servizio. RDS-EVENT-0081, categorie di eventi e messaggi di eventi di Amazon RDS.
		Aurora non è riuscito a copiare i dati di backup da un bucket Simple Storage Service (Amazon S3).	RDS-EVENT-0082, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
		Avviso di storage insufficiente quando l'istanza DB ha consumato più del 90% dello storage allocato	RDS-EVENT-0089, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
		Il servizio di notifica durante il ridimensionamento non è riuscito per il cluster DB Aurora Serverless.	RDS-EVENT-0143, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
		L'istanza database è in uno stato non valido. Nessuna operazion e richiesta. Il ridimensionamento automatico verrà riprovato in un secondo momento.	RDS-EVENT-0219, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
		L'istanza database ha raggiunto la soglia completa dello storage e il database è stato arrestato.	RDS-EVENT-0221, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
		Questo evento indica che la scalabili tà automatica dello storage delle istanze RDS non è in grado di scalare. I motivi per cui la scalabilità automatica non è riuscita possono essere diversi.	RDS-EVENT-0223, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
		La scalabilità automatica dello storage ha attivato un'attività di storage in sospeso che avrebbe raggiunto la soglia massima di storage.	RDS-EVENT-0224, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
		Il tipo di archiviazione dell'istanza database non è attualmente disponibile nella zona di disponibilità. Il ridimensionamento automatico verrà riprovato in un secondo momento.	RDS-EVENT-0237, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
		RDS non è stato in grado di allocare la capacità per il proxy perché non ci sono sufficienti indirizzi IP disponibili nelle sottoreti.	RDS-EVENT-0243, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
		Lo storage per il tuo account AWS ha superato la quota di storage consentita.	RDS-EVENT-0254, consulta i dettagli in Categorie di eventi e messaggi di eventi di Amazon RDS.
		CPUUtilization Utilizzo medio della CPU > 90% per 15 minuti, 2 volte consecutive.	CloudWatch allarme.
		DiskQueueDepth La somma è > 75 per 1 minuto, 15 volte consecutive.	
		FreeStorageSpace Media < 1.073.741.824 byte per 5 minuti, 2 volte consecutive.	

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
		SwapUsage Media = 104.857.600 byte per 5 minuti, 2 volte consecutive.	
Cluster Amazon Redshift	No	RedshiftClusterStatus Lo stato del cluster quando non è in modalità di manutenzione < 1 per 5 minuti.	1 rappresenta un cluster integro.
Amazon Macie	Sì	Avvisi appena generati e aggiornamenti agli avvisi esistenti. Macie rileva eventuali modifiche nei risultati. Queste modifiche includono i nuovi risultati generati e le occorrenze successive dei risultati esistenti.	Avviso Amazon Macie. Per un elenco dei tipi di avvisi Macie supportati, consulta Analyzing Amazon Macie Findings. Tieni presente che Macie non è abilitato per tutti gli account.

Impostazioni predefinite di conservazione e rotazione dei log

Questa sezione descrive le impostazioni predefinite per la gestione dei registri AMS; per ulteriori informazioni, consulta Gestione dei registri.

- Rotazione = Registra il turnover all'interno delle istanze
- Conservazione = periodo di tempo in cui conserviamo i log in Amazon CloudWatch Logs e Amazon Simple Storage Service (S3)

I log vengono conservati in CloudWatch Logs secondo necessità (puoi configurarlo) e in S3. Non scadono né vengono eliminati e sono soggetti alla durabilità del servizio. Per informazioni dettagliate sulla durabilità di S3, consulta Protezione dei dati in Amazon S3.

Puoi richiedere una modifica alla conservazione dei log per tutti i log, ad eccezione dei AWS CloudTrail log, che vengono conservati per 10 anni per motivi di controllo e sicurezza.

La rotazione dei log è configurata all'interno delle istanze. Per impostazione predefinita, i registri del sistema operativo e di sicurezza ruotano ogni ora se superano i 100 MB, in modo da non esaurire il disco nelle istanze.

L'agente di registro all'interno delle istanze carica il registro online in CloudWatch Logs, da cui i log vengono archiviati in S3.

I log vengono archiviati in CloudWatch Logs e S3 nel formato raw in cui vengono generati, senza alcuna preelaborazione.

Impostazioni predefinite per la gestione della continuità

Questa sezione descrive le impostazioni predefinite di gestione della continuità AMS; per ulteriori informazioni sui backup AMS, consulta il capitolo sulla gestione della continuità della Guida per l'utente di AMS.

La configurazione di backup viene eseguita al momento dell'onboarding. Queste sono le impostazioni di backup predefinite (consigliate).

Tag VPC e impostazioni predefinite

Per le informazioni più aggiornate sul backup AMS, consulta Gestione della continuità.

> **Important**
>
> Per impostazione predefinita, i backup in EC2 stack sono disabilitati (Backup = False). È possibile abilitare i backup delle EC2 istanze al momento della creazione aggiungendo un tag `Key: Backup, Value: True` quando si richiede uno EC2 stack tramite un RFC (CT ct-14027q0sjyt1h). Se desideri aggiungere il tag dopo la creazione dell'istanza, invia una RFC con Management | Advanced stack components | instance stack | Update CT (ct-38s4s4tm4ic4u). EC2

EC2 tag di istanza e impostazioni predefinite

Il tag EC2 stack backup specifica se lo stack richiede o meno un'istantanea dei volumi EBS collegati.

`Tag Key: Backup`

`Etichetta Value: True, False`

Per impostazione predefinita, il valore è `False` che il tag di backup non è presente e lo stack non ha backup pianificati.

Modifica il tag `Key: Backup` per `Value: True` abilitare i backup, che vengono poi eseguiti secondo la pianificazione impostata con il tag di backup VPC.

> **Note**
>
> L'involucro del valore del tag (solo Value) non è sensibile, quindi True/true sono tutti accettabili. False/false

Backup e impostazioni predefinite delle istanze RDS

I valori predefiniti di Amazon Relational Database Service (RDS) sono definiti nei modelli di stack:

```
Backup: Yes

Backup Window: 22:00-23:00 (RDS local time zone)

Retention Period: 7 (7 snapshots stored)
```

Impostazioni predefinite per l'applicazione delle patch

Questa sezione descrive le impostazioni predefinite di applicazione delle patch da parte di AMS; per ulteriori informazioni sull'applicazione di patch ad AMS, consulta il capitolo AMS User Guide Patch Management.

AMS rilascia patch AMIs su base mensile; tutte le nuove richieste di stack devono essere configurate con l'ultima AMI AMS.

> **Important**
>
> AMS Patch Orchestrator, l'applicazione di patch basate su tag, utilizza la funzionalità AWS Systems Manager (SSM) per consentirti di etichettare o assegnare un tag AMS alle istanze e di applicare le patch a tali istanze utilizzando una linea di base e una finestra configurate

dall'utente. Per saperne di più, consulta Patch Orchestrator: un modello di patching basato su tag.

Applicazione delle patch secondo lo standard AMS, basata sull'account: per ogni account con stack che ricevono patch in loco, poco dopo il «Patch Tuesday» viene inviata una notifica delle imminenti patch applicabili. La notifica contiene un elenco di tutti gli stack e delle patch applicabili, nonché la finestra di patch consigliata. Per le patch critiche, la finestra viene impostata con non più di 10 giorni di anticipo e per le patch standard con non più di 14 giorni di anticipo. Se non si risponde alla notifica, l'applicazione delle patch non viene eseguita. Se desideri escludere determinate patch, rispondi alla notifica o invia una richiesta di assistenza. Se rispondi con il consenso all'applicazione delle patch, ma non richiedi specificamente una pianificazione diversa, le patch vengono applicate come descritto nella notifica che ricevi.

> **Note**
>
> La notifica del servizio patch è un'e-mail inviata ai contatti dell'account e contiene un collegamento alla console AWS Support. Puoi rispondere tramite la console AWS Support o tramite la pagina di richiesta del servizio AMS, dove la notifica viene visualizzata come notifica di servizio.

Al momento del processo di patching standard di AMS, AMS esegue le seguenti operazioni:

1. All'utente viene inviata una notifica del servizio di applicazione delle patch quattordici giorni prima della finestra di patch proposta. La notifica del servizio di patch viene inviata via e-mail all'indirizzo e-mail di contatto registrato per l'account.
2. Identifica tutte le EC2 istanze raggiungibili nello stack in base all'elenco degli stack fornito nella notifica di patch. In questo caso, per «Reachable» si intendono le istanze che si trovano nello EC2 stato «Running» e che hanno l'agente Run Command completamente operativo. EC2
3. AMS esegue l'applicazione delle patch in modo da garantire l'esecuzione simultanea di un numero sufficiente di EC2 istanze (configurato tramite l'`healthy-host-threshold`impostazione) in modo che lo stack rimanga integro.
4. Una volta completata l'operazione di patching per tutte le EC2 istanze, AMS aggiorna la RFC con lo stato di applicazione delle patch: Operazione riuscita, Riuscita parziale o Fallimento. In caso di stato diverso da Successo, viene creato un ticket che consente a un operatore di verificare i risultati dell'applicazione delle patch e intraprendere eventuali azioni correttive.

Convalida il servizio AMS (SALZ)

Per verificare che il servizio AWS Managed Services (AMS) funzioni come previsto, in questo capitolo vengono descritti alcuni esercizi che è possibile eseguire.

Trova le impostazioni dell'account AMS

Impostazioni dell'account utilizzate per creare AMS RFCs, impostare pianificazioni e determinare chi riceve le notifiche.

Alcune impostazioni vengono create durante l'onboarding e richiedono una richiesta di servizio per essere modificate. È necessario prendere nota di questi dati dell'account perché li utilizzerai per comunicare con AMS:

- Credenziali: se hai bisogno di recuperare il nome utente o la password AMS, contatta l'amministratore IT locale: AMS utilizza l'Active Directory aziendale.
- Cloud Service Delivery Manager (CSDM): questa persona è il vostro referente con AMS ed è disponibile a rispondere alle domande sull'assistenza. Le informazioni di contatto di questa persona ti vengono fornite al momento dell'onboarding e dovresti tenerle disponibili a tutti i membri dell'organizzazione che interagiscono con AMS. Puoi aspettarti di ricevere report mensili sul tuo servizio AMS da questa persona.
- Accesso alla console: accedi alla console AMS tramite un URL configurato specificamente per il tuo account. Puoi ottenere l'URL dal tuo CSDM.
- AMS CLI: puoi ottenere l'AMS CLI tramite la pagina delle risorse per gli sviluppatori della console AMS o il pacchetto distribuibile che ottieni dal tuo CSDM. Dopo aver ottenuto il pacchetto distribuables, segui i passaggi descritti in Installazione o aggiornamento della CLI AMS.
- Finestra di manutenzione: la finestra di manutenzione determina quando applicare le patch alle istanze. EC2 La AWS Managed Services Maintenance Window (o Maintenance Window) esegue attività di manutenzione per AWS Managed Services (AMS) e si ripete il secondo giovedì di ogni mese dalle 15:00 alle 16:00 ora del Pacifico. AMS può modificare la finestra di manutenzione con un preavviso di 48 ore. Potresti aver scelto una finestra diversa al momento dell'onboarding: tieni traccia della finestra di manutenzione scelta.
- Monitoraggio: AMS fornisce una serie di CloudWatch metriche per impostazione predefinita, ma puoi anche richiedere metriche aggiuntive. Se lo fai, tienine traccia.
- Registri: per impostazione predefinita, i log sono archiviati in ams-a- *ACCOUNT_ID* -log-management- *REGION* dove si trova la regione in cui il registro *REGION* è stato generato.

- Attenuazione: al momento dell'onboarding, AMS registra l'azione di mitigazione scelta dall'utente nel caso in cui venga identificato un attacco di malware contro le risorse. Ad esempio, contatta determinate persone. Mantieni queste informazioni disponibili per tutti i membri dell'organizzazione che interagiscono con AMS.
- Regione: puoi consultare la pagina dei dettagli del VPC nella console AMS. Puoi eseguire questo comando anche dopo aver installato la CLI AMS SKMS (questo comando utilizza un profilo SAML, rimuovilo se il tuo metodo di autenticazione è diverso):

```
aws --profile saml amsskms get-vpc --vpc-id VPC_ID
```

Important

Note

Gli endpoint AMS API/CLI (amscm e amsskms) si trovano nella regione AWS della Virginia settentrionale,. `us-east-1` A seconda di come è impostata l'autenticazione e della regione AWS in cui si trovano l'account e le risorse, potrebbe essere necessario aggiungerli `--region us-east-1` quando si emettono i comandi. Potrebbe anche essere necessario aggiungere`--profile saml`, se questo è il metodo di autenticazione utilizzato.

Cerca FQDNs in AMS

I tipi di modifica degli accessi () di AWS Managed Services (AMSCTs) richiedono il nome di dominio completo, o FQDN, del tuo dominio affidabile AMS, sotto forma di. `C844273800838.amazonaws.com` Per scoprire il tuo AWS FQDN, esegui una delle seguenti operazioni:

- Console AWS: cerca nella console AWS Directory Service nella colonna Directory name.
- CLI: usa questi comandi mentre sei connesso al tuo dominio:

  Windows (restituisce utente e nome di dominio completo):

```
whoami /upn
```

o (DC+DC+DC=FQDN)

```
whoami /fqdn
```

Linux:

```
hostname --fqdn
```

> **Note**
>
> Gli endpoint AMS API/CLI (amscm e amsskms) si trovano nella regione AWS della Virginia settentrionale,. `us-east-1` A seconda di come è impostata l'autenticazione e della regione AWS in cui si trovano l'account e le risorse, potrebbe essere necessario aggiungerli `--region us-east-1` quando si emettono i comandi. Potrebbe anche essere necessario aggiungere`--profile saml`, se questo è il metodo di autenticazione utilizzato.

Trova le zone di disponibilità (AZs) in AMS

Zona di disponibilità: tutti gli account hanno almeno due zone di disponibilità. Per trovare con precisione i nomi delle zone di disponibilità, è necessario innanzitutto conoscere l'ID di sottorete associato.

- Console AMS: nel pannello di navigazione VPCs, fai clic, quindi fai clic sul VPC pertinente, se necessario. Nella pagina dei VPCs dettagli, seleziona la sottorete pertinente nella tabella delle sottoreti per aprire la pagina dei dettagli della sottorete con il nome della zona di disponibilità associata.
- API/CLI DI AMS SIMS:

```
aws amsskms list-subnet-summaries --output table
```

```
aws amsskms get-subnet --subnet-id SUBNET_ID
```

> **Note**
>
> Gli endpoint AMS API/CLI (amscm e amsskms) si trovano nella regione AWS della Virginia settentrionale,. `us-east-1` A seconda di come è impostata l'autenticazione e della regione AWS in cui si trovano l'account e le risorse, potrebbe essere necessario aggiungerli `--region us-east-1` quando si emettono i comandi. Potrebbe anche essere necessario aggiungere`--profile saml`, se questo è il metodo di autenticazione utilizzato.

Trova argomenti SNS in AMS

I tuoi argomenti SNS determinano chi riceve la notifica in varie circostanze. AMS fornisce argomenti SNS per le notifiche AMI (vedi Notifiche AMI AMS con SNS), gli CloudWatch allarmi e le EC2 risorse (vedi Ricezione di avvisi generati da AMS) e altro ancora. Per scoprire gli argomenti SNS esistenti:

- Console AWS: utilizza la console SNS per visualizzare tutti gli argomenti, le applicazioni e gli abbonamenti e un grafico dei messaggi. Inoltre, crea, elimina, sottoscrivi e pubblica su argomenti.
- API/CLI (quando accedi al tuo account AMS, richiede l'AWS CLI):

  Elenca i tuoi argomenti SNS:

  ```
  aws sns list-topics
  ```

  Elenca i tuoi abbonamenti SNS:

  ```
  aws sns list-subscriptions
  ```

> **Note**
>
> Gli endpoint AMS API/CLI (amscm e amsskms) si trovano nella regione AWS della Virginia settentrionale,. `us-east-1` A seconda di come è impostata l'autenticazione e della regione AWS in cui si trovano l'account e le risorse, potrebbe essere necessario aggiungerli `--region us-east-1` quando si emettono i comandi. Potrebbe anche essere necessario aggiungere`--profile saml`, se questo è il metodo di autenticazione utilizzato.

Trova le impostazioni di backup in AMS

I backup e le istantanee sono gestiti da AMS tramite il servizio nativo AWS Backup.

La configurazione è gestita tramite AWS Backup piani. È possibile disporre di più AWS Backup piani che associano le risorse contrassegnate a pianificazioni di backup e politiche di conservazione. Per trovare AWS Backup le impostazioni del tuo account AMS, usa la console https://console.aws.amazon.com/backup o l'AWS CLI Command Reference per i comandi di backup.

Per ulteriori informazioni su AMS e AWS Backup, consulta Continuity Management.

Ricerca di un ID di istanza o di un indirizzo IP

È necessario un indirizzo IP dell'istanza per accedere all'istanza.

- Per richiedere l'accesso a un'istanza, accedere a un'istanza o creare un AMI, è necessario disporre dell'ID dell'istanza. Per un' EC2 istanza (un'istanza autonoma o parte di uno stack) o un'istanza di database, puoi trovare l'ID in diversi modi:
  - La console AMS per un'istanza in uno stack ASG: cerca nella pagina dei dettagli RFC l'RFC che ha creato lo stack. Nella sezione Execution Output, troverai l'ID dello stack ASG e potrai quindi andare alla pagina Console Auto EC2 Scaling Groups e cercare quell'ID stack e trovarne le istanze. Quando trovi l'istanza, selezionala e nella parte inferiore della pagina si apre un'area con i dettagli, incluso l'indirizzo IP.
  - La console AMS per un'istanza autonoma EC2 o di database (DB): cerca nella pagina dei dettagli RFC la RFC che ha creato lo EC2 stack o l'istanza DB. Nella sezione Execution Output, troverai l'ID dell'istanza e l'indirizzo IP.
  - EC2 Console AWS:
    1. Nel pannello di navigazione, scegliere Instances (Istanze). Si apre la pagina Istanze.
    2. Fai clic sull'istanza per cui desideri l'ID. Si apre la pagina dei dettagli dell'istanza con l'ID e l'indirizzo IP.
  - Console di database AWS:
    1. Nella home page, seleziona Istanze DB. Viene visualizzata la pagina Istanze.
    2. Filtra per l'istanza DB per cui desideri l'ID. La pagina dei dettagli dell'istanza si apre e mostra l'ID.
  - CLI/API DI AMS.

> **Note**
>
> Affinché questi comandi funzionino, è necessario installare l'AMS CLI. Per installare l'API o la CLI AMS, vai alla pagina Risorse per gli sviluppatori della console AMS. Per materiale di riferimento sull'API AMS CM o sull'API AMS SKMS, consulta la sezione AMS Information Resources nella Guida per l'utente. Potrebbe essere necessario aggiungere un'`--profile`opzione per l'autenticazione, `aws amsskms` *`ams-cli-command`* `--profile SAML` ad esempio. Potrebbe essere necessario aggiungere l'`--region`opzione anche perché tutti i comandi AMS non utilizzano us-east-1, ad esempio. `aws amscm` *`ams-cli-command`* `--region=us-east-1`

> **Note**
>
> Gli endpoint AMS API/CLI (amscm e amsskms) si trovano nella regione AWS della Virginia settentrionale,. `us-east-1` A seconda di come è impostata l'autenticazione e della regione AWS in cui si trovano l'account e le risorse, potrebbe essere necessario aggiungerli `--region us-east-1` quando si emettono i comandi. Potrebbe anche essere necessario aggiungere`--profile saml`, se questo è il metodo di autenticazione utilizzato.

Esegui il comando seguente per ottenere i dettagli dell'output dell'esecuzione dello stack:

```
aws amsskms get-stack --stack-id STACK_ID
```

L'output è simile al seguente, con l'immagine InstanceId che appare in basso, sotto `Outputs` (i valori mostrati sono esempi):

```
{
    "Stack": {
        "StackId": "stack-7fa52bd5eb8240123",
        "Status": {
            "Id": "CreateCompleted",
            "Name": "CreateCompleted"
        },
        "VpcId": "vpc-01234567890abcdef",
```

```
        "Description": "Amazon",
        "Parameters": [
            {
                "Value": "sg-01234567890abcdef,sg-01234567890abcdef",
                "Key": "SecurityGroups"
            },
            {
                "Value": "subnet-01234567890abcdef",
                "Key": "InstanceSubnetId"
            },
            {
                "Value": "t2.large",
                "Key": "InstanceType"
            },
            {
                "Value": "ami-01234567890abcdef",
                "Key": "InstanceAmiId"
            }
        ],
        "Tags": [],
        "Outputs": [
            {
                "Value": "i-0b22a22eec53b9321",
                "Key": "InstanceId"
            },
            {
                "Value": "10.0.5.000",
                "Key": "InstancePrivateIP"
            }
        ],
        "StackTemplateId": "stm-s6xvs000000000000",
        "CreatedTime": "1486584508416",
        "Name": "Amazon"
    }
}
```


Nomi bastioni compatibili con DNS

MALZ

Per Multi-account landing zone (MALZ), vengono creati record DNS per i bastioni nell'FQDN dell'Active Directory gestita da AMS. AMS sostituisce i bastioni Linux e Windows in base alle

esigenze. Ad esempio, se è necessario implementare una nuova AMI bastion, i record DNS bastion si aggiornano dinamicamente per puntare a nuovi bastioni validi.

1. Per accedere ai bastioni SSH (Linux), usa record DNS come questi: `sshbastion(1-4).Your_Domain.com`

   Ad esempio, dove il dominio è: `Your_Domain`

   - `sshbastion1.Your_Domain.com`
   - `sshbastion2.Your_Domain.com`
   - `sshbastion3.Your_Domain.com`
   - `sshbastion4.Your_Domain.com`

2. Per accedere ai bastioni RDP (Windows), usa record DNS come questi:. `rdp-Username.Your_Domain.com`

   Ad esempio, dove il nome utente è`alex`, `test` demobob, o e il dominio è: `Your_Domain.com`

   - `rdp-alex.Your_Domain.com`
   - `rdp-test.Your_Domain.com`
   - `rdp-demo.Your_Domain.com`
   - `rdp-bob.Your_Domain.com`

SALZ

Se necessario, la landing zone a account singolo (SALZ) sostituisce i bastioni di Linux e Windows. Ad esempio, se è necessario implementare una nuova AMI bastion, i record DNS bastion si aggiornano dinamicamente per puntare a nuovi bastioni validi.

1. Per accedere ai bastioni SSH (Linux), usa record DNS come questi: `sshbastion(1-4).AAccountNumber.amazonaws.com.`

   Ad esempio, `123456789012` dov'è il numero di conto:

   - `sshbastion1.A123456789012.amazonaws.com`
   - `sshbastion2.A123456789012.amazonaws.com`
   - `sshbastion3.A123456789012.amazonaws.com`

- `sshbastion4.A123456789012.amazonaws.com`

2. Per accedere ai bastioni RDP (Windows), usa record DNS come questi:. `rdpbastion(1-4).AACCOUNT_NUMBER.amazonaws.com`

   Ad esempio, `123456789012` dov'è il numero di conto:

   - `rdpbastion1.A123456789012.amazonaws.com`
   - `rdpbastion2.A123456789012.amazonaws.com`
   - `rdpbastion3.A123456789012.amazonaws.com`
   - `rdpbastion4.A123456789012.amazonaws.com`

Individuazione degli indirizzi IP di Bastion

I clienti AMS possono utilizzare i bastioni SSH e RDP, Nomi bastioni compatibili con DNS descritti in precedenza, o gli indirizzi IP bastion.

Per trovare gli indirizzi IP bastion, SSH e RDP, per il tuo account:

1. Solo per le landing zone con più account: accedi all'account Shared Services.
2. Apri la EC2 console e scegli Running Instances.

   Viene visualizzata la pagina Istanze.
3. Nella casella del filtro in alto, inserisci ssh-bastion o rdp-bastion.

   Nella casella del filtro in alto, inserisci customer-ssh o customer-rdp.

   Vengono visualizzati i bastioni SSH and/or RDP del tuo account.

   Tieni presente che oltre ai bastioni SSH, nell'elenco potresti vedere i bastioni della rete perimetrale AMS, che non sono disponibili per questo scopo.
4. Seleziona un bastione SSH o RDP. Se utilizzi un computer Windows e desideri accedere a un'istanza Linux, utilizzi un bastione SSH. Se desideri accedere a un'istanza Windows, utilizzi un bastione RDP. Se utilizzi un sistema operativo Linux e desideri accedere a un'istanza Windows, utilizzi un bastione SSH tramite un tunnel RDP (in questo modo puoi accedere al desktop di Windows). Per accedere a un'istanza Linux da un sistema operativo Linux, si utilizza un bastione SSH.

Istanze EC2: creazione

Puoi utilizzare la console AMS o API/CLI creare un Amazon EC2 e un Amazon EC2 con volumi aggiuntivi.

Crea uno stack

Creazione di un'istanza EC2 con la console

Di seguito viene illustrato questo tipo di modifica nella console AMS.

Come funziona:

1. Vai alla pagina Crea RFC: nel riquadro di navigazione a sinistra della console AMS, fai clic RFCsper aprire la pagina di RFCs elenco, quindi fai clic su Crea RFC.
2. Scegli un tipo di modifica (CT) popolare nella visualizzazione predefinita Sfoglia i tipi di modifica o seleziona un CT nella visualizzazione Scegli per categoria.
   - Naviga per tipo di modifica: puoi fare clic su un CT popolare nell'area di creazione rapida per aprire immediatamente la pagina Run RFC. Nota che non puoi scegliere una versione CT precedente con creazione rapida.

     Per ordinare CTs, utilizzate l'area Tutti i tipi di modifica nella vista a scheda o tabella. In entrambe le visualizzazioni, selezionate un CT, quindi fate clic su Crea RFC per aprire la pagina Esegui RFC. Se applicabile, accanto al pulsante Crea RFC viene visualizzata l'opzione Crea con una versione precedente.
   - Scegli per categoria: seleziona una categoria, sottocategoria, articolo e operazione e la casella dei dettagli CT si apre con l'opzione Crea con una versione precedente, se applicabile. Fai clic su Crea RFC per aprire la pagina Esegui RFC.
3. Nella pagina Run RFC, apri l'area del nome CT per visualizzare la casella dei dettagli CT. È richiesto un oggetto (questo campo viene compilato automaticamente se si sceglie il CT nella vista Sfoglia i tipi di modifica). Apri l'area di configurazione aggiuntiva per aggiungere informazioni sull'RFC.

   Nell'area di configurazione dell'esecuzione, utilizza gli elenchi a discesa disponibili o inserisci i valori per i parametri richiesti. Per configurare i parametri di esecuzione opzionali, aprite l'area di configurazione aggiuntiva.

4. Al termine, fate clic su Esegui. Se non sono presenti errori, viene visualizzata la pagina RFC creata correttamente con i dettagli RFC inviati e l'output iniziale di Run.
5. Apri l'area dei parametri di esecuzione per visualizzare le configurazioni inviate. Aggiorna la pagina per aggiornare lo stato di esecuzione RFC. Facoltativamente, annulla la RFC o creane una copia con le opzioni nella parte superiore della pagina.

Creazione di un'istanza EC2 con la CLI

Come funziona:

1. Usa Inline Create (emetti un `create-rfc` comando con tutti i parametri RFC e di esecuzione inclusi) o Template Create (crei due file JSON, uno per i parametri RFC e uno per i parametri di esecuzione) ed emetti il `create-rfc` comando con i due file come input. Entrambi i metodi sono descritti qui.
2. Invia il `aws amscm submit-rfc --rfc-id` *ID* comando RFC: con l'ID RFC restituito.

   Monitora il comando RFC:. `aws amscm get-rfc --rfc-id` *ID*

Per verificare la versione del tipo di modifica, usa questo comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> È possibile utilizzare qualsiasi `CreateRfc` parametro con qualsiasi RFC, indipendentemente dal fatto che faccia parte o meno dello schema per il tipo di modifica. Ad esempio, per ricevere notifiche quando lo stato RFC cambia, aggiungi questa riga `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` alla parte dei parametri RFC della richiesta (non ai parametri di esecuzione). Per un elenco di tutti i CreateRfc parametri, consulta l'AMS Change Management API Reference.

CREAZIONE IN LINEA:

Esegui il comando create RFC con i parametri di esecuzione forniti in linea (evita le virgolette quando fornisci i parametri di esecuzione in linea), quindi invia l'ID RFC restituito. Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

```
aws amscm create-rfc --change-type-id "ct-14027q0sjyt1h" --change-type-version "4.0"
 --title "EC2-Create-RFC" --execution-parameters "{\"Description\": \"Create a new
 EC2 Instance stack\",\"VpcId\": \"vpc-0a60eb65b4EXAMPLE\",\"Name\": \"My-EC2\",
\"TimeoutInMinutes\": 60,\"Parameters\": {\"InstanceAmiId\": \"ami-1234567890EXAMPLE\",
\"InstanceDetailedMonitoring\": false,\"InstanceEBSOptimized\": false,\"InstanceProfile
\": \"customer-mc-ec2-instance-profile\",\"InstanceRootVolumeIops\": 3000,
\"InstanceRootVolumeType\": \"gp3\",\"InstanceType\": \"t2.large\",\"InstanceUserData
\": \"\",\"InstanceSubnetId\": \"subnet-0bb1c79de3EXAMPLE\",\"EnforceIMDSV2\":
 \"false\"}}"
```

CREAZIONE DEL MODELLO:

1. Esporta i parametri di esecuzione per questo tipo di modifica in un file JSON; questo esempio lo chiama Create EC2 Params.json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-14027q0sjyt1h" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2Params.json
   ```

2. Modificate e salvate il file Create Params. EC2 Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

   ```
   {
     "Description": "Create a new EC2 Instance stack",
     "VpcId": "vpc-0a60eb65b4EXAMPLE",
     "Name": "My-EC2",
     "TimeoutInMinutes": 60,
     "Parameters": {
       "InstanceAmiId": "ami-1234567890EXAMPLE",
       "InstanceDetailedMonitoring": false,
       "InstanceEBSOptimized": false,
       "InstanceProfile": "customer-mc-ec2-instance-profile",
       "InstanceRootVolumeIops": 3000,
       "InstanceRootVolumeType": "gp3",
       "InstanceType": "t2.large",
       "InstanceUserData": "",
       "InstanceSubnetId": "subnet-0bb1c79de3EXAMPLE",
       "EnforceIMDSV2": "false"
     }
   }
   ```

3. Esporta il modello RFC in un file nella cartella corrente; questo esempio lo chiama Create EC2 RFC.json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2Rfc.json
```

4. Modificate e salvate il file Create RFC.json. EC2 Ad esempio, puoi sostituire il contenuto con qualcosa del genere:.

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-14027q0sjyt1h",
"Title":                "EC2-Create-RFC"
}
```

5. Crea la RFC, specificando il file Create EC2 Rfc e il file EC2 Create Params:

```
aws amscm create-rfc --cli-input-json file://CreateEC2Rfc.json  --execution-
parameters file://CreateEC2Params.json
```

Nella risposta ricevi l'ID della nuova RFC e puoi utilizzarlo per inviare e monitorare la RFC. Finché non la invii, la RFC rimane nello stato di modifica e non si avvia.

Suggerimenti

Gruppi di sicurezza

A partire dalla versione 3.0 di questo tipo di modifica, AMS non associa i gruppi di sicurezza AMS predefiniti se si specificano gruppi di sicurezza propri. Se non specificate i vostri gruppi di sicurezza nella richiesta, AMS allega i gruppi di sicurezza AMS predefiniti. Nelle versioni precedenti, AMS associava i gruppi di sicurezza predefiniti indipendentemente dal fatto che fossero stati forniti o meno i propri gruppi di sicurezza.
Attualmente, se si specificano gruppi di sicurezza personalizzati, è necessario specificare anche i gruppi IDs di sicurezza AMS predefiniti per il proprio account `mc-initial-garden-SG-name` `emc-initial-garden-SG-name`.

Tipi di istanza

AMS non consiglia i tipi t2.micro/t3.micro e t2.nano/t3.nano. Si tratta di tipi di istanze più piccoli e possono ridurre le prestazioni dell'applicazione e degli strumenti AMS. Le istanze EC2 richiedono una capacità sufficiente per supportare strumenti AMS come EPS, SSM

e Cloudwatch oltre al carico di lavoro dell'applicazione. Per ulteriori informazioni, consulta Scelta del tipo di istanza EC2 giusto per l'applicazione.

Per creare uno stack EC2 con volumi aggiuntivi, consulta EC2 Stack | Create (with Additional Volumes).

Puoi aggiungere fino a 50 tag, ma per farlo devi abilitare la visualizzazione di configurazione aggiuntiva.

Se necessario, consulta EC2 instance stack create fail.

Crea uno stack (con volumi aggiuntivi)

Creazione di un'istanza EC2 e di volumi aggiuntivi con la console

Di seguito viene illustrato questo tipo di modifica nella console AMS.

Come funziona:

1. Vai alla pagina Crea RFC: nel riquadro di navigazione a sinistra della console AMS, fai clic RFCsper aprire la pagina di RFCs elenco, quindi fai clic su Crea RFC.
2. Scegli un tipo di modifica (CT) popolare nella visualizzazione predefinita Sfoglia i tipi di modifica o seleziona un CT nella visualizzazione Scegli per categoria.
   - Naviga per tipo di modifica: puoi fare clic su un CT popolare nell'area di creazione rapida per aprire immediatamente la pagina Run RFC. Nota che non puoi scegliere una versione CT precedente con creazione rapida.

     Per ordinare CTs, utilizzate l'area Tutti i tipi di modifica nella vista a scheda o tabella. In entrambe le visualizzazioni, selezionate un CT, quindi fate clic su Crea RFC per aprire la pagina Esegui RFC. Se applicabile, accanto al pulsante Crea RFC viene visualizzata l'opzione Crea con una versione precedente.
   - Scegli per categoria: seleziona una categoria, sottocategoria, articolo e operazione e la casella dei dettagli CT si apre con l'opzione Crea con una versione precedente, se applicabile. Fai clic su Crea RFC per aprire la pagina Esegui RFC.
3. Nella pagina Run RFC, apri l'area del nome CT per visualizzare la casella dei dettagli CT. È richiesto un oggetto (questo campo viene compilato automaticamente se si sceglie il CT nella

vista Sfoglia i tipi di modifica). Apri l'area di configurazione aggiuntiva per aggiungere informazioni sull'RFC.

Nell'area di configurazione dell'esecuzione, utilizza gli elenchi a discesa disponibili o inserisci i valori per i parametri richiesti. Per configurare i parametri di esecuzione opzionali, aprite l'area di configurazione aggiuntiva.

4. Al termine, fate clic su Esegui. Se non sono presenti errori, viene visualizzata la pagina RFC creata correttamente con i dettagli RFC inviati e l'output iniziale di Run.
5. Apri l'area dei parametri di esecuzione per visualizzare le configurazioni inviate. Aggiorna la pagina per aggiornare lo stato di esecuzione RFC. Facoltativamente, annulla la RFC o creane una copia con le opzioni nella parte superiore della pagina.

Creazione di un'istanza EC2 e di volumi aggiuntivi con la CLI

Come funziona:

1. Utilizza Inline Create (immetti un `create-rfc` comando con tutti i parametri RFC e di esecuzione inclusi) o Template Create (crei due file JSON, uno per i parametri RFC e uno per i parametri di esecuzione) ed emetti il `create-rfc` comando con i due file come input. Entrambi i metodi sono descritti qui.
2. Invia il `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con l'ID RFC restituito.

   Monitora il comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Per verificare la versione del tipo di modifica, usa questo comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> È possibile utilizzare qualsiasi `CreateRfc` parametro con qualsiasi RFC, indipendentemente dal fatto che faccia parte o meno dello schema per il tipo di modifica. Ad esempio, per ricevere notifiche quando lo stato RFC cambia, aggiungi questa riga `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` alla

parte dei parametri RFC della richiesta (non ai parametri di esecuzione). Per un elenco di tutti i CreateRfc parametri, consulta l'AMS Change Management API Reference.

CREAZIONE IN LINEA:

Esegui il comando create RFC con i parametri di esecuzione forniti in linea (evita le virgolette quando fornisci i parametri di esecuzione in linea), quindi invia l'ID RFC restituito (l'esempio mostra solo i parametri obbligatori). Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

```
aws amscm create-rfc --change-type-id "ct-1aqsjf86w6vxg" --change-type-version "4.0"
 --title "EC2-Create-A-V-QC" --execution-parameters "{\"Description\":\"My EC2 stack
 with addl vol\",\"VpcId\":\"VPC_ID\",\"Name\":\"My Stack\",\"StackTemplateId\":
\"stm-nn8v8ffhcal611bmo\",\"TimeoutInMinutes\":60,\"Parameters\":{\"InstanceAmiId\":
\"AMI_ID\",\"InstanceSubnetId\":\"SUBNET_ID\"}}
```

CREAZIONE DEL MODELLO:

1. Esporta i parametri di esecuzione per questo tipo di modifica in un file JSON denominato Create EC2 AVParams .json.

   ```
   aws amscm get-change-type-version --change-type-id "ct-1aqsjf86w6vxg" --query
    "ChangeTypeVersion.ExecutionInputSchema" --output text > CreateEC2AVParams.json
   ```

2. Modifica e salva il EC2 AVParams file Create (l'esempio mostra la maggior parte dei parametri). Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

   ```
   {
   "Description":      "EC2-Create-1-Addl-Volumes",
   "VpcId":            "VPC_ID",
   "StackTemplateId":  "stm-nn8v8ffhcal611bmo",
   "Name":             "My-EC2-1-Addl-Volume",
   "TimeoutInMinutes": 60,
   "Parameters":   {
       "InstanceAmiId":    "AMI_ID",
       "InstanceSecurityGroupIds": "SECURITY_GROUP_ID",
       "InstanceCoreCount": 1,
       "InstanceThreadsPerCore": 2,
       "InstanceDetailedMonitoring": "true",
       "InstanceEBSOptimized": "false",
       "InstanceProfile": "customer-mc-ec2-instance-profile",
   ```

```
    "InstanceRootVolumeIops": 100,
    "InstanceRootVolumeName": "/dev/xvda",
    "InstanceRootVolumeSize": 50,
    "InstanceRootVolumeType": "io1",
    "RootVolumeKmsKeyId": "default",
    "InstancePrivateStaticIp": "10.27.0.100",
    "InstanceSecondaryPrivateIpAddressCount": 0,
    "InstanceTerminationProtection": "false",
    "InstanceType": "t3.large",
    "CreditSpecification": "unlimited",
    "InstanceUserData": "echo $",
    "Volume1Encrypted": "true",
    "Volume1Iops":      "IOPS"
    "Volume1KmsKeyId":  "KMS_MASTER_KEY_ID",
    "Volume1Name":      "xvdh"
    "Volume1Size":      "2 GiB",
    "Volume1Snapshot":  "SNAPSHOT_ID",
    "Volume1Type":      "iol",
    "InstanceSubnetId": "SUBNET_ID"
    }
}
```

3. Esporta il modello RFC in un file nella cartella corrente; questo esempio lo chiama Create EC2 AVRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateEC2AVRfc.json
```

4. Modifica e salva il file Create .json EC2AVRfc. Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

```
{
"ChangeTypeVersion":    "4.0",
"ChangeTypeId":         "ct-1aqsjf86w6vxg",
"Title":                "EC2-Create-1-Addl-Volume-RFC"
}
```

5. Create la RFC, specificando Create EC2 AVRfc file e EC2 AVParams Create file:

```
aws amscm create-rfc --cli-input-json file://CreateEC2AVRfc.json  --execution-
parameters file://CreateEC2AVParams.json
```

Nella risposta ricevi l'ID della nuova RFC e puoi utilizzarlo per inviare e monitorare la RFC. Finché non la invii, la RFC rimane nello stato di modifica e non si avvia.

Suggerimenti

Important

Esiste una nuova versione di questo tipo di modifica, la v 4.0, che utilizza una versione diversa StackTemplateId (stm-nn8v8ffhcal611bmo). Questo è importante se si invia la RFC con questo tipo di modifica alla riga di comando. La nuova versione introduce due nuovi parametri (RootVolumeKmsKeyIde CreditSpecification) e modifica l'impostazione predefinita per un parametro esistente (). InstanceType

Tipi di istanza

- Se scegliete di specificare il numero di core o thread, dovete specificare i valori per entrambi. Utilizzate i parametri `InstanceCoreCount` e. `InstanceThreadsPerCore` Per trovare combinazioni valide di core/thread, consulta Core e thread della CPU per core di CPU per tipo di istanza.
- AMS non consiglia i tipi di istanza t2.micro/t3.micro o t2.nano/t3.nano. Sono troppo piccoli per supportare strumenti AMS come EPS, SSM e Cloudwatch in aggiunta al carico di lavoro aziendale. Per ulteriori informazioni, consulta Scelta del tipo di istanza EC2 giusto per la propria applicazione.
- Nella versione 4.0, il tipo predefinito è stato portato da t2.large a t3.large. Per impostazione predefinita, le istanze T3 vengono avviate con «crediti illimitati». Non si verificherà alcuna limitazione della CPU anche se l'istanza consuma tutti i crediti della CPU. Puoi invece scegliere le istanze T2 e utilizzare l'opzione illimitata. CreditSpecification
- Per ulteriori informazioni su Amazon EC2, incluse le raccomandazioni sulle dimensioni, consulta la documentazione di Amazon Elastic Compute Cloud.

Per aggiornare lo stack EC2 con volumi aggiuntivi dopo la creazione, consulta EC2 Instance Stack: aggiornamento (con volumi aggiuntivi)

Accesso, richiesta

Richiedi l'accesso amministrativo

Richiedere l'accesso da amministratore tramite la console

Di seguito viene illustrato questo tipo di modifica nella console AMS.

Come funziona:

1. Vai alla pagina Crea RFC: nel riquadro di navigazione a sinistra della console AMS, fai clic RFCsper aprire la pagina di RFCs elenco, quindi fai clic su Crea RFC.
2. Scegli un tipo di modifica (CT) popolare nella visualizzazione predefinita Sfoglia i tipi di modifica o seleziona un CT nella visualizzazione Scegli per categoria.
   - Naviga per tipo di modifica: puoi fare clic su un CT popolare nell'area di creazione rapida per aprire immediatamente la pagina Run RFC. Nota che non puoi scegliere una versione CT precedente con creazione rapida.

     Per ordinare CTs, utilizzate l'area Tutti i tipi di modifica nella vista a scheda o tabella. In entrambe le visualizzazioni, selezionate un CT, quindi fate clic su Crea RFC per aprire la pagina Esegui RFC. Se applicabile, accanto al pulsante Crea RFC viene visualizzata l'opzione Crea con una versione precedente.
   - Scegli per categoria: seleziona una categoria, sottocategoria, articolo e operazione e la casella dei dettagli CT si apre con l'opzione Crea con una versione precedente, se applicabile. Fai clic su Crea RFC per aprire la pagina Esegui RFC.
3. Nella pagina Run RFC, apri l'area del nome CT per visualizzare la casella dei dettagli CT. È richiesto un Oggetto (questo campo viene compilato automaticamente se si sceglie il CT nella vista Sfoglia i tipi di modifica). Apri l'area di configurazione aggiuntiva per aggiungere informazioni sull'RFC.

   Nell'area di configurazione dell'esecuzione, utilizza gli elenchi a discesa disponibili o inserisci i valori per i parametri richiesti. Per configurare i parametri di esecuzione opzionali, aprite l'area di configurazione aggiuntiva.
4. Al termine, fate clic su Esegui. Se non sono presenti errori, viene visualizzata la pagina RFC creata correttamente con i dettagli RFC inviati e l'output iniziale di Run.

5. Apri l'area dei parametri di esecuzione per visualizzare le configurazioni inviate. Aggiorna la pagina per aggiornare lo stato di esecuzione RFC. Facoltativamente, annulla la RFC o creane una copia con le opzioni nella parte superiore della pagina.

Richiesta dell'accesso da amministratore con la CLI

Come funziona:

1. Utilizza Inline Create (immetti un `create-rfc` comando con tutti i parametri RFC e di esecuzione inclusi) o Template Create (crei due file JSON, uno per i parametri RFC e uno per i parametri di esecuzione) ed esegui il `create-rfc` comando con i due file come input. Entrambi i metodi sono descritti qui.
2. Invia il `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con l'ID RFC restituito.

   Monitora il comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Per verificare la versione del tipo di modifica, usa questo comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> È possibile utilizzare qualsiasi `CreateRfc` parametro con qualsiasi RFC, indipendentemente dal fatto che faccia parte o meno dello schema per il tipo di modifica. Ad esempio, per ricevere notifiche quando lo stato RFC cambia, aggiungi questa riga `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` alla parte dei parametri RFC della richiesta (non ai parametri di esecuzione). Per un elenco di tutti i CreateRfc parametri, consulta l'AMS Change Management API Reference.

CREAZIONE IN LINEA:

Esegui il comando create RFC con i parametri di esecuzione forniti in linea (evita le virgolette quando fornisci i parametri di esecuzione in linea), quindi invia l'ID RFC restituito. Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

```
aws --profile saml amscm create-rfc --change-type-id "ct-1dmlg9g1l91h6" --change-type-
version "3.0" --title "Stack-Admin-Access-QC" --execution-parameters "{\"DomainFQDN
\":\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

CREAZIONE DEL MODELLO:

1. Esporta lo schema JSON dei parametri di esecuzione per questo tipo di modifica in un file; questo esempio lo chiama GrantAdminAccessParams .json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-1dmlg9g1l91h6"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantAdminAccessParams.json
   ```

   Modificate e salvate il file. GrantAdminAccessParams Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

   ```
   {
   "DomainFQDN":           "mycorpdomain.acme.com",
   "StackIds":             [STACK_ID, STACK_ID],
   "TimeRequestedInHours": 12,
   "Username":             ["USERNAME", "USERNAME"],
   "VpcId":                "VPC_ID"
   }
   ```

   Nota che l'`TimeRequestedInHours`opzione predefinita è un'ora. Puoi richiedere fino a dodici ore.

2. Esporta il modello RFC in un file nella cartella corrente; questo esempio lo chiama GrantAdminAccessRfc .json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > GrantAdminAccessRfc.json
   ```

3. Modifica e salva il file.json. GrantAdminAccessRfc Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

   ```
   {
   "ChangeTypeId":         "ct-1dmlg9g1l91h6",
   "ChangeTypeVersion":    "3.0",
   "Title":                "Request-Admin-Access-to-EC2-RFC"
   ```

```
}
```

4. Crea la RFC, specificando il GrantAdminAccessRfc file e il GrantAdminAcessParams file:

```
aws amscm create-rfc --cli-input-json file://GrantAdminAccessRfc.json --execution-
parameters file://GrantAdminAccessParams.json
```

Nella risposta ricevi l'ID della nuova RFC e puoi utilizzarlo per inviare e monitorare la RFC. Finché non la invii, la RFC rimane nello stato di modifica e non si avvia.

Per accedere all'istanza tramite un bastione, segui la procedura successiva, Instance access examples.

Suggerimenti

> **Note**
>
> Puoi inviare un aggiornamento alla tua richiesta di accesso prima che scada. Per informazioni, consulta Stack Admin Access | Update.
> Per accedere a un'istanza che fa parte di un ASG, richiedi l'accesso allo stack ASG, che ti dà accesso a tutte le istanze associate.

Per un esempio sulla richiesta di accesso, consulta ReadOnly access: requesting. ReadOnly

Richiedi l'accesso ReadOnly

Richiesta di accesso tramite la console ReadOnly

Di seguito viene illustrato questo tipo di modifica nella console AMS.

Come funziona:

1. Vai alla pagina Crea RFC: nel riquadro di navigazione a sinistra della console AMS, fai clic RFCsper aprire la pagina di RFCs elenco, quindi fai clic su Crea RFC.
2. Scegli un tipo di modifica (CT) popolare nella visualizzazione predefinita Sfoglia i tipi di modifica o seleziona un CT nella visualizzazione Scegli per categoria.

- Naviga per tipo di modifica: puoi fare clic su un CT popolare nell'area di creazione rapida per aprire immediatamente la pagina Run RFC. Nota che non puoi scegliere una versione CT precedente con creazione rapida.

  Per ordinare CTs, utilizzate l'area Tutti i tipi di modifica nella vista a scheda o tabella. In entrambe le visualizzazioni, selezionate un CT, quindi fate clic su Crea RFC per aprire la pagina Esegui RFC. Se applicabile, accanto al pulsante Crea RFC viene visualizzata l'opzione Crea con una versione precedente.
- Scegli per categoria: seleziona una categoria, sottocategoria, articolo e operazione e la casella dei dettagli CT si apre con l'opzione Crea con una versione precedente, se applicabile. Fai clic su Crea RFC per aprire la pagina Esegui RFC.

3. Nella pagina Run RFC, apri l'area del nome CT per visualizzare la casella dei dettagli CT. È richiesto un Oggetto (questo campo viene compilato automaticamente se si sceglie il CT nella vista Sfoglia i tipi di modifica). Apri l'area di configurazione aggiuntiva per aggiungere informazioni sull'RFC.

   Nell'area di configurazione dell'esecuzione, utilizza gli elenchi a discesa disponibili o inserisci i valori per i parametri richiesti. Per configurare i parametri di esecuzione opzionali, aprite l'area di configurazione aggiuntiva.
4. Al termine, fate clic su Esegui. Se non sono presenti errori, viene visualizzata la pagina RFC creata correttamente con i dettagli RFC inviati e l'output iniziale di Run.
5. Apri l'area dei parametri di esecuzione per visualizzare le configurazioni inviate. Aggiorna la pagina per aggiornare lo stato di esecuzione RFC. Facoltativamente, annulla la RFC o creane una copia con le opzioni nella parte superiore della pagina.

Richiesta di ReadOnly accesso con la CLI

Come funziona:

1. Utilizzate Inline Create (emettete un `create-rfc` comando con tutti i parametri RFC e di esecuzione inclusi) o Template Create (create due file JSON, uno per i parametri RFC e uno per i parametri di esecuzione) ed emettete il `create-rfc` comando con i due file come input. Entrambi i metodi sono descritti qui.
2. Invia il `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con l'ID RFC restituito.

   Monitora il comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Per verificare la versione del tipo di modifica, usa questo comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> È possibile utilizzare qualsiasi `CreateRfc` parametro con qualsiasi RFC, indipendentemente dal fatto che faccia parte o meno dello schema per il tipo di modifica. Ad esempio, per ricevere notifiche quando lo stato RFC cambia, aggiungi questa riga `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` alla parte dei parametri RFC della richiesta (non ai parametri di esecuzione). Per un elenco di tutti i CreateRfc parametri, consulta l'AMS Change Management API Reference.

CREAZIONE IN LINEA:

Esegui il comando create RFC con i parametri di esecuzione forniti in linea (evita le virgolette quando fornisci i parametri di esecuzione in linea), quindi invia l'ID RFC restituito. Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

```
aws --profile saml amscm create-rfc --change-type-id "ct-199h35t7uz6jl" --change-type-
version "3.0" --title "Stack-RO-Access-QC" --execution-parameters "{\"DomainFQDN\":
\"TEST.com\",\"StackIds\":[\"stack-01234567890abcdef\"],\"TimeRequestedInHours\":1,
\"Usernames\":[\"TEST\"],\"VpcId\":\"VPC_ID\"}"
```

CREAZIONE DEL MODELLO:

1. Esporta lo schema JSON dei parametri di esecuzione per questo tipo di modifica in un file; questo esempio lo chiama GrantReadOnlyAccessParams .json:

   ```
   aws amscm get-change-type-version --change-type-id "ct-199h35t7uz6jl"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    GrantReadOnlyAccessParams.json
   ```

   Modificate e salvate il file. GrantReadOnlyAccessParams Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

   ```
   {
   ```

```
"DomainFQDN":           "mycorpdomain.acme.com",
"StackIds":             [STACK_ID, STACK_ID],
"TimeRequestedInHours": 12,
"Usernames":             ["USERNAME", "USERNAME"],
"VpcId":                "VPC_ID"
}
```

Nota che l'`TimeRequestedInHours`opzione predefinita è un'ora. Puoi richiedere fino a dodici ore.

2. Esporta il modello RFC in un file nella cartella corrente; questo esempio lo chiama GrantReadOnlyAccessRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > GrantReadOnlyAccessRfc.json
```

3. Modifica e salva il file.json. GrantReadOnlyAccessRfc Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

```
{
"ChangeTypeId":         "ct-199h35t7uz6jl",
"ChangeTypeVersion":    "3.0",
"Title":                "Request-ReadOnly-Access-to-EC2-RFC"
}
```

4. Crea la RFC, specificando il GrantReadOnlyAccessRfc file e il GrantReadOnlyAcessParams file:

```
aws amscm create-rfc --cli-input-json file://GrantReadOnlyAccessRfc.json --
execution-parameters file://GrantReadOnlyAccessParams.json
```

Nella risposta ricevi l'ID della nuova RFC e puoi utilizzarlo per inviare e monitorare la RFC. Finché non la invii, la RFC rimane nello stato di modifica e non si avvia.

Per accedere all'istanza tramite un bastione, segui la procedura successiva, Instance access examples.

Suggerimenti

> **Note**
>
> Puoi inviare un aggiornamento alla tua richiesta di accesso prima che scada. Per i dettagli, consulta Stack Read-Only Access | Update.

Per accedere a un'istanza che fa parte di un gruppo di Auto Scaling (ASG) EC2, richiedi l'accesso allo stack ASG, che ti dà accesso a tutte le istanze associate.

Per una procedura dettagliata sulla richiesta dell'accesso da amministratore, consulta Admin Access: requesting.

Altro | Altro RFC, creazione (CLI)

Questo esempio mostra come richiedere la modifica di nessuno degli CTs indirizzi disponibili utilizzando Management | Other | Other | Create CT (ct-1e1xtak34nx76).

Usa questo CT quando non riesci a trovare un tipo di modifica per quello che desideri; tuttavia, se non sei sicuro di come specificare i parametri in un CT esistente, è meglio inviare una richiesta di assistenza. Per informazioni sull'invio di richieste di assistenza, consulta Esempi di richieste di assistenza.

Questo tipo di RFC è obbligatorio per l'approvazione, il che significa che richiede l'approvazione di AMS prima di poter essere implementato. Dopo aver inviato la RFC, un operatore AMS ti contatterà per discutere dello stack che desideri implementare.

> **Note**
>
> Quando si utilizza la CTs modalità manuale, AMS consiglia di utilizzare l'opzione ASAP Scheduling (scegliere ASAP nella console, lasciare vuote le date di inizio e fine nell'API/CLI) in quanto CTs richiedono che un operatore AMS esamini la RFC ed eventualmente comunichi con l'utente prima che possa essere approvata ed eseguita. Se li pianifichi RFCs, assicurati di attendere almeno 24 ore. Se l'approvazione non avviene prima dell'orario di inizio programmato, la RFC viene rifiutata automaticamente.

DATI RICHIESTI:

- `Comment`: A cosa serve l'RFC.
- `ChangeTypeIdeChangeTypeVersion`: Usa Other | Create (`ct-1e1xtak34nx76`) per richiedere nuove risorse, usa Other | Update (`ct-0xdawir96cy7k`) per modificare le risorse esistenti; entrambi lo sono`v1`.

DATI OPZIONALI`Priority`: I valori accettabili sono `High`, `Medium`, o`Low`.

CREAZIONE IN LINEA:

- Esegui il comando create RFC con i parametri di esecuzione forniti in linea (evita le virgolette quando fornisci i parametri di esecuzione in linea). L'esempio utilizza Other | Create.

```
aws amscm create-rfc --change-type-id "ct-1e1xtak34nx76" --change-type-version "1.0"
 --title "TITLE" --execution-parameters "{\"Comment\": \"What you want created\"}"
```

- Invia la RFC utilizzando l'ID RFC restituito nell'operazione di creazione RFC. Fino all'invio, la RFC rimane nello `Editing` stato e non viene applicata.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- Monitora lo stato RFC e visualizza l'output di esecuzione:

```
aws amscm get-rfc --rfc-id RFC_ID
```

CREAZIONE DEL MODELLO:

1. Crea e salva un file JSON per i parametri di esecuzione; l'esempio lo chiama OtherParams .json e include il parametro opzionale: `Priority`

```
{
"Comment":          "What you want created",
"Priority":         "Medium"
}
```

2. Crea e salva un file JSON per i parametri RFC; l'esempio lo chiama .json. OtherRfc

```
{
"ChangeTypeId":         "ct-1e1xtak34nx76",
"ChangeTypeVersion":    "1.0",
"Title":                "TITLE"
}
```

3. Crea l'RFC, specificando il file e il file: OtherRfc OtherParams

```
aws amscm create-rfc --cli-input-json file://OtherRfc.json  --execution-parameters
 file://OtherParams.json
```

Riceverai RfcId il nuovo RFC nella risposta. Esempio:

```
{
"RfcId": "RFC-ID"
}
```

4. Invia la RFC:

```
aws amscm submit-rfc --rfc-id RFC-ID
```

Se non vengono segnalati errori, l'operazione è andata a buon fine.

5. Per monitorare lo stato della richiesta e visualizzare l'output di esecuzione:

```
aws amscm get-rfc --rfc-id RFC-ID
```

Qualsiasi pila: eliminazione, riavvio, avvio, arresto

È possibile utilizzare la console AMS o API/CLI per eliminare, riavviare, avviare o arrestare uno stack AMS.

Elimina lo stack

Eliminazione di uno stack con la console

Schermata di questo tipo di modifica nella console AMS:

Come funziona:

1. Vai alla pagina Crea RFC: nel riquadro di navigazione a sinistra della console AMS, fai clic RFCsper aprire la pagina di RFCs elenco, quindi fai clic su Crea RFC.
2. Scegli un tipo di modifica (CT) popolare nella visualizzazione predefinita Sfoglia i tipi di modifica o seleziona un CT nella visualizzazione Scegli per categoria.

- Naviga per tipo di modifica: puoi fare clic su un CT popolare nell'area di creazione rapida per aprire immediatamente la pagina Run RFC. Nota che non puoi scegliere una versione CT precedente con creazione rapida.

  Per ordinare CTs, utilizzate l'area Tutti i tipi di modifica nella vista a scheda o tabella. In entrambe le visualizzazioni, selezionate un CT, quindi fate clic su Crea RFC per aprire la pagina Esegui RFC. Se applicabile, accanto al pulsante Crea RFC viene visualizzata l'opzione Crea con una versione precedente.

- Scegli per categoria: seleziona una categoria, sottocategoria, articolo e operazione e la casella dei dettagli CT si apre con l'opzione Crea con una versione precedente, se applicabile. Fai clic su Crea RFC per aprire la pagina Esegui RFC.

3. Nella pagina Run RFC, apri l'area del nome CT per visualizzare la casella dei dettagli CT. È richiesto un Oggetto (questo campo viene compilato automaticamente se si sceglie il CT nella visualizzazione Sfoglia i tipi di modifica). Apri l'area di configurazione aggiuntiva per aggiungere informazioni sull'RFC.

   Nell'area di configurazione dell'esecuzione, utilizza gli elenchi a discesa disponibili o inserisci i valori per i parametri richiesti. Per configurare i parametri di esecuzione opzionali, aprite l'area di configurazione aggiuntiva.

4. Al termine, fate clic su Esegui. Se non sono presenti errori, viene visualizzata la pagina RFC creata correttamente con i dettagli RFC inviati e l'output iniziale di Run.

5. Apri l'area dei parametri di esecuzione per visualizzare le configurazioni inviate. Aggiorna la pagina per aggiornare lo stato di esecuzione RFC. Facoltativamente, annulla la RFC o creane una copia con le opzioni nella parte superiore della pagina.

Eliminazione di uno stack con la CLI

Come funziona:

1. Utilizza Inline Create (immetti un `create-rfc` comando con tutti i parametri RFC e di esecuzione inclusi) o Template Create (crei due file JSON, uno per i parametri RFC e uno per i parametri di esecuzione) ed esegui il `create-rfc` comando con i due file come input. Entrambi i metodi sono descritti qui.
2. Invia il `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con l'ID RFC restituito.

   Monitora il comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Per verificare la versione del tipo di modifica, usa questo comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> È possibile utilizzare qualsiasi `CreateRfc` parametro con qualsiasi RFC, indipendentemente dal fatto che faccia parte o meno dello schema per il tipo di modifica. Ad esempio, per ricevere notifiche quando lo stato RFC cambia, aggiungi questa riga `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` alla parte dei parametri RFC della richiesta (non ai parametri di esecuzione). Per un elenco di tutti i CreateRfc parametri, consulta l'AMS Change Management API Reference.

CREAZIONE IN LINEA:

Esegui il comando create RFC con i parametri di esecuzione forniti in linea (evita le virgolette quando fornisci i parametri di esecuzione in linea), quindi invia l'ID RFC restituito. Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0" --
title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CREAZIONE DEL MODELLO:

1. Esporta il modello RFC in un file nella cartella corrente; questo esempio lo chiama DeleteStackRfc .json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. Modifica e salva il file.json. DeleteStackRfc

   Le virgolette interne dell'estensione ExecutionParameters JSON devono essere eliminate con una barra rovesciata (\). Esempio senza ora di inizio e fine:

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   ```

```
"Title":                "Delete-My-Stack-RFC"
"ExecutionParameters":  "{
        \"StackId\":\"STACK_ID\"}"
}
```

3. Crea la RFC:

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

Nella risposta ricevi l'ID della nuova RFC e puoi utilizzarlo per inviare e monitorare la RFC. Finché non la invii, la RFC rimane nello stato di modifica e non si avvia.

Suggerimenti

> **Note**
>
> Se si elimina un bucket S3, è necessario prima svuotarlo degli oggetti.

> **Important**
>
> L'eliminazione degli stack può avere conseguenze indesiderate e impreviste. Per avvertenze importanti, consulta la sezione Risoluzione dei problemi RFC per Delete Stack. RFCs

Riavvia lo stack

Riavvio di uno stack con la console

Schermata di questo tipo di modifica nella console AMS:

Come funziona:

1. Vai alla pagina Crea RFC: nel riquadro di navigazione a sinistra della console AMS, fai clic RFCsper aprire la pagina di RFCs elenco, quindi fai clic su Crea RFC.
2. Scegli un tipo di modifica (CT) popolare nella visualizzazione predefinita Sfoglia i tipi di modifica o seleziona un CT nella visualizzazione Scegli per categoria.

- Naviga per tipo di modifica: puoi fare clic su un CT popolare nell'area di creazione rapida per aprire immediatamente la pagina Run RFC. Nota che non puoi scegliere una versione CT precedente con creazione rapida.

  Per ordinare CTs, utilizzate l'area Tutti i tipi di modifica nella vista a scheda o tabella. In entrambe le visualizzazioni, selezionate un CT, quindi fate clic su Crea RFC per aprire la pagina Esegui RFC. Se applicabile, accanto al pulsante Crea RFC viene visualizzata l'opzione Crea con una versione precedente.

- Scegli per categoria: seleziona una categoria, sottocategoria, articolo e operazione e la casella dei dettagli CT si apre con l'opzione Crea con una versione precedente, se applicabile. Fai clic su Crea RFC per aprire la pagina Esegui RFC.

3. Nella pagina Run RFC, apri l'area del nome CT per visualizzare la casella dei dettagli CT. È richiesto un Oggetto (questo campo viene compilato automaticamente se si sceglie il CT nella visualizzazione Sfoglia i tipi di modifica). Apri l'area di configurazione aggiuntiva per aggiungere informazioni sull'RFC.

   Nell'area di configurazione dell'esecuzione, utilizza gli elenchi a discesa disponibili o inserisci i valori per i parametri richiesti. Per configurare i parametri di esecuzione opzionali, aprite l'area di configurazione aggiuntiva.

4. Al termine, fate clic su Esegui. Se non sono presenti errori, viene visualizzata la pagina RFC creata correttamente con i dettagli RFC inviati e l'output iniziale di Run.

5. Apri l'area dei parametri di esecuzione per visualizzare le configurazioni inviate. Aggiorna la pagina per aggiornare lo stato di esecuzione RFC. Facoltativamente, annulla la RFC o creane una copia con le opzioni nella parte superiore della pagina.

Riavvio di uno stack con la CLI

Come funziona:

1. Usa Inline Create (immetti un `create-rfc` comando con tutti i parametri RFC e di esecuzione inclusi) o Template Create (crei due file JSON, uno per i parametri RFC e uno per i parametri di esecuzione) ed esegui il comando con i due file come input. `create-rfc` Entrambi i metodi sono descritti qui.
2. Invia il `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con l'ID RFC restituito.

   Monitora il comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Per verificare la versione del tipo di modifica, usa questo comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> È possibile utilizzare qualsiasi `CreateRfc` parametro con qualsiasi RFC, indipendentemente dal fatto che faccia parte o meno dello schema per il tipo di modifica. Ad esempio, per ricevere notifiche quando lo stato RFC cambia, aggiungi questa riga `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` alla parte dei parametri RFC della richiesta (non ai parametri di esecuzione). Per un elenco di tutti i CreateRfc parametri, consulta l'AMS Change Management API Reference.

CREAZIONE IN LINEA:

Esegui il comando create RFC con i parametri di esecuzione forniti in linea (evita le virgolette quando fornisci i parametri di esecuzione in linea), quindi invia l'ID RFC restituito. Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

```
aws amscm create-rfc --change-type-id "ct-02u0hoaa9grat" --change-type-version "1.0" --
title "Reboot My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CREAZIONE DEL MODELLO:

1. Esporta il modello RFC in un file nella cartella corrente. Questo esempio lo chiama RebootStackRfc .json. Si noti che, poiché esiste un solo parametro di esecuzione per arrestare (riavviare o avviare) un'istanza, il parametro di esecuzione può trovarsi nel file JSON dello schema stesso e non è necessario creare un file JSON con parametri di esecuzione separato.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopInstanceRfc.json
   ```

2. Modifica e salva il file.json. RebootStackRfc

   Le virgolette interne dell'estensione `ExecutionParameters` JSON devono essere eliminate con una barra rovesciata (\). Esempio:

   ```
   {
   ```

```
"ChangeTypeId":          "ct-02u0hoaa9grat",
"Title":                 "Reboot-My-EC2-RFC",
"TimeoutInMinutes":      60,
"ExecutionParameters":   "{
        \"StackId\":\"STACK_ID\"
    }"
}
```

3. Crea la RFC:

```
aws amscm create-rfc --cli-input-json file://RebootStackRfc.json
```

Nella risposta ricevi l'ID della nuova RFC e puoi utilizzarlo per inviare e monitorare la RFC. Finché non la invii, la RFC rimane nello stato di modifica e non si avvia.

Suggerimenti

Per informazioni su Application Load Balancers, consulta Application Load Balancers.

Stack di avvio

Avvio di uno stack con la console

Schermata di questo tipo di modifica nella console AMS:

Come funziona:

1. Vai alla pagina Crea RFC: nel riquadro di navigazione a sinistra della console AMS, fai clic RFCsper aprire la pagina di RFCs elenco, quindi fai clic su Crea RFC.
2. Scegli un tipo di modifica (CT) popolare nella visualizzazione predefinita Sfoglia i tipi di modifica o seleziona un CT nella visualizzazione Scegli per categoria.
   - Naviga per tipo di modifica: puoi fare clic su un CT popolare nell'area di creazione rapida per aprire immediatamente la pagina Run RFC. Nota che non puoi scegliere una versione CT precedente con creazione rapida.

     Per ordinare CTs, utilizzate l'area Tutti i tipi di modifica nella vista a scheda o tabella. In entrambe le visualizzazioni, selezionate un CT, quindi fate clic su Crea RFC per aprire la pagina Esegui RFC. Se applicabile, accanto al pulsante Crea RFC viene visualizzata l'opzione Crea con una versione precedente.

- Scegli per categoria: seleziona una categoria, sottocategoria, articolo e operazione e la casella dei dettagli CT si apre con l'opzione Crea con una versione precedente, se applicabile. Fai clic su Crea RFC per aprire la pagina Esegui RFC.

3. Nella pagina Run RFC, apri l'area del nome CT per visualizzare la casella dei dettagli CT. È richiesto un Oggetto (questo campo viene compilato automaticamente se si sceglie il CT nella visualizzazione Sfoglia i tipi di modifica). Apri l'area di configurazione aggiuntiva per aggiungere informazioni sull'RFC.

   Nell'area di configurazione dell'esecuzione, utilizza gli elenchi a discesa disponibili o inserisci i valori per i parametri richiesti. Per configurare i parametri di esecuzione opzionali, aprite l'area di configurazione aggiuntiva.
4. Al termine, fate clic su Esegui. Se non sono presenti errori, viene visualizzata la pagina RFC creata correttamente con i dettagli RFC inviati e l'output iniziale di Run.
5. Apri l'area dei parametri di esecuzione per visualizzare le configurazioni inviate. Aggiorna la pagina per aggiornare lo stato di esecuzione RFC. Facoltativamente, annulla la RFC o creane una copia con le opzioni nella parte superiore della pagina.

Avvio di uno stack con la CLI

Come funziona:

1. Utilizzate Inline Create (emettete un `create-rfc` comando con tutti i parametri RFC e di esecuzione inclusi) o Template Create (create due file JSON, uno per i parametri RFC e uno per i parametri di esecuzione) ed emettete il `create-rfc` comando con i due file come input. Entrambi i metodi sono descritti qui.
2. Invia il `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con l'ID RFC restituito.

   Monitora il comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Per verificare la versione del tipo di modifica, usa questo comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> È possibile utilizzare qualsiasi `CreateRfc` parametro con qualsiasi RFC, indipendentemente dal fatto che faccia parte o meno dello schema per il tipo di modifica. Ad esempio, per ricevere notifiche quando lo stato RFC cambia, aggiungi questa riga `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` alla parte dei parametri RFC della richiesta (non ai parametri di esecuzione). Per un elenco di tutti i CreateRfc parametri, consulta l'AMS Change Management API Reference.

CREAZIONE IN LINEA:

Esegui il comando create RFC con i parametri di esecuzione forniti in linea (evita le virgolette quando fornisci i parametri di esecuzione in linea), quindi invia l'ID RFC restituito. Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

```
aws amscm create-rfc --change-type-id "ct-1h5xgl9cr4bzy" --change-type-version "1.0" --
title "Start My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CREAZIONE DEL MODELLO:

1. Esporta il modello RFC in un file nella cartella corrente. Questo esempio lo chiama StartInstanceRfc .json. Si noti che, poiché esiste un solo parametro di esecuzione per avviare uno stack, il parametro di esecuzione può trovarsi nel file JSON dello schema stesso e non è necessario creare un file JSON dei parametri di esecuzione separato.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StartStackRfc.json
   ```

2. Modifica e salva il file.json. StartStackRfc Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

   ```
   {
   "ChangeTypeId":          "ct-1h5xgl9cr4bzy",
   "Title":                 "Start-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. Crea la RFC:

```
aws amscm create-rfc --cli-input-json file://StartStackRfc.json
```

Nella risposta ricevi l'ID della nuova RFC e puoi utilizzarlo per inviare e monitorare la RFC. Finché non la invii, la RFC rimane nello stato di modifica e non si avvia.

Suggerimenti

Per informazioni su Application Load Balancers, consulta Application Load Balancers.

Stop stack

Fermare uno stack con la console

Schermata di questo tipo di modifica nella console AMS:

Come funziona:

1. Vai alla pagina Crea RFC: nel riquadro di navigazione a sinistra della console AMS, fai clic RFCsper aprire la pagina di RFCs elenco, quindi fai clic su Crea RFC.
2. Scegli un tipo di modifica (CT) popolare nella visualizzazione predefinita Sfoglia i tipi di modifica o seleziona un CT nella visualizzazione Scegli per categoria.
   - Naviga per tipo di modifica: puoi fare clic su un CT popolare nell'area di creazione rapida per aprire immediatamente la pagina Run RFC. Nota che non puoi scegliere una versione CT precedente con creazione rapida.

     Per ordinare CTs, utilizzate l'area Tutti i tipi di modifica nella vista a scheda o tabella. In entrambe le visualizzazioni, selezionate un CT, quindi fate clic su Crea RFC per aprire la pagina Esegui RFC. Se applicabile, accanto al pulsante Crea RFC viene visualizzata l'opzione Crea con una versione precedente.
   - Scegli per categoria: seleziona una categoria, sottocategoria, articolo e operazione e la casella dei dettagli CT si apre con l'opzione Crea con una versione precedente, se applicabile. Fai clic su Crea RFC per aprire la pagina Esegui RFC.
3. Nella pagina Run RFC, apri l'area del nome CT per visualizzare la casella dei dettagli CT. È richiesto un Oggetto (questo campo viene compilato automaticamente se si sceglie il CT nella

visualizzazione Sfoglia i tipi di modifica). Apri l'area di configurazione aggiuntiva per aggiungere informazioni sull'RFC.

Nell'area di configurazione dell'esecuzione, utilizza gli elenchi a discesa disponibili o inserisci i valori per i parametri richiesti. Per configurare i parametri di esecuzione opzionali, aprite l'area di configurazione aggiuntiva.

4. Al termine, fate clic su Esegui. Se non sono presenti errori, viene visualizzata la pagina RFC creata correttamente con i dettagli RFC inviati e l'output iniziale di Run.
5. Apri l'area dei parametri di esecuzione per visualizzare le configurazioni inviate. Aggiorna la pagina per aggiornare lo stato di esecuzione RFC. Facoltativamente, annulla la RFC o creane una copia con le opzioni nella parte superiore della pagina.

Arresto di uno stack con la CLI

Come funziona:

1. Usa Inline Create (immetti un `create-rfc` comando con tutti i parametri RFC e di esecuzione inclusi) o Template Create (crei due file JSON, uno per i parametri RFC e uno per i parametri di esecuzione) ed esegui il `create-rfc` comando con i due file come input. Entrambi i metodi sono descritti qui.
2. Invia il `aws amscm submit-rfc --rfc-id` *`ID`* comando RFC: con l'ID RFC restituito.

   Monitora il comando RFC:. `aws amscm get-rfc --rfc-id` *`ID`*

Per verificare la versione del tipo di modifica, usa questo comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=CT_ID
```

> **Note**
>
> È possibile utilizzare qualsiasi `CreateRfc` parametro con qualsiasi RFC, indipendentemente dal fatto che faccia parte o meno dello schema per il tipo di modifica. Ad esempio, per ricevere notifiche quando lo stato RFC cambia, aggiungi questa riga `--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"` alla

parte dei parametri RFC della richiesta (non ai parametri di esecuzione). Per un elenco di tutti i CreateRfc parametri, consulta l'AMS Change Management API Reference.

CREAZIONE IN LINEA:

Esegui il comando create RFC con i parametri di esecuzione forniti in linea (evita le virgolette quando fornisci i parametri di esecuzione in linea), quindi invia l'ID RFC restituito. Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

```
aws amscm create-rfc --change-type-id "ct-3dgbnh6gpst4d" --change-type-version "1.0" --
title "Stop My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

CREAZIONE DEL MODELLO:

1. Esporta il modello RFC in un file nella cartella corrente. Questo esempio lo chiama StopStackRfc .json. Si noti che, poiché esiste un solo parametro di esecuzione per arrestare (riavviare o avviare) un'istanza, il parametro di esecuzione può trovarsi nel file JSON dello schema stesso e non è necessario creare un file JSON con parametri di esecuzione separato.

   ```
   aws amscm create-rfc --generate-cli-skeleton > StopStackRfc.json
   ```

2. Modifica e salva il file.json. StopStackRfc Ad esempio, puoi sostituire il contenuto con qualcosa del genere:

   ```
   {
   "ChangeTypeId":          "ct-3dgbnh6gpst4d",
   "Title":                 "Stop-My-EC2-RFC",
   "TimeoutInMinutes":      60,
   "ExecutionParameters":   "{
           \"StackId\":\"STACK_ID\"
       }"
   }
   ```

3. Crea la RFC:

   ```
   aws amscm create-rfc --cli-input-json file://StopInstanceRfc.json
   ```

   Nella risposta ricevi l'ID della nuova RFC e puoi utilizzarlo per inviare e monitorare la RFC. Finché non la invii, la RFC rimane nello stato di modifica e non si avvia.

Suggerimenti

Le istanze interrotte rimangono ferme a meno che non siano stati pianificati i riavvii utilizzando AMS Resource Scheduler.

Se necessario, consulta EC2 instance stack stop fail.

Esempi di accesso

Questi esempi mostrano come accedere a un'istanza tramite un bastione dopo aver ottenuto l'accesso tramite una RFC. Per i dettagli sulla concessione dell'accesso, consulta Richieste di accesso.

> **Note**
>
> Un' EC2 istanza creata tramite un gruppo Auto Scaling avrà un indirizzo IP che si accende e si chiude ciclicamente e sarà necessario utilizzare la EC2 console per trovare quell'indirizzo IP.

Dati richiesti:

- Nome o indirizzo IP descrittivo di Bastion DNS: utilizza un nome DNS descrittivo come descritto in Nomi bastioni compatibili con DNS o trova gli indirizzi IP di Bastion come descritto in. Individuazione degli indirizzi IP di Bastion
- Nome utente (ad esempio username@customerdomain.com) e password: credenziali per l'account.
- Indirizzo IP dello stack: puoi ottenerlo consultando la pagina Stacks della console AMS relativa allo stack a cui desideri accedere, quindi filtrando l'ID dello stack nella console del tuo account. EC2 Per una singola EC2 istanza, puoi anche utilizzare il comando AMS SKMS. Per il riferimento all'API AMS SKMS, consulta la scheda Report nella Console AWS Artifact. Per trovare l'ID dello stack, quindi per il riferimento all'API AMS SKMS, consulta la scheda Report nella Console AWS Artifact per trovare l'indirizzo IP dello stack.

Accedi all'indirizzo IP del bastione, SSH o RDP, a seconda dei casi, e accedi utilizzando una delle seguenti procedure.

Da computer Linux a istanza Linux

Usa SSH per connetterti al bastione SSH e poi all'istanza Linux.

MALZ

Per ulteriori informazioni sui nomi descrittivi dei bastioni, consulta DNS bastions.

Per connetterti all'istanza Linux, devi prima connetterti a un bastione SSH.

1. Apri una finestra di shell e inserisci:

```
ssh Domain_FQDN\\Username@SSH_bastion_name
    or SSH_bastion_IP
```

Avrebbe questo aspetto se il tuo dominio_FQDN è «corp.domain.com», il tuo numero di account è «123456789123", il tuo_dominio è «amazonaws.com», scegli bastion «4" e il tuo nome utente è" «: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.A123456789123.amazonaws.com
```

2. Accedi con le tue credenziali aziendali di Active Directory.
3. Quando viene visualizzato un prompt di Bash, accedi con SSH all'istanza, quindi inserisci:

```
ssh Domain_FQDN\\Username@Instance_IP
```

In alternativa, puoi usare il flag di accesso (-l):

```
ssh -l Domain_FQDN\\Username@Instance_IP
```

SALZ

Per ulteriori informazioni sui nomi amichevoli dei bastioni, consulta DNS bastions.

Per connetterti all'istanza Linux, devi prima connetterti a un bastione SSH.

1. Apri una finestra di shell e inserisci:

```
ssh DOMAIN_FQDN\\USERNAME@SSH_BASTION_name
```

```
    or SSH_BASTION_IP
```

Assomiglierebbe a questo se il tuo numero di account è 123456789123, scegli bastion 4 e il tuo nome utente è: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion1.A123456789123.amazonaws.com
```

2. Accedi con le tue credenziali aziendali di Active Directory.
3. Quando viene visualizzato un prompt di Bash, accedi con SSH all'istanza, quindi inserisci:

```
ssh DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

In alternativa, puoi usare il flag di accesso (-l):

```
ssh -l DOMAIN_FQDN\\USERNAME@INSTANCE_IP
```

Istanza da computer Linux a Windows

Usa un tunnel SSH e un client RDP per connetterti a un'istanza Windows dal tuo computer Linux.

MALZ

Questa procedura richiede un client Remote Desktop Connection per Linux; l'esempio utilizza Microsoft Remote Desktop (un client UNIX open source per la connessione a Windows Remote Desktop Services). Rdesktop è un'alternativa.

> **Note**
>
> Il modo in cui si accede alle istanze di Windows potrebbe cambiare in base al client desktop remoto utilizzato.

Per prima cosa stabilisci un tunnel SSH e poi accedi.

Per ulteriori informazioni sui nomi amichevoli dei bastioni, vedi. Nomi bastioni compatibili con DNS

Prima di iniziare:

- Richiedi l'accesso all'istanza a cui desideri connetterti; per informazioni, consulta Richieste di accesso.
- Scegli un nome DNS SSH intuitivo a cui connetterti; ad esempio:

```
sshbastion(1-4).Your_Domain
```

Assomiglierebbe a questo se il tuo dominio_FQDN è «corp.domain.com», il tuo dominio_dominio gestito da AMS è «amazonaws.com», scegli il bastion «4" e il tuo nome utente è" «: JoeSmith

```
ssh corp.domain.com\\JoeSmith sshbastion4.amazonaws.com
```

- Trova l'indirizzo IP dell'istanza a cui desideri connetterti; per informazioni, consulta Trovare l'ID o l'indirizzo IP di un'istanza.

1. Configura RDP su un tunnel SSH da un desktop Linux a un'istanza Windows. Per emettere il `ssh` comando con i valori corretti, ci sono un paio di modi per procedere:

   - Nella shell Linux, imposta le variabili, quindi inserisci il comando di connessione SSH:

   ```
   BASTION="sshbastion(1-4).Your_Domain""
   WINDOWS="Windows_Instance_Private_IP"
   AD="AD_Account_Number"
   USER="AD_Username"
   ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
   ```

   Ad esempio, se vengono utilizzati i seguenti valori:

   ```
   BASTION="sshbastion4.A123456789123.amazonaws.com"

   WINDOWS="172.16.3.254"

   AD="ACORP_example"

   USER="john.doe"
   ```

   - Aggiungere i valori delle variabili direttamente al `ssh` comando.

In entrambi i casi, questo è ciò che sarebbe la richiesta renderizzata (assumendo lo stesso insieme di valori variabili):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\\john.doe@myamsadomain.com
```

2. In entrambi i casi: apri il tuo client di desktop remoto, inserisci l'indirizzo e la porta di loopback, 127.0.0. 1:3389, quindi apri la connessione.

   Oppure, accedi all'istanza di Windows da una nuova shell desktop Linux. Se lo usi RDesktop, il comando è simile al seguente:

   ```
   rdesktop 127.0.0.1:3389
   ```

   Sul desktop Linux viene visualizzata una finestra del desktop remoto per l'istanza di Windows.

   > **Tip**
   >
   > Se la sessione di desktop remoto non si avvia, verifica che la connettività di rete all'istanza Windows dal bastione SSH sia consentita sulla porta 3389 della shell nel passaggio 1 (`private_ip_address_of_windows_instance`sostituiscila in modo appropriato):
   >
   > ```
   > nc private_ip_address_of_windows_instance 3389 -v –z
   > ```
   >
   > Successo:
   >
   > ```
   > nc 172.16.0.83 3389 -v -z
   >        Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
   >        netstat -anvp | grep 3389
   >        tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
   > ```

SALZ

Questa procedura per una landing zone con account singolo richiede un client Remote Desktop Connection per Linux; l'esempio utilizza Microsoft Remote Desktop (un client UNIX open source per la connessione a Windows Remote Desktop Services). Rdesktop è un'alternativa.

> **Note**
>
> Il modo in cui si accede alle istanze di Windows potrebbe cambiare in base al client desktop remoto utilizzato.

Per prima cosa stabilisci un tunnel SSH e poi accedi.

Per ulteriori informazioni sui nomi amichevoli dei bastioni, vedi. Nomi bastioni compatibili con DNS

Prima di iniziare:

- Richiedi l'accesso all'istanza a cui desideri connetterti; per informazioni, consulta Richieste di accesso.
- Scegli un nome DNS SSH intuitivo a cui connetterti; ad esempio:

  ```
  sshbastion(1-4).AAMSAccountNumber.amazonaws.com
  ```

  Assomiglierebbe a questo se il tuo numero di account è 123456789123 e scegli bastion 4:

  ```
  sshbastion4.A123456789123.amazonaws.com
  ```

- Trova l'indirizzo IP dell'istanza a cui desideri connetterti; per informazioni, consulta Finding an Instance ID o IP address.

1. Configura RDP su un tunnel SSH da un desktop Linux a un'istanza Windows. Per emettere il `ssh` comando con i valori corretti, ci sono un paio di modi per procedere:

   - Nella shell Linux, imposta le variabili, quindi inserisci il comando di connessione SSH:

     ```
     BASTION="sshbastion(1-4).AAMSAccountNumber.amazonaws.com"
     WINDOWS="WINDOWS_INSTANCE_PRIVATE_IP"
     AD="AD_ACCOUNT_NUMBER"
     ```

```
USER="AD_USERNAME"
ssh -L 3389:$WINDOWS:3389 A$AD\\\\$USER@$BASTION
```

Ad esempio, se vengono utilizzati i seguenti valori:

```
BASTION="sshbastion4.A123456789123.amazonaws.com"

WINDOWS="172.16.3.254"

AD="ACORP_example"

USER="john.doe"
```

- Aggiungere i valori delle variabili direttamente al `ssh` comando.

In entrambi i casi, questo è ciò che sarebbe la richiesta renderizzata (assumendo lo stesso insieme di valori variabili):

```
ssh -L 3389:172.16.3.254:3389 ACORP_example\\\
\john.doe@sshbastion4.A123456789123.amazonaws.com
```

2. In entrambi i casi: apri il tuo client di desktop remoto, inserisci l'indirizzo e la porta di loopback, 127.0.0. 1:3389, quindi apri la connessione.

   Oppure, accedi all'istanza di Windows da una nuova shell desktop Linux. Se lo usi RDesktop, il comando è simile al seguente:

   ```
   rdesktop 127.0.0.1:3389
   ```

   Sul desktop Linux viene visualizzata una finestra del desktop remoto per l'istanza di Windows.

   > **Tip**
   >
   > Se la sessione di desktop remoto non si avvia, verifica che la connettività di rete all'istanza Windows dal bastione SSH sia consentita sulla porta 3389 della shell nel passaggio 1 (`private_ip_address_of_windows_instance`sostituiscila in modo appropriato):
   >
   > ```
   > nc private_ip_address_of_windows_instance 3389 -v -z
   > ```

Successo:

```
nc 172.16.0.83 3389 -v -z
        Connection to 172.16.0.83 3389 port [tcp/ms-wbt-server] succeeded
        netstat -anvp | grep 3389
        tcp    0     0 172.16.0.253:48079 172.16.3.254:3389 ESTABLISHED
```

Istanza da computer Windows a Windows

Usa il client Windows Remote Desktop Connection per connetterti a un'istanza Windows dal tuo computer Windows.

MALZ

Per ulteriori informazioni sui nomi amichevoli dei bastioni, consultaNomi bastioni compatibili con DNS.

1. Apri il programma Remote Desktop Connection, un programma Windows standard, e inserisci il nome DNS descrittivo del bastione di Windows nel campo hostname.

2. Scegli Connetti. La Remote Desktop Connection tenta una connessione RDP al bastione.

   In caso di successo, si apre una finestra di dialogo con le credenziali. Per accedere, utilizzate le credenziali aziendali di Active Directory, come fareste con l'istanza di Windows.

3. Apri il programma Remote Desktop Connection sul bastione e inserisci l'indirizzo IP dell'istanza di Windows a cui desideri connetterti (ad esempio, 10.0.0.100), quindi scegli Connect. Le credenziali aziendali di Active Directory sono nuovamente necessarie prima di connettersi all'istanza di Windows.

SALZ

Per ulteriori informazioni sui nomi amichevoli dei bastioni, consulta. Nomi bastioni compatibili con DNS

1. Apri il programma Remote Desktop Connection, un programma Windows standard, e inserisci il nome DNS descrittivo del bastione di Windows nel campo hostname, ad esempio`rdpbastion`*`(1-4)`*`.A`*`AMSAccountNumber`*`.amazonaws.com`, che avrebbe questo aspetto se il tuo numero di account è 123456789123 e scegli bastion 4,. `rdpbastion4.A123456789123.amazonaws.com`

2. Scegli Connetti. La Remote Desktop Connection tenta una connessione RDP al bastione.

   In caso di successo, si apre una finestra di dialogo con le credenziali. Per accedere, utilizzate le credenziali aziendali di Active Directory, come fareste con l'istanza di Windows.

3. Apri il programma Remote Desktop Connection sul bastione e inserisci l'indirizzo IP dell'istanza di Windows a cui desideri connetterti (ad esempio, 10.0.0.100), quindi scegli Connect. Le credenziali aziendali di Active Directory sono nuovamente necessarie prima di connettersi all'istanza di Windows.

Istanza da computer Windows a Linux

Per eseguire l'RDP verso un bastione SSH da un ambiente Windows, segui questi passaggi.

MALZ

Prima di iniziare:

- Richiedi l'accesso all'istanza a cui desideri connetterti; per informazioni, consulta Richieste di accesso.
- Scegli un nome DNS SSH intuitivo a cui connetterti; ad esempio:

  ```
  sshbastion(1-4).YOUR_DOMAIN
  ```

  Assomiglierebbe a questo se YOUR_DOMAIN è «myamsaddomain.com» e scegli «bastion 4»:

  ```
  sshbastion4.myamsaddomain.com
  ```

- Trova l'indirizzo IP dell'istanza a cui desideri connetterti; per informazioni, consulta Finding an Instance ID o IP address.

Per connetterti all'istanza Linux dal tuo computer Windows, devi prima connetterti a un bastione SSH.

Usa il client nativo di Windows OpenSSH o installa PuTTY sul tuo computer locale. Per ulteriori informazioni su OpenSSH, consulta OpenSSH in Windows.

1. Usa Windows nativo o apri PuTTY e inserisci il nome host del bastione SSH o l'indirizzo IP del bastione SSH. Ad esempio, 10.65.2.214 (22 è la porta utilizzata per SSH; sarà impostata di default).
2. OpenSSH o PuTTY tenta una connessione SSH al bastione e apre una finestra di shell.
3. Utilizzate le vostre credenziali aziendali di Active Directory come fareste con gli host RDP per ottenere l'accesso.
4. Quando viene visualizzato un prompt di Bash, inserisci SSH nell'istanza. Inserisci:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

SALZ

Prima di iniziare:

- Richiedi l'accesso all'istanza a cui desideri connetterti; per informazioni, consulta Richieste di accesso.
- Scegli un nome DNS SSH intuitivo a cui connetterti; ad esempio:

```
sshbastion(1-4).AAMSAccountNumber.amazonaws.com
```

Assomiglierebbe a questo se il tuo numero di account è 123456789123 e scegli bastion 4:

```
sshbastion4.A123456789123.amazonaws.com
```

- Trova l'indirizzo IP dell'istanza a cui desideri connetterti; per informazioni, consulta Trovare l'ID o l'indirizzo IP di un'istanza.

Per connetterti all'istanza Linux dal tuo computer Windows, devi prima connetterti a un bastione SSH.

Usa il client nativo di Windows OpenSSH o installa PuTTY sul tuo computer locale. Per ulteriori informazioni su OpenSSH, consulta OpenSSH in Windows.

1. Usa Windows nativo o apri PuTTY e inserisci il nome host del bastione SSH o l'indirizzo IP del bastione SSH. Ad esempio, 10.65.2.214 (22 è la porta utilizzata per SSH; sarà impostata di default).
2. OpenSSH o PuTTY tenta una connessione SSH al bastione e apre una finestra di shell.
3. Utilizzate le vostre credenziali aziendali di Active Directory come fareste con gli host RDP per ottenere l'accesso.
4. Quando viene visualizzato un prompt di Bash, inserisci SSH nell'istanza. Inserisci:

```
ssh DOMAIN_FQDN\USERNAME@INSTANCE_IP
```

Segnalazione di un incidente

Usa la console AMS per segnalare un incidente. È importante creare un nuovo incidente per ogni nuovo problema o domanda. Quando si aprono casi relativi a vecchie richieste, è utile includere il numero del caso correlato in modo da poter fare riferimento alla corrispondenza precedente.

> **Note**
>
> Se la corrispondenza del caso si discosta dal numero originale, un operatore AMS potrebbe chiederti di segnalare un nuovo incidente.

Per segnalare un incidente utilizzando la console AMS:

1. Dalla barra di navigazione a sinistra, scegli Incidenti

   Si apre l'elenco degli Incidenti:

   Se l'elenco degli incidenti è vuoto, l'opzione Cancella filtro reimposta lo stato del filtro su Qualsiasi.

Se sai di voler usare il telefono o la chat, fai clic su Crea incidente in Support Center per aprire la pagina Crea incidente nella console di Support Center, compilata automaticamente con il tipo di servizio AMS.

> **Important**
>
> - Le telefonate iniziate con Supporto vengono registrate per migliorare la risposta. Se la chiamata si interrompe, è necessario richiamare tramite la custodia del Support Center, non AWS è disponibile alcun meccanismo per richiamarti.
> - L'assistenza telefonica e via chat è progettata per risolvere i casi di assistenza, gli incidenti e le richieste di assistenza, non per problemi di RFC o di sicurezza.
> - Per problemi RFC, utilizza l'opzione di corrispondenza nella pagina dei dettagli RFC pertinente, per contattare un tecnico AMS.
> - Per problemi di sicurezza, crea un caso di supporto ad alta priorità (P1 o P2). La funzione di chat dal vivo non è destinata agli eventi di sicurezza.

2. Se desideri trovare un incidente esistente, seleziona un filtro relativo allo stato dell'incidente nell'elenco a discesa.

	• Tutti gli incidenti non ancora risolti. • Un nuovo incidente non ancora assegnato. • Un incidente che è stato assegnato. • Un incidente che hai riaperto. • Un incidente assegnato e complicato. • Incidenti che richiedono il tuo feedback prima della fase successiva. • Incidenti per i quali hai inviato informazioni di recente. • Un incidente che si è concluso. • Tutti gli incidenti dell'account.

3. Scegli Create (Crea).

   Viene visualizzata la pagina Crea un incidente:

4. Seleziona una priorità:

   - Bassa: le funzioni non critiche del servizio o dell'applicazione aziendale relative alle risorse AWS/AMS ne risentono.
   - Medio: un servizio o un'applicazione aziendale relativi alle risorse AWS/AMS subisce un impatto moderato e funziona in uno stato degradato.
   - Alto: la tua attività ne risente in modo significativo. Le funzioni critiche dell'applicazione relative alle risorse AWS/AMS non sono disponibili. Riservato alle interruzioni più critiche che interessano i sistemi di produzione.

5. Seleziona una categoria.

   > **Note**
   >
   > Se intendi testare la funzionalità dell'incidente, aggiungi il flag no-action (AMSTestNoOpsActionRequired) al titolo dell'incidente.

6. Inserisci le informazioni per:

   - Oggetto: un titolo descrittivo per il rapporto sull'incidente.
   - Email CC: un elenco di indirizzi e-mail per le persone che desideri informare sulla segnalazione e sulla risoluzione dell'incidente.
   - Dettagli: una descrizione completa dell'incidente, dei sistemi interessati e dell'esito previsto della risoluzione. Rispondi alle domande preimpostate o eliminale e inserisci le informazioni pertinenti.

   Per aggiungere un allegato, scegliete Aggiungi allegato, individuate l'allegato desiderato e fate clic su Apri. Per eliminare l'allegato, fate clic sull'icona Elimina:

7. Seleziona Invia.

   Viene visualizzata una pagina dei dettagli con informazioni sull'incidente, ad esempio Tipo, Oggetto, Creato, ID e Stato, e un'area di corrispondenza che include la descrizione della richiesta creata.

Fai clic su Rispondi per aprire un'area di corrispondenza e fornire ulteriori dettagli o aggiornamenti sullo stato.

Fai clic su Chiudi caso quando l'incidente è stato risolto.

Fai clic su Carica altro se la corrispondenza è superiore a quella contenuta in una pagina.

Non dimenticare di valutare la comunicazione!

L'incidente viene visualizzato nella pagina dell'elenco degli incidenti.

Creazione di una richiesta di assistenza

Per creare una richiesta di servizio utilizzando la console AWS Managed Services (AMS):

1. Dalla barra di navigazione a sinistra, scegli Richieste di assistenza.

   Si apre l'elenco delle richieste di assistenza.

   Se l'elenco delle richieste di assistenza è vuoto, l'opzione Cancella filtro reimposta lo stato del filtro su Qualsiasi.

   Se sai di voler usare il telefono o la chat, fai clic su Crea richiesta di servizio in Support Center per aprire la pagina Crea richiesta di servizio nella console di Support Center, compilata automaticamente con il tipo di servizio AMS.

   > **Note**
   >
   > Le chiamate telefoniche avviate con il Supporto centro vengono registrate, per migliorare la risposta. Se la chiamata si interrompe, è necessario richiamare tramite la custodia del Support Center, non AWS è disponibile alcun meccanismo per richiamarti.

> **Important**
>
> L'assistenza telefonica e via chat è progettata per aiutare con casi di supporto, incidenti e richieste di assistenza. Per problemi relativi alla RFC, utilizza l'opzione di corrispondenza nella pagina dei dettagli RFC pertinente, per contattare un tecnico AMS.

2. Se desideri trovare una richiesta di servizio esistente, seleziona un filtro di stato della richiesta di servizio nell'elenco a discesa.

	• Tutte le richieste di assistenza non ancora risolte. • Una nuova richiesta di servizio non ancora assegnata. • Una richiesta di servizio che è stata assegnata. • Una richiesta di servizio che hai riaperto. • Una richiesta di assistenza assegnata e complicata. • Richieste di assistenza che richiedono il feedback dell'utente prima della fase successiva. • Richieste di assistenza per le quali hai inviato informazioni di recente. • Una richiesta di servizio conclusa. • Tutte le richieste di assistenza nell'account.

3. Scegli Create (Crea).

   Viene visualizzata la pagina Crea una richiesta di assistenza.

4. Seleziona una categoria.

> **Note**
>
> Se intendi testare la funzionalità di richiesta di assistenza, aggiungi il flag no-action,`AMSTestNoOpsActionRequired`. al titolo della richiesta di servizio.

5. Inserisci le informazioni per:

   - Oggetto: viene creato un collegamento ai dettagli della richiesta di assistenza nella pagina dell'elenco.
   - Email CC: queste e-mail ricevono corrispondenza in aggiunta ai contatti e-mail predefiniti.
   - Dettagli: Fornisci qui quante più informazioni possibili.

   Per aggiungere un allegato, scegliete Aggiungi allegato, individuate l'allegato desiderato e fate clic su Apri. Per eliminare l'allegato, fate clic sull'icona Elimina:

6. Seleziona Invia.

   Viene visualizzata una pagina dei dettagli con informazioni sulla richiesta di servizio, ad esempio Tipo, Oggetto, Creato, ID e Stato, e un'area di corrispondenza che include la descrizione della richiesta creata.

   Inoltre, la richiesta di assistenza viene visualizzata nella pagina dell'elenco delle richieste di assistenza. Usala quando ricevi un avviso ma non hai ancora ricevuto alcuna risposta da AMS.

   Fai clic su Rispondi per aprire un'area di corrispondenza e fornire ulteriori dettagli o aggiornamenti sullo stato.

   Fai clic su Risolvi caso quando la richiesta di assistenza è stata risolta.

   Fai clic su Carica altro per visualizzare altre corrispondenze che non rientrano nella pagina iniziale.

   Non dimenticare di valutare la comunicazione!

Per le domande relative alla fatturazione, utilizza l'altra categoria nella console AMS, l'`ChangeTypeId ct-1e1xtak34nx76`API AMS CM o `IssueType=AMS` l'API AWS Support.

Fasi successive all'onboarding

Ora che hai attivato un account AMS, ti consigliamo di leggere altra documentazione AMS. Consulta questi documenti:

- I tutorial per l'utilizzo dello stack HA Two-Tier CT per creare uno stack perfettamente funzionante, inoltre, forniscono un' WordPress esperienza AMS completa.
- Guida per l'utente AMS: la guida per l'utente AMS descrive le funzionalità di AMS, elenca i termini chiave, le operazioni e le interfacce e fornisce una panoramica di una tipica architettura di infrastruttura gestita AMS. Inoltre, vengono forniti i dettagli sulla gestione degli accessi e le impostazioni predefinite di AMS. Vengono inoltre fornite descrizioni dettagliate su come utilizzare il sistema di gestione delle modifiche AMS e vengono fornite diverse procedure dettagliate. Vengono descritti anche concetti di gestione aggiuntivi.
- Riferimento all'API AMS: questo riferimento API fornisce descrizioni di tutte le chiamate API, incluse richieste, risposte ed esempi.
- Guida all'applicazione AMS: la Guida all'applicazione AMS descrive diverse opzioni e metodi per la distribuzione e la manutenzione delle applicazioni in AMS.

Tutorial

I seguenti tutorial descrivono in dettaglio i passaggi per creare uno stack a due livelli con il CT High Availability (advanced) (ct-06mjngx5flwto), utilizzando la CLI e utilizzando la console. Viene fornito un tutorial per la distribuzione di un gruppo Linux Auto Scaling (ASG) e per la distribuzione di un ASG Windows.

Le descrizioni di tutte le opzioni CT, incluse ChangeTypeId , sono disponibili nell'AMS Change Type Reference.

Tutorial CLI: Stack a due livelli ad alta disponibilità (Linux/RHEL)

Questa sezione descrive come implementare uno stack a due livelli ad alta disponibilità (HA) in un ambiente AMS utilizzando l'AMS CLI.

> **Note**
>
> Questa procedura dettagliata di implementazione è stata testata in ambienti AMZN Linux e RHEL.

Riepilogo delle attività e dei requisiti richiesti: RFCs

1. Crea un'infrastruttura (stack HA a due livelli)
2. Crea un bucket S3 per le applicazioni CodeDeploy
3. Crea il pacchetto di WordPress applicazioni e caricalo nel bucket S3
4. Distribuisci l'applicazione con CodeDeploy
5. Accedi al WordPress sito e accedi per convalidare la distribuzione

Prima di iniziare

The Deployment | Advanced Stack Components | High Availability Two Tier Stack Advanced | Create CT crea un gruppo Auto Scaling, un load balancer, un database e CodeDeploy un nome di applicazione e un gruppo di implementazione (con lo stesso nome assegnato all'applicazione). Per informazioni su CodeDeploy , consulta What is? CodeDeploy

Questa procedura dettagliata utilizza un RFC High Availability Two-Tier Stack (Advanced) che include UserData e descrive anche come creare un WordPress pacchetto da distribuire. CodeDeploy

L'esempio `UserData` illustrato nell'esempio ottiene i metadati dell'istanza, come l'ID dell'istanza, la regione e così via, dall'interno di un'istanza in esecuzione interrogando il servizio di metadati dell'istanza disponibile all'indirizzo http://169.254.169.254/latest/meta-data/. EC2 Questa riga dello script dei dati utente:`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, recupera il nome della zona di disponibilità dal servizio di metadati nella variabile $REGION per le nostre regioni supportate e lo utilizza per completare l'URL per il bucket S3 in cui viene scaricato l'agente. CodeDeploy L'IP 169.254.169.254 è instradabile solo all'interno del VPC (tutti possono interrogare il servizio). VPCs Per informazioni sul servizio, consulta Metadati dell'istanza e dati utente. Nota anche che gli script immessi come UserData vengono eseguiti come utente «root» e non è necessario utilizzare il comando «sudo».

Questa procedura dettagliata lascia i seguenti parametri al valore predefinito (mostrato):

- Gruppo Auto Scaling:. `Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2, ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`
- Load Balancer:. `HealthCheckInterval=30, HealthCheckTimeout=5`
- Banca dati:`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.
- Applicazione:`DeploymentConfigName=CodeDeployDefault.OneAtATime`.
- Secchio S3:. `AccessControl=Private`

IMPOSTAZIONI AGGIUNTIVE:

`RequestedStartTime`e `RequestedEndTime` se desideri pianificare la tua RFC: puoi usare Time.is per determinare l'ora UTC corretta. Gli esempi forniti devono essere modificati in modo appropriato. Una RFC non può procedere se è trascorsa l'ora di inizio. In alternativa, puoi lasciare questi valori disattivati per creare un RFC ASAP che venga eseguito non appena vengono approvate.

> **Note**
>
> Ci sono molti parametri che potreste scegliere di impostare in modo diverso da quelli mostrati. I valori dei parametri mostrati nell'esempio sono stati testati ma potrebbero non essere adatti a te.

Crea l'infrastruttura

La raccolta dei seguenti dati prima di iniziare velocizzerà la distribuzione.

I DATI RICHIESTI HANNO UNO STACK:

- AutoScalingGroup:
  - `UserData`: Questo valore è fornito in questo tutorial. Include comandi per configurare la risorsa CodeDeploy e avviare l' CodeDeploy agente.
  - `AMI-ID`: Questo valore determina il tipo di EC2 istanze che verrà avviato dal gruppo Auto Scaling (ASG). Assicurati di selezionare nel tuo account un'AMI che inizi con «cliente-» e sia del sistema operativo che desideri. Trova AMI IDs con il riferimento all'API Per l'AMS SKMS, consulta la scheda Report nella Console AWS Artifact. operation (CLI: list-amis) o nella pagina dei dettagli della console AMS ->. VPCs VPCs Questa procedura dettagliata è destinata alla ASGs configurazione per l'utilizzo di un'AMI Linux.
- Database:
  - Questi parametri, `DBEngineEngineVersion`, `LicenseModel` devono essere impostati in base alla situazione, sebbene i valori mostrati nell'esempio siano stati testati.
  - Questi parametri,`RDSSubnetIds`, `DBNameMasterUsername`, e `MasterUserPassword` sono necessari per la distribuzione del pacchetto di applicazioni. Per gli RDSSubnet ID, utilizzate due sottoreti private.
- LoadBalancer:
  - Questi parametri, `DBEngineEngineVersion`, `LicenseModel` devono essere impostati in base alla situazione, sebbene i valori mostrati nell'esempio siano stati testati.
  - `ELBSubnetIds`: utilizza due sottoreti pubbliche.
- Applicazione: il `ApplicationName` valore imposta il nome dell' CodeDeploy applicazione e il nome del gruppo CodeDeploy di distribuzione. Lo usi per distribuire la tua applicazione. Deve essere unico nell'account. Per verificare la presenza di CodeDeploy nomi nel tuo account, consulta la CodeDeploy Console. L'esempio utilizza "WordPress" ma, se intendi utilizzare quel valore, assicurati che non sia già in uso.

Questa procedura utilizza lo stack a due livelli ad alta disponibilità (avanzato) CT (ct-06mjngx5flwto) e lo storage CT Create S3 (ct-1a68ck03fn98r). Dal tuo account autenticato, segui questi passaggi nella riga di comando.

1. Avvia lo stack di infrastruttura.

   a. Invia lo schema JSON dei parametri di esecuzione per lo stack CT a due livelli HA in un file nella cartella corrente denominata .json. CreateStackParams

```
aws amscm get-change-type-version --change-type-id "ct-06mjngx5flwto"
 --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
 CreateStackParams.json
```

b. Modifica lo schema. Sostituire *variables* il file appropriato. Ad esempio, utilizzate il sistema operativo desiderato per EC2 le istanze che l'ASG creerà. Registratele `ApplicationName` mentre le utilizzerete in seguito per distribuire l'applicazione. Tieni presente che puoi aggiungere fino a 50 tag.

```
{
"Description":      "HA two tier stack for WordPress",
"Name":             "WordPressStack",
"TimeoutInMinutes":  360,
"Tags": [
        {
            "Key": "ApplicationName",
            "Value": "WordPress"
        }
    ],
"AutoScalingGroup": {
            "AmiId":    "AMI-ID",
            "UserData": "#!/bin/bash \n
            REGION=$(curl 169.254.169.254/latest/meta-data/placement/
availability-zone/ | sed 's/[a-z]$//') \n
            yum -y install ruby httpd \n
            chkconfig httpd on \n
            service httpd start \n
            touch /var/www/html/status \n
            cd /tmp \n
            curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/
install \n
            chmod +x ./install \n
            ./install auto \n
            chkconfig codedeploy-agent on \n
            service codedeploy-agent start"
    },
    "LoadBalancer": {
        "Public":               true,
        "HealthCheckTarget":    "HTTP:80/status"
    },
    "Database":     {
        "DBEngine":             "MySQL",
```

```
        "DBName":               "wordpress",
        "EngineVersion":        "8.0.16 ",
        "LicenseModel":         "general-public-license",
        "MasterUsername":       "admin",
        "MasterUserPassword":   "p4ssw0rd"
    },
    "Application":  {
    "ApplicationName":  "WordPress"
        }
}
```

c. Esporta il modello CreateRfc JSON in un file nella cartella corrente denominata CreateStackRfc .json:

```
aws amscm create-rfc --generate-cli-skeleton > CreateStackRfc.json
```

d. Modifica il modello RFC come segue e salvalo, puoi eliminare e sostituire i contenuti. Tieni presente che `RequestedStartTime` ora `RequestedEndTime` sono facoltativi; la loro esclusione crea un RFC ASAP che viene eseguito non appena viene approvato (cosa che di solito avviene automaticamente). Per inviare una RFC pianificata, aggiungi questi valori.

```
{
"ChangeTypeVersion":    "3.0",
"ChangeTypeId":         "ct-06mjngx5flwto",
"Title":                "HA-Stack-For-WP-RFC"
}
```

e. Crea la RFC, specificando il CreateStackRfc file.json e il file dei parametri di esecuzione .json: CreateStackParams

```
aws amscm create-rfc --cli-input-json file://CreateStackRfc.json --execution-
parameters file://CreateStackParams.json
```

Riceverai l'ID RFC nella risposta. Salva l'ID per i passaggi successivi.

f. Invia la RFC:

```
aws amscm submit-rfc --rfc-id  RFC_ID
```

Se la RFC ha esito positivo, non riceverai alcun output.

g. Per verificare lo stato della RFC, esegui

```
aws amscm get-rfc --rfc-id RFC_ID
```

Prendi nota dell'ID RFC.

2. Avvia un bucket S3

   La raccolta dei seguenti dati prima di iniziare velocizzerà la distribuzione.

   BUCKET S3 DI DATI RICHIESTO:

   - `VPC-ID`: questo valore determina dove sarà il tuo S3 Bucket. Usa lo stesso ID VPC che hai usato in precedenza.
   - `BucketName`: Questo valore imposta il nome del bucket S3, lo usi per caricare il pacchetto dell'applicazione. Deve essere univoco in tutta l'area dell'account e non può includere lettere maiuscole. L'inclusione dell'ID dell'account come parte di non BucketName è un requisito, ma semplifica l'identificazione del bucket in un secondo momento. Per vedere quali nomi di bucket S3 esistono nell'account, accedi alla console Amazon S3 del tuo account.

   a. Invia lo schema JSON dei parametri di esecuzione per lo storage S3, crea CT in un file JSON denominato CreateS3 .json. StoreParams

   ```
   aws amscm get-change-type-version --change-type-id "ct-1a68ck03fn98r"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    CreateS3StoreParams.json
   ```

   b. Modifica lo schema come segue, puoi eliminare e sostituire i contenuti. Sostituisci *VPC_ID* in modo appropriato. I valori dell'esempio sono stati testati, ma potrebbero non essere adatti a te.

   > **Tip**
   >
   > `BucketName`Devono essere univoci in tutta l'area dell'account e non possono includere lettere maiuscole. L'inclusione dell'ID dell'account come parte di non BucketName è un requisito, ma semplifica l'identificazione del bucket in un secondo momento. Per vedere quali nomi di bucket S3 esistono nell'account, accedi alla console Amazon S3 del tuo account.

```
{
"Description":      "S3BucketForWordPressBundle",
"VpcId":            "VPC_ID",
"StackTemplateId":  "stm-s2b72beb000000000",
"Name":             "S3BucketForWP",
"TimeoutInMinutes":  60,
"Parameters":   {
    "AccessControl":    "Private",
    "BucketName":       "ACCOUNT_ID-BUCKET_NAME"
    }
}
```

c. Esporta il modello JSON in un file, nella cartella corrente, denominato CreateS3 .json: CreateRfc StoreRfc

```
aws amscm create-rfc --generate-cli-skeleton > CreateS3StoreRfc.json
```

d. Modifica e salva il file CreateS3 StoreRfc .json, puoi eliminare e sostituire il contenuto. Tieni presente che `RequestedStartTime` ora `RequestedEndTime` sono facoltativi; la loro esclusione crea un RFC ASAP che viene eseguito non appena viene approvato (cosa che di solito avviene automaticamente). Per inviare una RFC pianificata, aggiungi questi valori.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-1a68ck03fn98r",
"Title":                "S3-Stack-For-WP-RFC"
}
```

e. Crea la RFC, specificando il file CreateS3 .json e il file dei parametri di esecuzione CreateS3 StoreRfc .json: StoreParams

```
aws amscm create-rfc --cli-input-json file://CreateS3StoreRfc.json  --
execution-parameters file://CreateS3StoreParams.json
```

Riceverai il nuovo RFC nella risposta. RfcId Salva l'ID per i passaggi successivi.

f. Invia la RFC:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Se la RFC ha esito positivo, non riceverai alcun output.

g. Per verificare lo stato della RFC, esegui

```
aws amscm get-rfc --rfc-id RFC_ID
```

Crea, carica e distribuisci l'applicazione

Innanzitutto, create un pacchetto di WordPress applicazioni, quindi utilizzate il CodeDeploy CTs per creare e distribuire l'applicazione.

1. Scarica WordPress, estrai i file e crea un file. cartella /scripts.

   Comando Linux:

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: incolla `https://github.com/WordPress/WordPress/archive/master.zip` in una finestra del browser e scarica il file zip.

   Crea una directory temporanea in cui assemblare il pacchetto.

   Linux:

   ```
   mkdir /tmp/WordPress
   ```

   Windows: crea una cartella "WordPress", utilizzerai il percorso della directory in seguito.

2. Estrai il WordPress codice sorgente nella cartella WordPress "" e crea un file. cartella /scripts.

   Linux:

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

   Windows: vai alla cartella "WordPress" che hai creato e lì crea una cartella «scripts».

Se utilizzate un ambiente Windows, assicuratevi di impostare il tipo di interruzione per i file di script su Unix (LF). In Notepad ++, questa è un'opzione in basso a destra della finestra.

3. Crea il file CodeDeploy appspec.yml, nella WordPress directory (se copi l'esempio, controlla l'indentazione, ogni spazio conta). IMPORTANTE: assicurati che il percorso «sorgente» sia corretto per copiare WordPress i file (in questo caso, nella tua WordPress directory) nella destinazione prevista (/). var/www/html/WordPress Nell'esempio, il file appspec.yml si trova nella directory con WordPress i file, quindi è necessario solo «/». Inoltre, anche se hai usato un'AMI RHEL per il tuo gruppo Auto Scaling, lascia la riga «os: linux» così com'è. Esempio di file appspec.yml:

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. Crea script di file bash in. WordPress cartella /scripts.

   Innanzitutto, crea `config_wordpress.sh` con il seguente contenuto (se preferisci, puoi modificare direttamente il file wp-config.php).

> **Note**
>
> Sostituisci *DBName* con il valore fornito nell'HA Stack RFC (ad esempio,`wordpress`).
> Sostituisci *DB_MasterUsername* con il `MasterUsername` valore fornito nell'HA Stack RFC (ad esempio,). `admin`
> Sostituisci *DB_MasterUserPassword* con il `MasterUserPassword` valore fornito nell'HA Stack RFC (ad esempio,). `p4ssw0rd`
> Sostituire *DB_ENDPOINT* con il nome DNS dell'endpoint negli output di esecuzione di HA Stack RFC (ad esempio,). `srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com` Puoi trovarlo con l'GetRfcoperazione (CLI: get-rfc --rfc-id RFC_ID) o nella pagina dei dettagli RFC della console AMS per l'HA Stack RFC che hai inviato in precedenza.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-
config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. `install_dependencies.sh`Nella stessa directory, crea con il seguente contenuto:

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS viene installato come parte dei dati utente al momento del lancio per consentire il funzionamento dei controlli sanitari sin dall'inizio.

6. Nella stessa directory, crea `start_server.sh` con il seguente contenuto:

- Per le istanze Amazon Linux, usa questo:

```
#!/bin/bash
service httpd start
```

- Per le istanze RHEL, usa questo (i comandi aggiuntivi sono politiche che consentono a SELINUX di accettare): WordPress

```
#!/bin/bash
setsebool -P  httpd_can_network_connect_db 1
setsebool -P  httpd_can_network_connect 1
chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
restorecon -Rv /var/www/html
service httpd start
```

7. Nella stessa directory create `stop_server.sh` con il seguente contenuto:

```
#!/bin/bash
service httpd stop
```

8. Crea il pacchetto zip.

   Linux:

```
$ cd /tmp/WordPress
$ zip -r wordpress.zip .
```

   Windows: vai alla cartella WordPress "" e seleziona tutti i file e crea un file zip, assicurati di chiamarlo wordpress.zip.

1. Carica il pacchetto dell'applicazione nel bucket S3.

   Il pacchetto deve essere disponibile per continuare a distribuire lo stack.

   Hai automaticamente accesso a qualsiasi istanza di bucket S3 che crei. Puoi accedervi tramite i tuoi bastioni o tramite la console S3 e caricare il WordPress pacchetto drag-and-drop o sfogliare e selezionare il file zip.

   Puoi anche usare il seguente comando in una finestra di shell; assicurati di avere il percorso corretto del file zip:

```
aws s3 cp wordpress.zip s3://BUCKET_NAME/
```

2. Distribuite il pacchetto di WordPress applicazioni.

   La raccolta dei seguenti dati prima di iniziare velocizzerà la distribuzione.

   DATI RICHIESTI:

   - `VPC-ID`: Questo valore determina dove si troverà il tuo S3 Bucket. Usa lo stesso ID VPC che hai usato in precedenza.
   - `CodeDeployApplicationNameeCodeDeployApplicationName`: il `ApplicationName` valore utilizzato nell'RFC HA 2-Tier Stack imposta e il. CodeDeployApplicationName CodeDeployDeploymentGroupName L'esempio utilizza "WordPress" ma potresti aver usato un valore diverso.
   - `S3Location`: Per`S3Bucket`, usa quello `BucketName` che hai creato in precedenza. I `S3BundleType` e `S3Key` provengono dal pacchetto che hai inserito nel tuo negozio S3.

   a. Emetti lo schema JSON dei parametri di esecuzione per l' CodeDeploy applicazione, distribuisci CT in un file JSON denominato Deploy Params.json. CDApp

   ```
   aws amscm get-change-type-version --change-type-id "ct-2edc3sd1sqmrb"
    --query "ChangeTypeVersion.ExecutionInputSchema" --output text >
    DeployCDAppParams.json
   ```

   b. Modifica lo schema come segue e salvalo come, puoi eliminare e sostituire i contenuti.

   ```
   {
   "Description":                        "DeployWPCDApp",
   "VpcId":                              "VPC_ID",
   "Name":                               "WordPressCDAppDeploy",
   "TimeoutInMinutes":                   60,
   "Parameters":   {
       "CodeDeployApplicationName":                "WordPress",
       "CodeDeployDeploymentGroupName":            "WordPress",
       "CodeDeployIgnoreApplicationStopFailures":   false,
       "CodeDeployRevision": {
         "RevisionType": "S3",
         "S3Location": {
           "S3Bucket":     "BUCKET_NAME",
   ```

```
        "S3BundleType": "zip",
        "S3Key":        "wordpress.zip" }
        }
    }
}
```

c. Esporta il modello JSON CreateRfc per in un file, nella cartella corrente, denominato Deploy CDApp RFC.json:

```
aws amscm create-rfc --generate-cli-skeleton > DeployCDAppRfc.json
```

d. Modifica e salva il file Deploy CDApp RFC.json, puoi eliminare e sostituire il contenuto. Tieni presente che `RequestedStartTime` ora `RequestedEndTime` sono facoltativi; la loro esclusione crea un RFC ASAP che viene eseguito non appena viene approvato (cosa che di solito avviene automaticamente). Per inviare una RFC pianificata, aggiungi questi valori.

```
{
"ChangeTypeVersion":    "1.0",
"ChangeTypeId":         "ct-2edc3sd1sqmrb",
"Title":                "CD-Deploy-For-WP-RFC"
}
```

e. Crea la RFC, specificando il file Deploy CDApp Rfc e il file dei parametri di esecuzione CDApp Deploy Params:

```
aws amscm create-rfc --cli-input-json file://DeployCDAppRfc.json  --execution-
parameters file://DeployCDAppParams.json
```

Riceverai il nuovo RFC nella RfcId risposta. Salva l'ID per i passaggi successivi.

f. Invia la RFC:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Se la RFC ha esito positivo, non riceverai alcun output.

g. Per verificare lo stato della RFC, esegui

```
aws amscm get-rfc --rfc-id RFC_ID
```

Convalida della distribuzione dell'applicazione

Passa all'endpoint (ELB CName) del sistema di bilanciamento del carico creato in precedenza, con il percorso distribuito:/. WordPress WordPress Ad esempio:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

Riduci la distribuzione delle applicazioni

Una volta terminato il tutorial, ti consigliamo di interrompere l'implementazione in modo da non farti pagare per le risorse.

Di seguito è riportata un'operazione generica di eliminazione dello stack. Ti consigliamo di inviarla due volte, una per lo stack HA 2-Tier e una volta per lo stack di bucket S3. Come ultima operazione, invia una richiesta di servizio per eliminare tutte le istantanee per il bucket S3 (include l'ID dello stack del bucket S3 nella richiesta di servizio). Vengono eliminati automaticamente dopo 10 giorni, ma eliminarli anticipatamente consente di risparmiare un po' di costi.

Questa procedura dettagliata fornisce un esempio di utilizzo della console AMS per eliminare uno stack S3; questa procedura si applica all'eliminazione di qualsiasi stack utilizzando la console AMS.

> **Note**
>
> Se si elimina un bucket S3, è necessario prima svuotarlo degli oggetti.

DATI RICHIESTI:

- `StackId`: Lo stack da usare. Puoi trovarlo consultando la pagina AMS Console Stacks, disponibile tramite un link nel menu di navigazione a sinistra. Utilizzando l'API/CLI AMS SKMS, esegui il riferimento per l'API AMS SKMS, consulta la scheda Report nella Console AWS Artifact. Operazione (nella CLI). `list-stack-summaries`
- L'ID del tipo di modifica per questa procedura dettagliata è «1.0"`ct-0q0bic0ywqk6c`, per scoprire la versione più recente, esegui questo comando:

```
aws amscm list-change-type-version-summaries --filter
 Attribute=ChangeTypeId,Value=ct-0q0bic0ywqk6c
```

CREAZIONE IN LINEA:

- Esegui il comando create RFC con i parametri di esecuzione forniti in linea (evita le virgolette quando fornisci i parametri di esecuzione in linea). E

```
aws amscm create-rfc --change-type-id "ct-0q0bic0ywqk6c" --change-type-version "1.0"
 --title "Delete My Stack" --execution-parameters "{\"StackId\":\"STACK_ID\"}"
```

- Invia la RFC utilizzando l'ID RFC restituito nell'operazione di creazione RFC. Fino all'invio, la RFC rimane nello `Editing` stato e non viene applicata alcuna modifica.

```
aws amscm submit-rfc --rfc-id RFC_ID
```

- Monitora lo stato RFC e visualizza l'output di esecuzione:

```
aws amscm get-rfc --rfc-id RFC_ID
```

CREAZIONE DEL MODELLO:

1. Esporta il modello RFC in un file nella cartella corrente; l'esempio lo chiama DeleteStackRfc .json:

   ```
   aws amscm create-rfc --generate-cli-skeleton > DeleteStackRfc.json
   ```

2. Modifica e salva il file.json. DeleteStackRfc Poiché l'eliminazione di uno stack ha un solo parametro di esecuzione, i parametri di esecuzione possono essere contenuti nel DeleteStackRfc file.json stesso (non è necessario creare un file JSON separato con parametri di esecuzione).

   Le virgolette interne dell'estensione ExecutionParameters JSON devono essere eliminate con una barra rovesciata (\). Esempio senza ora di inizio e fine:

   ```
   {
   "ChangeTypeVersion":    "1.0",
   "ChangeTypeId":         "ct-0q0bic0ywqk6c",
   "Title":                "Delete-My-Stack-RFC"
   "ExecutionParameters":  "{
           \"StackId\":\"STACK_ID\"}"
   }
   ```

3. Crea la RFC:

```
aws amscm create-rfc --cli-input-json file://DeleteStackRfc.json
```

Riceverai RfcId il nuovo RFC nella risposta. Ad esempio:

```
{
"RfcId": "daaa1867-ffc5-1473-192a-842f6b326102"
}
```

Salva l'ID per i passaggi successivi.

4. Invia la RFC:

```
aws amscm submit-rfc --rfc-id RFC_ID
```

Se la RFC ha esito positivo, non riceverai alcuna conferma dalla riga di comando.

5. Per monitorare lo stato della richiesta e visualizzare l'output di esecuzione:

```
aws amscm get-rfc --rfc-id RFC_ID --query "Rfc.
{Status:Status.Name,Exec:ExecutionOutput}" --output table
```

Tutorial sulla console: Stack a due livelli ad alta disponibilità (Linux/RHEL)

Questa sezione descrive come implementare un WordPress sito ad alta disponibilità (HA) in un ambiente AMS utilizzando la console AMS.

> **Note**
>
> Questa procedura dettagliata di implementazione è stata testata in ambienti AMZN Linux e RHEL.

Riepilogo delle attività e dei requisiti richiesti: RFCs

1. Crea un'infrastruttura (stack HA a due livelli)
2. Crea un bucket S3 per le applicazioni CodeDeploy
3. Crea il pacchetto di WordPress applicazioni e caricalo nel bucket S3
4. Distribuisci l'applicazione con CodeDeploy

5. Accedi al WordPress sito e accedi per convalidare la distribuzione
6. Distruggi la distribuzione

Le descrizioni di tutte le opzioni CT, incluse ChangeTypeId, sono disponibili in AMS Change Type Reference.

Prima di iniziare

The Deployment | Advanced Stack Components | High Availability Two Tier Stack | Create CT crea un gruppo Auto Scaling, un load balancer, un database e CodeDeploy un nome di applicazione e un gruppo di implementazione (con lo stesso nome assegnato all'applicazione). Per informazioni su CodeDeploy , consulta What is? CodeDeploy

Questa procedura dettagliata utilizza uno stack RFC a due livelli ad alta disponibilità che include `UserData` e descrive anche come creare un WordPress pacchetto da distribuire. CodeDeploy

L'esempio `UserData` illustrato nell'esempio ottiene i metadati dell'istanza, come l'ID dell'istanza, la regione e così via, dall'interno di un'istanza in esecuzione interrogando il servizio di metadati dell'istanza disponibile all'indirizzo http://169.254.169.254/latest/meta-data/. EC2 Questa riga dello script dei dati utente:`REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/ | sed 's/[a-z]$//')`, recupera il nome della zona di disponibilità dal servizio di metadati nella variabile $REGION per le nostre regioni supportate e lo utilizza per completare l'URL per il bucket S3 in cui viene scaricato l'agente. CodeDeploy L'IP 169.254.169.254 è instradabile solo all'interno del VPC (tutti possono interrogare il servizio). VPCs Per informazioni sul servizio, consulta Metadati dell'istanza e dati utente. Nota anche che gli script immessi come UserData vengono eseguiti come utente «root» e non è necessario utilizzare il comando «sudo».

Questa procedura dettagliata lascia i seguenti parametri al valore predefinito (mostrato):

- Gruppo Auto Scaling:. `Cooldown=300, DesiredCapacity=2, EBSOptimized=false, HealthCheckGracePeriod=600, IAMInstanceProfile=customer-mc-ec2-instance-profile, InstanceDetailedMonitoring=true, InstanceRootVolumeIops=0, InstanceRootVolumeType=standard, InstanceType=m3.medium, MaxInstances=2, MinInstances=2, ScaleDownPolicyCooldown=300, ScaleDownPolicyEvaluationPeriods=4, ScaleDownPolicyPeriod=60, ScaleDownPolicyScalingAdjustment=-1, ScaleDownPolicyStatistic=Average, ScaleDownPolicyThreshold=35, ScaleMetricName=CPUUtilization, ScaleUpPolicyCooldown=60, ScaleUpPolicyEvaluationPeriods=2,`

`ScaleUpPolicyPeriod=60, ScaleUpPolicyScalingAdjustment=2, ScaleUpPolicyStatistic=Average, ScaleUpPolicyThreshold=75`

- Load Balancer:. `HealthCheckInterval=30, HealthCheckTimeout=5`
- Banca dati:`BackupRetentionPeriod=7, Backups=true, InstanceType=db.m3.medium, IOPS=0, MultiAZ=true, PreferredBackupWindow=22:00-23:00, PreferredMaintenanceWindow=wed:03:32-wed:04:02, StorageEncrypted=false, StorageEncryptionKey="", StorageType=gp2`.
- Applicazione:`DeploymentConfigName=CodeDeployDefault.OneAtATime`.

Parametri variabili:

La console offre un'opzione ASAP per l'ora di inizio e questa procedura dettagliata consiglia di utilizzarla. ASAP fa sì che la RFC venga eseguita non appena vengono approvate.

> **Note**
>
> Ci sono molti parametri che potreste scegliere di impostare in modo diverso da quelli mostrati. I valori per i parametri mostrati nell'esempio sono stati testati ma potrebbero non essere adatti a te. Negli esempi vengono mostrati solo i valori obbligatori. I valori nei *`replaceable`* caratteri devono essere modificati in quanto sono specifici del tuo account.

Crea l'infrastruttura

Questa procedura utilizza lo stack CT a due livelli ad alta disponibilità seguito dallo storage CT Create S3.

La raccolta dei seguenti dati prima di iniziare velocizzerà la distribuzione.

I DATI RICHIESTI HANNO UNO STACK:

- AutoScalingGroup:
  - UserData: Questo valore è fornito in questo tutorial. Include comandi per configurare la risorsa CodeDeploy e avviare l' CodeDeploy agente.
  - AMI-ID: questo valore determina il sistema operativo delle EC2 istanze che verrà avviato dal gruppo Auto Scaling (ASG). Seleziona un'AMI nel tuo account che inizi con «cliente-» e sia del sistema operativo che desideri. Trova AMI IDs nella pagina dei VPCs dettagli della console AMS

VPCs ->. Questa procedura dettagliata è destinata alla ASGs configurazione per l'utilizzo di un'AMI Amazon Linux o RHEL.

- Database:
  - Questi parametri, DBEngineEngineVersion, e LicenseModeldevono essere impostati in base alla situazione, sebbene i valori mostrati nell'esempio siano stati testati. Il tutorial utilizza rispettivamente questi valori:*MySQL*,*8.0.16*,*general-public-license*.
  - Questi parametri, DBNameMasterUserPassword, e MasterUsernamesono necessari per la distribuzione del pacchetto di applicazioni. Il tutorial utilizza rispettivamente questi valori:,*wordpressDB*,*p4ssw0rd*. *admin* Nota che DBName può contenere solo caratteri alfanumerici.
  - Quando inserisci il codice MasterUsernameper il DB RDS, verrà visualizzato in chiaro, quindi accedi al database il prima possibile e modifica la password per garantire la tua sicurezza.
  - Per gli RDSSubnetID, usa due sottoreti private. Inseriscili uno alla volta premendo «Invio» dopo ciascuno. Trova Subnet IDs con il riferimento all'API Per l'AMS SKMS, consulta la scheda Report nella Console AWS Artifact. operation (CLI: list-subnet-summaries) o nella pagina dei dettagli della console AMS -> VPC. VPCs
- LoadBalancer:
  - Imposta questo parametro, Public, su true perché il tutorial utilizza sottoreti ELB pubbliche.
  - ELBSubnetID: utilizza due sottoreti pubbliche. Inseriscili uno alla volta premendo «Invio» dopo ciascuno. Trova Subnet IDs con il riferimento all'API Per l'AMS SKMS, consulta la scheda Report nella Console AWS Artifact. operation (CLI: list-subnet-summaries) o nella pagina dei dettagli della console AMS -> VPC. VPCs
- Applicazione: il ApplicationNamevalore imposta il nome dell'applicazione e il nome del gruppo di distribuzione CodeDeploy . CodeDeploy Lo usi per distribuire la tua applicazione. Deve essere unico nell'account. Per verificare la presenza di CodeDeploy nomi nel tuo account, consulta la CodeDeploy Console. L'esempio utilizza *WordPress* ma, se intendi utilizzare quel valore, assicurati che non sia già in uso.

1. Avvia lo stack ad alta disponibilità.
   a. Nella pagina Crea RFC, seleziona la categoria Deployment, la sottocategoria Standard Stacks, la voce High availability two tier stack e l'operazione Create, dall'elenco.
   b. IMPORTANTE: scegli Advanced e imposta i valori come mostrato.

Devi solo inserire i valori per le opzioni contrassegnate da un asterisco (*), i valori testati sono mostrati nell'esempio; puoi lasciare vuote le opzioni vuote non obbligatorie.

c. Per la sezione Descrizione RFC:

```
Subject: WP-HA-2-Tier-RFC
```

d. Per la sezione Informazioni sulle risorse, impostate i parametri per Database AutoScalingGroupLoadBalancer, Applicazione e Tag.

Inoltre, lo scopo della chiave di tag AppName "" è consentire di cercare facilmente le istanze ASG nella EC2 console; è possibile chiamare questa chiave di tag «Nome» o qualsiasi altro nome di chiave desiderato. Tieni presente che puoi aggiungere fino a 50 tag.

```
UserData:
    #!/bin/bash
    REGION=$(curl 169.254.169.254/latest/meta-data/placement/availability-zone/
 | sed 's/[a-z]$//')
    yum -y install ruby httpd
    chkconfig httpd on
    service httpd start
    touch /var/www/html/status
    cd /tmp
    curl -O https://aws-codedeploy-$REGION.s3.amazonaws.com/latest/install
    chmod +x ./install
    ./install auto
    chkconfig codedeploy-agent on
    service codedeploy-agent start
AmiId:               AMI-ID
Description:         WP-HA-2-Tier-Stack

Database:
    LicenseModel:    general-public-license (USE RADIO BUTTON)
    EngineVersion:   8.0.16
    DBEngine:        MySQL
    RDSSubnetIds:    PRIVATE_AZ1 PRIVATE_AZ2 (ENTER ONE AT A TIME PRESSING
 "ENTER" AFTER EACH)
    MasterUserPassword:  p4ssw0rd
    MasterUsername:      admin
    DBName:              wordpressDB

LoadBalancer:
```

```
    Public:              true (USE RADIO BUTTON)
    ELBSubnetIds:        PUBLIC_AZ1 PUBLIC_AZ2

Application:
    ApplicationName:     WordPress

Tags:
    Name:                WP-Rhel-Stack
```

e. Al termine, fai clic su Invia.

2. Accedi al database che hai creato e modifica la password.
3. Avvia uno stack di bucket S3.

   La raccolta dei seguenti dati prima di iniziare velocizzerà la distribuzione.

   BUCKET S3 DI DATI RICHIESTO:

   - VPC-ID: questo valore determina dove si troverà il tuo S3 Bucket. Trova un VPC IDs con il riferimento all'API For the AMS SKMS, consulta la scheda Report nella Console AWS Artifact Operation (list-vpc-summariesCLI:) o nella pagina della console AMS. VPCs
   - BucketName: Questo valore imposta il nome del bucket S3, lo usi per caricare il pacchetto dell'applicazione. Deve essere univoco in tutta l'area dell'account e non può includere lettere maiuscole. L'inclusione dell'ID dell'account come parte di non BucketName è un requisito, ma semplifica l'identificazione del bucket in un secondo momento. Per vedere quali nomi di bucket S3 esistono nell'account, accedi alla console Amazon S3 del tuo account.

   a. Nella pagina Crea RFC, seleziona la categoria Deployment, la sottocategoria Advanced Stack Components, l'elemento S3 storage e l'operazione Create dall'elenco di selezione RFC CT.

   b. Mantieni l'opzione Basic predefinita e imposta i valori come mostrato.

```
Subject:              S3-Bucket-WP-HA-RFC
Description:          S3BucketForWordPressBundles
BucketName:           ACCOUNT_ID-BUCKET_NAME
AccessControl:        Private
VpcId:                VPC_ID
Name:                 S3-Bucket-WP-HA-Stack
TimeoutInMinutes:     60
```

c. Al termine, fate clic su Invia. Il bucket distribuito con questo tipo di modifica consente read/write l'accesso completo all'intero account.

Crea, carica e distribuisci l'applicazione

Innanzitutto, create un pacchetto di WordPress applicazioni, quindi utilizzate il CodeDeploy CTs per creare e distribuire l'applicazione.

1. Scarica WordPress, estrai i file e crea un file. cartella /scripts.

   Comando Linux:

   ```
   wget https://github.com/WordPress/WordPress/archive/master.zip
   ```

   Windows: incolla `https://github.com/WordPress/WordPress/archive/master.zip` in una finestra del browser e scarica il file zip.

   Crea una directory temporanea in cui assemblare il pacchetto.

   Linux:

   ```
   mkdir /tmp/WordPress
   ```

   Windows: crea una cartella "WordPress", utilizzerai il percorso della directory in seguito.

2. Estrai il WordPress codice sorgente nella cartella WordPress "" e crea un file. cartella /scripts.

   Linux:

   ```
   unzip master.zip -d /tmp/WordPress_Temp
   cp -paf /tmp/WordPress_Temp/WordPress-master/* /tmp/WordPress
   rm -rf /tmp/WordPress_Temp
   rm -f master
   cd /tmp/WordPress
   mkdir scripts
   ```

   Windows: vai alla cartella "WordPress" che hai creato e lì crea una cartella «scripts».

   Se utilizzate un ambiente Windows, assicuratevi di impostare il tipo di interruzione per i file di script su Unix (LF). In Notepad ++, questa è un'opzione in basso a destra della finestra.

3. Crea il file CodeDeploy appspec.yml, nella WordPress directory (se copi l'esempio, controlla l'indentazione, ogni spazio conta). IMPORTANTE: assicurati che il percorso «sorgente» sia corretto per copiare WordPress i file (in questo caso, nella tua WordPress directory) nella destinazione prevista (/). var/www/html/WordPress Nell'esempio, il file appspec.yml si trova nella directory con WordPress i file, quindi è necessario solo «/». Inoltre, anche se hai usato un'AMI RHEL per il tuo gruppo Auto Scaling, lascia la riga «os: linux» così com'è. Esempio di file appspec.yml:

```
version: 0.0
os: linux
files:
  - source: /
    destination: /var/www/html/WordPress
hooks:
  BeforeInstall:
    - location: scripts/install_dependencies.sh
      timeout: 300
      runas: root
  AfterInstall:
    - location: scripts/config_wordpress.sh
      timeout: 300
      runas: root
  ApplicationStart:
    - location: scripts/start_server.sh
      timeout: 300
      runas: root
  ApplicationStop:
    - location: scripts/stop_server.sh
      timeout: 300
      runas: root
```

4. Crea script di file bash in. WordPress cartella /scripts.

   Innanzitutto, crea `config_wordpress.sh` con il seguente contenuto (se preferisci, puoi modificare direttamente il file wp-config.php).

   > **Note**
   >
   > Sostituisci *`DBName`* con il valore fornito nell'HA Stack RFC (ad esempio,`wordpress`). Sostituisci *`DB_MasterUsername`* con il `MasterUsername` valore fornito nell'HA Stack RFC (ad esempio,). `admin`

Sostituisci *DB_MasterUserPassword* con il `MasterUserPassword` valore fornito nell'HA Stack RFC (ad esempio,). `p4ssw0rd`
Sostituire *DB_ENDPOINT* con il nome DNS dell'endpoint negli output di esecuzione di HA Stack RFC (ad esempio,). `srt1cz23n45sfg.clgvd67uvydk.us-east-1.rds.amazonaws.com` Puoi trovarlo con l'GetRfcoperazione (CLI: get-rfc --rfc-id RFC_ID) o nella pagina dei dettagli RFC della console AMS per l'HA Stack RFC che hai inviato in precedenza.

```
#!/bin/bash
chmod -R 755 /var/www/html/WordPress
cp /var/www/html/WordPress/wp-config-sample.php /var/www/html/WordPress/wp-config.php
cd /var/www/html/WordPress
sed -i "s/database_name_here/DBName/g" wp-config.php
sed -i "s/username_here/DB_MasterUsername/g" wp-config.php
sed -i "s/password_here/DB_MasterUserPassword/g" wp-config.php
sed -i "s/localhost/DB_ENDPOINT/g" wp-config.php
```

5. `install_dependencies.sh`Nella stessa directory, crea con il seguente contenuto:

```
#!/bin/bash
yum install -y php
yum install -y php-mysql
yum install -y mysql
service httpd restart
```

> **Note**
>
> HTTPS viene installato come parte dei dati utente al momento del lancio per consentire il funzionamento dei controlli sanitari sin dall'inizio.

6. Nella stessa directory, crea `start_server.sh` con il seguente contenuto:

   - Per le istanze Amazon Linux, usa questo:

```
#!/bin/bash
service httpd start
```

- Per le istanze RHEL, usa questo (i comandi aggiuntivi sono politiche che consentono a SELINUX di accettare): WordPress

```
#!/bin/bash
setsebool -P  httpd_can_network_connect_db 1
setsebool -P  httpd_can_network_connect 1
chcon -t httpd_sys_rw_content_t /var/www/html/WordPress/wp-content -R
restorecon -Rv /var/www/html
service httpd start
```

7. Nella stessa directory create `stop_server.sh` con il seguente contenuto:

```
#!/bin/bash
service httpd stop
```

8. Crea il pacchetto zip.

   Linux:

```
$ cd /tmp/WordPress
$ zip -r wordpress.zip .
```

   Windows: vai alla cartella WordPress "" e seleziona tutti i file e crea un file zip, assicurati di chiamarlo wordpress.zip.

1. Carica il pacchetto dell'applicazione nel bucket S3

   Il pacchetto deve essere attivo per continuare a distribuire lo stack.

   Hai automaticamente accesso a qualsiasi istanza di bucket S3 che crei. Puoi accedervi tramite i tuoi Bastions (vedi Accesso alle istanze) o tramite la console S3 e caricare il CodeDeploy pacchetto con drag-and-drop, oppure sfogliando e selezionando il file.

   Puoi anche usare il seguente comando in una finestra di shell; assicurati di avere il percorso corretto del file zip:

```
aws s3 cp wordpress/wordpress.zip s3://BUCKET_NAME/
```

2. Distribuite l' WordPress CodeDeploy Application Bundle

CODICE DI DATI RICHIESTO, DISTRIBUZIONE DELL'APPLICAZIONE:

- CodeDeployApplicationName: Il nome che hai assegnato all' CodeDeploy applicazione.
- CodeDeployGroupName: Poiché l' CodeDeploy applicazione e il gruppo sono stati entrambi creati dal nome assegnato all' CodeDeploy applicazione nello stack HA RFC, questo nome è lo stesso del. CodeDeployApplicationName
- S3Bucket: il nome che hai assegnato al bucket S3.
- S3 BundleType e S3Key: fanno parte del pacchetto di applicazioni che hai distribuito. WordPress
- VpcId: Il VPC pertinente.

a. Nella pagina Crea RFC, seleziona la categoria Distribuzione, la sottocategoria Applicazioni, CodeDeploy l'elemento applicazione e l'operazione Deploy dall'elenco di selezione RFC CT.

b. Mantieni l'opzione Basic predefinita e imposta i valori come mostrato.

> **Note**
>
> Fai riferimento all' CodeDeploy applicazione, al gruppo CodeDeploy di distribuzione, al bucket S3 e al bundle creati in precedenza.

```
Subject:                                    WP-CD-Deploy-RFC
Description:                                DeployWordPress
S3Bucket:                                   BUCKET_NAME
S3Key:                                      wordpress.zip
S3BundleType:                               zip
CodeDeployApplicationName:                  WordPress
CodeDeployDeploymentGroupName:              WordPress
CodeDeployIgnoreApplicationStopFailures:    false
RevisionType:                               S3



VpcId:                                      VPC_ID
Name:                                       WP-CD-Deploy-Op
TimeoutInMinutes:                           60
```

c. Al termine, fai clic su Invia.

Convalida della distribuzione dell'applicazione

Passa all'endpoint (LoadBalancerCName) del sistema di bilanciamento del carico creato in precedenza, con il percorso distribuito:/. WordPress WordPress Esempio:

```
http://stack-ID-FOR-ELB.us-east-1.elb.amazonaws.com/WordPress
```

Dovresti vedere una pagina come questa:

Eliminare l'implementazione ad alta disponibilità

Per interrompere l'implementazione, invii il Delete Stack CT sullo stack HA Two-Tier e il bucket S3, e puoi richiedere l'eliminazione delle istantanee RDS (vengono eliminate automaticamente dopo dieci giorni, ma costano una piccola somma). Raccogli lo stack IDs per lo stack HA e il bucket S3, quindi segui questi passaggi. Vedi Stack | Elimina.

Appendice: Questionario di onboarding SALZ

Argomenti

- Riepilogo della distribuzione
- Considerazioni sull'architettura dell'ambiente
- Avvisi di monitoraggio della zona di atterraggio con account singolo
- Finestra di manutenzione
- Fasi successive

Queste sono alcune delle informazioni a cui dovrai pensare prima di effettuare l'onboarding di un account.

Riepilogo della distribuzione

Una descrizione della distribuzione. Ad esempio:

- Questo account serve per la distribuzione di un' Line-of-Businessapplicazione (al contrario della distribuzione di un'applicazione del prodotto).
- L'implementazione prevede un ARP (proxy inverso autenticato) con scalabilità automatica all'interno della sottorete pubblica o DMZ dell'account.

- I server Web e applicativi verranno distribuiti all'interno della sottorete privata dell'account.
- Un'istanza RDS (Amazon Relational Database Service) verrà inoltre distribuita all'interno della sottorete privata dell'account.
- I server (ARP, web, applicazioni, database, load balancer, ecc.) sono separati in gruppi di sicurezza distinti.
- L'account richiede un design HA (alta disponibilità) distribuito tra le zone di disponibilità (AZs), ad esempio «Multi-AZ».

Considerazioni sull'architettura dell'ambiente

Considerate i seguenti criteri per decidere come configurare l'ambiente e l'architettura.

- Il vostro data center virtuale si ricollegherà alla rete aziendale?
  - Disponi di un AWS DirectConnect servizio esistente o hai bisogno di un nuovo DirectConnect servizio?
  - Hai una connessione VPN esistente o hai bisogno di un nuovo servizio VPN?
- Qual è l'intervallo di blocchi CIDR disponibile di indirizzi interni che è possibile allocare? (/16 consigliato, non deve sovrapporsi agli intervalli di rete aziendali)
- Il tuo data center virtuale richiederà l'accesso a Internet?
- Quali regioni intendi utilizzare? (Sydney/N. Virginia/Dublin)
- Avrete bisogno di una sottorete Shared Services per ospitare applicazioni con connettività a tutte le altre sottoreti?
- Quali sono le divisioni organizzative che vorresti fossero ospitate come sottoreti separate. Per ognuna:
  - Di quale connettività hai bisogno con le altre sottoreti?
  - La sottorete richiede l'accesso a Internet?
  - Esistono restrizioni alla distribuzione delle applicazioni in quella sottorete?
  - Esistono requisiti di rete particolari per quella sottorete?
- Desiderate ambienti di and/or test di sviluppo separati? (Includerà servizi condivisi duplicati per l'accesso in qualsiasi momento)
- Quali sono i requisiti per il backup delle istantanee?
- Hai già un processo di manutenzione o una o più finestre di patch che vorresti mantenere?
- Quali sono i requisiti per la registrazione del dominio?

- Hai dei requisiti per il Single Sign-On? (ad esempio, AD, LDAP)
- Quali sono il sistema operativo complessivo previsto e i requisiti di capacità previsti?

Avvisi di monitoraggio della zona di atterraggio con account singolo

AMS offre un modo per ricevere avvisi diretti (anziché ricevere notifiche dal servizio AMS) per determinati avvisi di monitoraggio. Per iscriverti, assicurati che il tuo Cloud Architect (CA) o il Cloud Service Delivery Manager (CSDM) ricevano le seguenti informazioni:

Direct Alerts Email: questi sono gli indirizzi e-mail a cui desideri che AMS invii determinati avvisi basati sulle risorse. Per informazioni dettagliate su quali avvisi vengono inviati direttamente via e-mail, consulta la sezione Alerts from Baseline Monitoring in AMS nella Guida per l'utente di AMS per Single-Account Landing Zone. Per ulteriori informazioni sul monitoraggio AMS, consulta Monitoring Management nella AMS User Guide for Single-Account Landing Zone.

Finestra di manutenzione

Ti consigliamo di creare una finestra di manutenzione che tenga conto delle diverse esigenze applicative, dei diversi Regioni AWS e diversi periodi di stress. La finestra di manutenzione è quella in cui AMS applicherà le patch. Ecco alcune linee guida:

- Per limitare l'impatto sugli utenti, pianifica la finestra di manutenzione in base al Regione AWS luogo in cui sono distribuiti gli ambienti.
- Pianifica una finestra al di fuori del normale orario lavorativo e quando è previsto il minor traffico sui server di produzione.
- In genere, gli stack di infrastruttura richiedono aggiornamenti mensili.
- Pianifica una finestra di manutenzione per almeno 300 minuti. L'applicazione delle patch al sistema operativo richiede 60-90 minuti, l'applicazione delle patch allo stack dell'infrastruttura richiede 180-300 minuti.

Fasi successive

Il team di onboarding di AMS ti assisterà in ogni fase dell'onboarding del tuo account su AMS. Questi sono i requisiti per l'onboarding:

- Fornisci un nuovo codice Account AWS da utilizzare per AMS e fornisci un Account AWS ID.
- Registrati per ottenere il livello di Support desiderato.

- Crea un ruolo IAM su più account per concedere l'accesso all'account di provisioning AMS e fornire il nome del ruolo ad AMS.
- Aggiungi l'account 753102745277 come entità affidabile.

Appendice: Regola di reclamo di ActiveDirectory Federation Services (ADFS) e impostazioni SAML

Per step-by-step istruzioni dettagliate su come installare e configurare ADFS, consulta Enabling Federation to AWS Using Windows Active Directory, ADFS e SAML 2.0.

Configurazioni delle regole di reclamo ADFS

Se disponi già di un'implementazione ADFS, configura quanto segue:

- Affidarsi alla fiducia delle parti
- Regole sui reclami

Le procedure relative alla fiducia e ai reclami dei relying party sono tratte dal blog Enabling Federation to AWS Using Windows Active Directory, AD FS e SAML 2.0

- Regole relative ai reclami:
  - Nameid: configurazione per post del blog
  - RoleSessionName: Configura come segue
    - Nome della regola di rivendicazione: **`RoleSessionName`**
    - Archivio attributi: **`Active Directory`**
    - Attributo LDAP: **`SAM-Account-Name`**
    - Tipo di reclamo in uscita: **`https://aws.amazon.com/SAML/Attributes/RoleSessionName`**
    - Get AD Groups: configurazione per post sul blog
    - Richiesta di ruolo: configura come segue

```
c:[Type == "http://temp/variable", Value =~ "(?i)^AWS-([^d]{12})-"]
```

```
=> issue(Type = "https://aws.amazon.com/SAML/Attributes/Role", Value =
 RegExReplace(c.Value, "AWS-([^d]{12})-", "arn:aws:iam::$1:saml-provider/
customer-readonly-saml,arn:aws:iam::$1:role/"));
```

Console Web

Puoi accedere alla console Web AWS utilizzando il link seguente sostituendolo *[ADFS-FQDN]* con il nome di dominio completo della tua implementazione ADFS.

https://.aspx *[ADFS-FQDN]* adfs/ls/IdpInitiatedSignOn

Il reparto IT può distribuire il link sopra riportato alla popolazione di utenti tramite una politica di gruppo.

Accesso a API e CLI con SAML

Come configurare l'accesso alle API e alla CLI con SAML.

I pacchetti python provengono dai seguenti post del blog:

- NTLM: come implementare API federate e accesso CLI utilizzando SAML 2.0 e AD FS
- Moduli: come implementare una soluzione generale per l'accesso API/CLI federato utilizzando SAML 2.0
- PowerShell: Come configurare l'accesso alle API federate ad AWS utilizzando Windows PowerShell

Configurazione dello script

1. Utilizzando Notepad++, modifica la regione predefinita nella regione corretta
2. Utilizzando Notepad++, disabilita la verifica SSL per gli ambienti di test e sviluppo
3. Utilizzando Notepad++, configura idpentryurl

```
https://[ADFS-FDQN]/adfs/ls/IdpInitiatedSignOn.aspx?
loginToRp=urn:amazon:webservices
```

Configurazione di Windows

Le istruzioni riportate di seguito si riferiscono ai pacchetti python. Le credenziali generate saranno valide per 1 ora.

1. Scarica e installa python (2.7.11)

2. Scarica e installa gli strumenti dell'interfaccia a riga di comando di AWS
3. Installa l'AMS CLI:

   a. Scarica il file zip AMS distribuibile fornito dal tuo cloud service delivery manager (CSDM) e decomprimilo.

      Sono disponibili diverse directory e file.

   b. Apri la directory Managed Cloud Distributables -> CLI -> Windows o la directory Managed Cloud Distributables -> CLI -> Linux /macOS, a seconda del sistema operativo in uso, e:

      Per Windows, esegui il programma di installazione appropriato (questo metodo funziona solo su sistemi Windows a 32 o 64 bit):

      - 32 bit: API_x86.msi ManagedCloud
      - 64 bit: API_x64.msi ManagedCloud

      Per Mac/Linux, esegui il file denominato: MC_CLI.sh. Puoi farlo eseguendo questo comando:. `sh MC_CLI.sh` Nota che le directory amscm e amsskms e il loro contenuto devono trovarsi nella stessa directory del file MC_CLI.sh.

   c. Se le credenziali aziendali vengono utilizzate tramite federazione con AWS (la configurazione predefinita di AMS), è necessario installare uno strumento di gestione delle credenziali in grado di accedere al servizio di federazione. Ad esempio, puoi utilizzare questo AWS Security Blog How to Implementation Federated API and CLI Access Using SAML 2.0 e AD FS per aiutarti a configurare i tuoi strumenti di gestione delle credenziali.

   d. Dopo l'installazione, esegui e visualizza i comandi `aws amscm help` e le opzioni`aws amsskms help`.

4. Scarica lo script SAML richiesto

   Scarica in c:\aws\scripts

5. Scarica PIP

   Scarica in c:\aws\downloads

6. Utilizzando PowerShell, installa PIP

   <pythondir>. \ python.exe c:\aws\downloads\get -pip.py

7. Utilizzando PowerShell, installa il modulo di avvio

<pythondir\ scripts>Usare, installare il modulo boto ----sep----pip install boto

8. Utilizzo del modulo di PowerShell richiesta di installazione

   <pythondir\ scripts>Utilizzo, installa il modulo ----sep----pip install requests

9. Utilizzo del PowerShell modulo di sicurezza delle richieste di installazione

   <pythondir\ scripts>Utilizzo, installa il modulo di sicurezza ----sep----pip install requests [sicurezza]

10. Usando PowerShell, installa il modulo beautifulsoup

    <pythondir\ scripts>Usando, installa il modulo beautifulsoup ----sep----pip install beautifulsoup4

11. Utilizzando PowerShell, crea una cartella chiamata .aws nel profilo degli utenti (%userprofile% \ .aws)

    mkdir .aws

12. Utilizzando PowerShell, crea un file di credenziali nella cartella.aws

    Credenziali New-Item -type file —force

    Il file delle credenziali non deve avere un'estensione

    Il nome del file deve essere tutto minuscolo e avere le credenziali del nome

13. Apri il file delle credenziali con il blocco note e incolla i seguenti dati, specificando la regione corretta

    ```
    [default]
    output = json
    region = us-east-1
    aws_access_key_id =
    aws_secret_access_key =
    ```

14. Utilizzo dello script PowerShell SAML e dell'accesso

    <pythondir>. \ python.exe c:\aws\scripts\samlapi.py

    NOME UTENTE: [NOME UTENTE] @upn

    Scegli il ruolo che vorresti assumere

Configurazione Linux

Le credenziali generate saranno valide per 1 ora.

1. Utilizzando WinSCP, trasferisci lo script SAML
2. Utilizzando WinSCP, trasferisci il certificato Root CA (ignoralo per test e sviluppo)
3. Aggiungi la CA ROOT ai certificati root affidabili (ignora per test e sviluppo)

   $ openssl x509 -inform der -in [certname] .cer -out certificate.pem (ignora per test e sviluppo)

   Aggiungi il contenuto di certificate.pem alla fine del file/-bundle.crt (ignora per test dev) etc/ssl/certs/ca
4. Crea la cartella.aws in home/ec2-user 5

   ```
   [default]
   output = json
   region = us-east-1
   aws_access_key_id =
   aws_secret_access_key =
   ```
5. Utilizzando WinSCP, trasferisci il file delle credenziali nella cartella.aws
6. Installa il modulo di avvio

   $ sudo pip installa boto
7. Modulo di richieste di installazione

   Richieste di installazione di $ sudo pip
8. Installa il modulo beautifulsoup

   $ sudo pip installa beautifulsoup4
9. Copia lo script in home/ec2-user

   Imposta le autorizzazioni richieste

   Esegui lo script: samlapi.py

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti alla documentazione dall'ultima versione di AMS.

- Versione API: 2019-05-21
- Ultimo aggiornamento della documentazione: 23 settembre 2025

Modifica	Descrizione	Data
Impostazioni predefinite aggiornate per la conservazione e la rotazione dei log nella sezione SALZ: impostazioni predefinite	Impostazioni predefinite di conservazione e rotazione dei log. Informazioni aggiornate sui AWS CloudTrail log.	11 febbraio 2026
Tipo di modifica aggiornato per la scalabilità automatica degli endpoint nell' SageMaker IA nella sezione Domande frequenti su AWS Managed Services	Utilizza AMS SSP per effettuare il provisioning di Amazon SageMaker AI nel tuo account AMS. Invia una RFC con Management | Advanced stack components | Identity and Access Management (IAM) and Access Management | Aggiorna il tipo di modifica dell'entità o della policy (automazione gestita) (ct-27tuth19k52b4) per aumentare le autorizzazioni di scalabilità automatica temporaneamente o permanentemente, poiché la scalabilità automatica richiede l'accesso permissivo sul servizio. CloudWatch	25 settembre 2025
Riferimenti precisi sui tipi di modifica	Creare, modificare o eliminare gruppi di sicurezza. Per aggiungere un utente: invia una RFC utilizzando Management | Directory Service | Utenti e gruppi | Aggiungi utente al gruppo [ct-24pi85mjtza8k] e Per rimuovere un utente: Invia una RFC utilizzando Management |	08 agosto 2025

Modifica	Descrizione	Data
	Directory Service | Utenti e gruppi | Rimuovi utente dal gruppo [ct-2019s9y3nfml4]	
Link TOC rimosso	Link al AWS glossario TOC rimosso.	08 agosto 2025
Aggiunto link per la guida alla prescrizione	Configura la fatturazione consolidata: collega il nuovo account all'account Payer.	08 maggio 2025
Istruzioni aggiornate per attivare l'accesso IAM a Console di gestione AWS	Sono state chiarite le istruzioni per l'attivazione dell'accesso IAM a. Console di gestione AWS	Attiva l'accesso IAM alla AWS console
Numero aggiornato di interfacce virtuali di transito consentite sulle connessioni dedicate Direct Connect	Le connessioni dedicate Direct Connect ora hanno un limite di 4 interfacce virtuali di transito per connessione	Connessione di Direct Connect a Transit Gateway
Migliora la formulazione.	Ha specificato che «utilizzato solo come elenco «Deny» "deve includere «Allow All» per garantire le operazioni di monitoraggio e gestione di AMS.	Configurazione di rete
Informazioni aggiuntive sull'uso della CLI AMS.	«Nota aggiunta che l'`--region`opzione potrebbe essere necessaria per alcuni comandi CLI»	Installa l'AMS CLIs
Aggiornamento: i titoli dei capitoli per motivi di coerenza e leggibilità, hanno spostato alcune sottosezioni degli argomenti in sezioni più appropriate	«Modalità per la gestione delle modifiche» è la nuova rubrica «Gestione delle modifiche»	Modifiche alle modalità di gestione

Modifica	Descrizione	Data
Contenuti aggiornati	La modalità AMS precedentemente nota come «modalità di gestione delle modifiche» o «modalità CM standard» è ora nota come «modalità RFC». La sezione delle modalità è stata ampliata.	modalità RFC.
Contenuti aggiornati	La modalità AMS precedentemente nota come «modalità di gestione delle modifiche» o «modalità CM standard» è ora nota come «modalità RFC». La sezione sulle modalità è stata abbreviata e sono stati aggiunti i collegamenti alle sezioni dell'AMS Advanced User Guide sulle modalità.	Modalità AMS.
MALZ: diagramma dell'architettura di rete aggiornato	Architettura degli account di retem	16 giugno 2022
L'elenco degli argomenti è stato spostato sotto i paragrafi di apertura	Introduzione all'onboarding di AWS Managed Services	16 giugno 2022
Contenuti aggiornati, iniziativa linguistica inclusiva	«Account di gestione», non «Account principale».	Ruolo utente IAM in AMS, sezione «Esempi di politiche»
Contenuto aggiornato, nomi dei ruoli degli account Tools	Nome del ruolo aggiornato CustomerMigrationAccessRole a AWSManagedServicesMigrationRole.	AWS Servizio di migrazione delle applicazioni (AWS MGN)
SALZ: impostazioni predefinite per la gestione della continuità	Link aggiornato e informazioni obsolete rimosse da Tag VPC e impostazioni predefinite	28 febbraio 2022

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.