Concetti e procedure avanzate di AMS

Guida per l'utente avanzato di AMS

Version October 3, 2025

Guida per l'utente avanzato di AMS: Concetti e procedure avanzate di AMS

Table of Contents

Che cos'è AWS Managed Services?

Benvenuto in AWS Managed Services (AMS), gestione delle operazioni infrastrutturali per Amazon Web Services (AWS). AMS è un servizio aziendale che fornisce la gestione continua dell' AWS infrastruttura.

Questa guida per l'utente è destinata ai professionisti IT e agli sviluppatori di applicazioni. Si presuppone una conoscenza di base delle funzionalità IT, delle reti e dei termini e delle pratiche di distribuzione delle applicazioni.

AMS implementa le migliori pratiche e mantiene l'infrastruttura per ridurre i costi operativi e i rischi. AMS fornisce servizi per l'intero ciclo di vita per la fornitura, la gestione e il supporto dell'infrastruttura e automatizza le attività comuni come le richieste di modifica, il monitoraggio, la gestione delle patch, la sicurezza e i servizi di backup. AMS applica le vostre politiche aziendali e di infrastruttura di sicurezza e vi consente di sviluppare soluzioni e applicazioni utilizzando il vostro approccio di sviluppo preferito.

Per comprendere meglio l'architettura AMS, consulta questi diagrammi.

Argomenti

> **Note**
>
> Regioni AWS I nuovi vengono aggiunti frequentemente. Per i sistemi operativi più recenti supportati da AMS e i più recenti supportati da AMS Regioni AWS, vedere. Configurazioni supportate
> Per ulteriori informazioni, consulta Gestione. Regioni AWSRegioni AWS

AMS cerca di migliorare continuamente i nostri servizi in base al feedback degli utenti. Utilizziamo diversi meccanismi per abilitare il self-service, automatizzare le attività ripetitive e implementare nuove funzionalità non appena vengono Servizi AWS rilasciate. Puoi inviare una richiesta di assistenza AMS in qualsiasi momento per suggerire nuove funzionalità o miglioramenti delle funzionalità.

L'orario di lavoro di AMS è 24 ore al giorno, 7 giorni alla settimana, 365 giorni all'anno.

AMS segue una serie di pratiche per la gestione dei servizi IT (ITSM) incentrate sull'allineamento dei servizi IT alle esigenze della vostra azienda.

Informazioni su questa guida per l'utente di AMS

Questa guida per l'utente è destinata ai clienti AMS Advanced con una landing zone con più o meno account. Per maggiori dettagli sulle offerte AMS landing zone, consulta i Termini chiave di AMS; vedi anche l'architettura Multi-Account Landing Zone e l'architettura Single-Account Landing Zone.

Piani operativi AMS

AWS Managed Services (AMS) è disponibile con due piani operativi: AMS Accelerate e AMS Advanced. Un piano operativo offre un set specifico di funzionalità e prevede diversi livelli di servizio, capacità tecniche, requisiti, prezzi e restrizioni. I nostri piani operativi ti offrono la flessibilità necessaria per selezionare le capacità operative giuste per ciascuno dei tuoi AWS carichi di lavoro. Questa sezione descrive le capacità e le differenze, nonché le responsabilità, le caratteristiche e i vantaggi associati a ciascun piano, in modo che possiate capire quale piano operativo è il migliore per i vostri account.

Per un confronto dettagliato delle funzionalità dei due piani operativi, consulta AWS Managed Services Features.

Piano operativo AMS Accelerate

AMS Accelerate è il piano operativo AMS che ti aiuta a gestire l' day-to-dayinfrastruttura del tuo AWS ambiente nuovo o esistente. AMS Accelerate fornisce servizi operativi, come il monitoraggio, la gestione degli incidenti e la sicurezza. AMS Accelerate offre anche un componente aggiuntivo opzionale per carichi di lavoro EC2 basati su Amazon che richiedono patch regolari.

Con AMS Accelerate, sei Account AWS tu a decidere in che modo utilizzare AMS Accelerate, in quali regioni AWS desideri che AMS Accelerate operi, i componenti aggiuntivi necessari e gli accordi sui livelli di servizio (SLAs) di cui hai bisogno. Per maggiori dettagli, consulta Utilizzo del piano operativo di AMS Accelerate e descrizione del servizio.

Piano operativo AMS Advanced

AMS Advanced fornisce servizi per l'intero ciclo di vita per fornire, gestire e supportare l'infrastruttura. Oltre ai servizi operativi forniti da AMS Accelerate, AMS Advanced include anche servizi aggiuntivi, come la gestione delle landing zone, le modifiche e il provisioning dell'infrastruttura, la gestione degli accessi e la sicurezza degli endpoint.

AMS Advanced implementa una landing zone verso la quale migrare i AWS carichi di lavoro e ricevere i servizi operativi AMS. Le nostre zone di atterraggio gestite con più account sono preconfigurate con l'infrastruttura per facilitare l'autenticazione, la sicurezza, il networking e la registrazione.

AMS Advanced include anche un sistema di gestione delle modifiche e degli accessi che protegge i carichi di lavoro impedendo l'accesso non autorizzato o l'implementazione di modifiche rischiose all'infrastruttura. AWS I clienti devono creare una richiesta di modifica (RFC) utilizzando il nostro sistema di gestione delle modifiche per implementare la maggior parte delle modifiche nei vostri account AMS Advanced. Puoi creare modifiche automatiche a RFCs partire da una libreria di modifiche automatizzate verificate preventivamente dai nostri team di sicurezza e operativi oppure richiedi modifiche manuali che vengono riviste e implementate dal nostro team operativo se sono ritenute sicure e supportate da AMS Advanced.

AMS Advanced offre anche diverse opzioni. SLAs Per ulteriori informazioni, consulta la descrizione del servizio AWS Managed Services AMS Advanced.

Guida introduttiva a AWS Managed Services

Per ulteriori informazioni su come iniziare a usare il servizio AMS multi-account landing zone, consulta l'introduzione all'onboarding di AWS Managed Services. Le due guide di onboarding forniscono descrizioni del servizio e domande da considerare per aiutarti a iniziare. Consulta il set di funzionalità AWS Managed Services Features e le risorse correnti su AWS Managed Services Resources.

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.

Descrizione del servizio

AMS Advanced (AMS) è un piano operativo del servizio AWS Managed Services per la gestione delle operazioni dell' AWS infrastruttura. AMS Advanced fornisce operazioni infrastrutturali di routine come patch, gestione della continuità, gestione della sicurezza e processi di gestione IT come la gestione di incidenti, modifiche e richieste di assistenza. Per un elenco dei servizi supportati, consulta AWS Servizi supportati.

YouTube Video: In che modo AMS può aiutarmi a raggiungere l'eccellenza operativa nel cloud?

Argomenti

- AWS Managed Services (AMS) Caratteristiche del piano operativo AMS Advanced
- Cosa facciamo, cosa non facciamo
- Matrice di responsabilità AMS (RACI)
- Componenti di base dell'ambiente AMS
- Limiti dell'account AMS
- Obiettivi del livello di servizio AMS (SLOs)
- AWS Servizi supportati
- Configurazioni supportate
- Funzionalità per sistemi operativi non supportati in AMS
- Interfacce AMS Advanced

- Endpoint VPC AMS
- Namespace protetti da AMS
- Prefissi riservati AMS
- Finestra di manutenzione AMS

AWS Managed Services (AMS) Caratteristiche del piano operativo AMS Advanced

AMS Advanced offre le seguenti funzionalità per AWS i servizi supportati:

- Registrazione, monitoraggio, guardrail e gestione degli eventi:

  AMS configura e monitora l'ambiente gestito per la registrazione delle attività e definisce gli avvisi in base a una serie di controlli di integrità. Gli avvisi vengono analizzati da AMS per i servizi AWS applicabili e quelli che influiscono negativamente sull'utilizzo di tali servizi provocano la creazione di incidenti. AMS aggrega e archivia tutti i log generati come risultato di tutte le operazioni in e CloudWatch i CloudTrail log di sistema in Amazon S3. Puoi richiedere l'inserimento di avvisi aggiuntivi. Oltre ai controlli preventivi di AMS, AMS implementa barriere di configurazione e controlli investigativi per fornirti una protezione continua da configurazioni errate che potrebbero ridurre l'integrità operativa e di sicurezza degli account gestiti, per far rispettare i tuoi controlli come l'etichettatura e la conformità. Quando viene rilevato un controllo monitorato, viene generato un allarme che comporta la notifica, la modifica o la cessazione delle risorse in base alle impostazioni predefinite di AMS che possono essere modificate dall'utente.
- Gestione della continuità (Backup e ripristino):

  AMS fornisce backup di risorse utilizzando la funzionalità AWS Backup standard esistente a intervalli pianificati determinati da te. Le azioni di ripristino da istantanee specifiche possono essere eseguite da AMS con la tua RFC. Le modifiche ai dati che si verificano tra gli intervalli di snapshot sono responsabilità dell'utente in materia di backup. È possibile inviare una RFC per le richieste di backup o di snapshot al di fuori degli intervalli pianificati. In caso di indisponibilità della zona di disponibilità (AZ) in una AWS regione, con l'autorizzazione dell'utente, AMS ripristina l'ambiente gestito ricreando nuovi stack basati su modelli e istantanee EBS disponibili degli stack interessati.
- Gestione della sicurezza e degli accessi:

  AMS fornisce la sicurezza degli endpoint (EPS), come la configurazione della protezione antivirus e antimalware. È inoltre possibile utilizzare strumenti e processi EPS personalizzati e non utilizzare

AMS per EPS utilizzando una funzionalità chiamata bring your own EPS (BYOEPS). AMS configura anche funzionalità di AWS sicurezza predefinite che vengono approvate dall'utente durante l'onboarding, come i ruoli AWS Identity and Access Management (IAM) e i gruppi di EC2 sicurezza Amazon, e utilizza AWS strumenti standard (ad esempio Amazon AWS Security Hub CSPM Macie, Amazon GuardDuty) per monitorare e rispondere ai problemi di sicurezza. Gestisci i tuoi utenti tramite un servizio di directory approvato da te fornito. Per un elenco dei servizi di directory approvati, vedereConfigurazioni supportate.

AMS include la sicurezza degli endpoint (EPS), che include la protezione antivirus (AV), e la protezione antimalware e il rilevamento di malware e intrusioni (Trend Micro). I gruppi di sicurezza sono definiti per modello di stack e vengono modificati all'avvio in base alla visibilità dei gruppi di sicurezza dell'applicazione (pubblici/privati).

L'accesso ai sistemi viene richiesto tramite le richieste di gestione delle modifiche per change (). RFCs La gestione degli accessi fornisce l'accesso a risorse distinte, come EC2 le istanze Amazon Console di gestione AWS, e APIs. Dopo aver stabilito un trust unidirezionale con una distribuzione AMS Microsoft Active Directory durante l'onboarding e la federazione in AWS, puoi utilizzare le tue credenziali aziendali esistenti per tutte le interazioni.

- Gestione delle patch:

  AMS applica e installa gli aggiornamenti alle EC2 istanze per i sistemi operativi supportati (OSs) e il software preinstallato con i sistemi operativi supportati. Per un elenco dei sistemi operativi supportati, consulta. Configurazioni supportate

  AMS offre due modelli per l'applicazione delle patch:

  - Patch standard AMS per l'applicazione di patch tradizionale basata su account e
  - AMS Patch Orchestrator, per l'applicazione di patch basate su tag.

  Nella patch standard di AMS, viene scelta una finestra di manutenzione mensile per consentire ad AMS di eseguire la maggior parte delle attività di patching. AMS applica aggiornamenti di sicurezza critici al di fuori della finestra di manutenzione selezionata (con notifiche appropriate) e aggiornamenti importanti durante la finestra di manutenzione selezionata. AMS applica inoltre gli aggiornamenti agli strumenti di gestione dell'infrastruttura durante la finestra di manutenzione selezionata. Se lo desideri, puoi escludere gli stack dalla gestione delle patch o rifiutare gli aggiornamenti.

  Con AMS Patch Orchestrator, viene definita dall'utente una finestra di manutenzione predefinita per account per consentire ad AMS di eseguire le attività di patching. Puoi pianificare ulteriori

finestre di manutenzione personalizzate per AMS per applicare patch a un set specifico di istanze definite dall'utente con tag. AMS applica tutti gli aggiornamenti disponibili, ma puoi filtrare o rifiutare gli aggiornamenti creando una baseline di patch personalizzata. Per entrambi i modelli, se approvate o rifiutate un aggiornamento fornito nell'ambito della gestione delle patch ma successivamente cambiate idea, siete responsabili dell'avvio dell'aggiornamento tramite una RFC. AMS monitora lo stato delle patch delle risorse ed evidenzia i sistemi non aggiornati nella revisione aziendale mensile. La gestione delle patch è limitata agli stack nell'ambiente gestito, incluse tutte le applicazioni gestite da AMS e i servizi AWS supportati con funzionalità di patching (ad esempio, RDS). Per supportare tutti i tipi di configurazioni dell'infrastruttura quando viene rilasciato un aggiornamento, AMS a) aggiorna l' EC2 istanza e b) fornisce un AMI AMS aggiornato da utilizzare. È responsabilità dell'utente installare, configurare, applicare patch e monitorare tutte le applicazioni aggiuntive non specificatamente trattate in precedenza.

- Gestione delle modifiche:

  La gestione delle modifiche AMS è il meccanismo che consente di controllare le modifiche nell'ambiente gestito. AMS utilizza una combinazione di controlli preventivi e investigativi per facilitare questo processo e offre diversi livelli di controllo e di rischio associato a seconda della modalità AMS selezionata.

  Tutte le azioni nell'ambiente AMS vengono registrate. AWS CloudTrail

  Per ulteriori informazioni su AMS Change Management e sulle diverse modalità, consulta la guida AMS Change Management e AMS Modes.

- Gestione automatizzata e self-service del provisioning:

  Puoi effettuare il provisioning di risorse AWS su AMS Advanced in diversi modi:

  - Invia richieste di modifica per il provisioning e la configurazione () RFCs
  - Implementazione tramite AWS Service Catalog
  - Implementa tramite la modalità Direct Change
  - Implementa tramite la modalità Sviluppatore. Ricorda che le risorse create tramite la modalità Sviluppatore non sono gestite da AMS.
  - Configura i servizi AWS direttamente utilizzando il provisioning self-service per una selezione Servizi AWS (vediAWS Servizi supportati).

- Gestione degli incidenti:

  AMS ti notifica in modo proattivo gli incidenti rilevati da AMS. AMS risponde sia agli incidenti inviati dai clienti che a quelli generati da AMS e li risolve in base alla priorità degli incidenti. Salvo

diversa indicazione dell'utente, gli incidenti che secondo AMS rappresentano un rischio per la sicurezza dell'ambiente gestito e gli incidenti relativi alla disponibilità di AMS e di altri servizi AWS vengono affrontati in modo proattivo. AMS interviene su tutti gli altri incidenti una volta ricevuta l'autorizzazione. Gli incidenti ricorrenti vengono risolti mediante il processo di gestione dei problemi.

- Gestione dei problemi:

  AMS esegue analisi delle tendenze per identificare e indagare sui problemi e identificarne la causa principale. I problemi vengono risolti con una soluzione alternativa o una soluzione permanente che impedisca il ripetersi di impatti futuri simili sui servizi. È possibile richiedere un rapporto post incidente (PIR) per qualsiasi incidente «elevato», previa risoluzione. Il PIR analizza la causa principale e le azioni preventive intraprese, inclusa l'implementazione di misure preventive.

- Segnalazione:

  AMS fornisce un rapporto mensile sull'assistenza che riassume i principali parametri prestazionali di AMS, tra cui un riepilogo e approfondimenti, metriche operative, risorse gestite, aderenza agli accordi sul livello di servizio AMS (SLA) e metriche finanziarie relative alla spesa, ai risparmi e all'ottimizzazione dei costi. I report vengono forniti dal cloud service delivery manager (CSDM) di AMS assegnato all'utente.

- Gestione delle richieste di assistenza:

  Per richiedere informazioni sull'ambiente gestito, su AMS o sulle offerte di AWS servizi, invia le richieste di servizio utilizzando la console AMS. Puoi inviare una richiesta di servizio per domande «pratiche» su AWS servizi e funzionalità o per richiedere servizi AMS aggiuntivi.

- Service Desk:

  AMS si occupa della progettazione delle operazioni con dipendenti Amazon a tempo pieno per soddisfare le richieste non automatizzate, tra cui la gestione degli incidenti, la gestione delle richieste di assistenza e la gestione delle modifiche. Il Service Desk è operativo 24 ore su 24, 365 giorni all'anno.

- Risorse designate:

  A ogni cliente viene assegnato un Cloud Service Delivery Manager (CSDM) e un Cloud Architect (CA).

  - CSDMs può essere contattato direttamente. Eseguono revisioni dei servizi e forniscono report e approfondimenti in tutte le fasi dell'implementazione, della migrazione e del ciclo di vita operativo. CSDMs effettuano revisioni aziendali mensili e forniscono informazioni

dettagliate come la spesa finanziaria, i consigli per il risparmio sui costi, l'utilizzo dei servizi e la rendicontazione dei rischi. Esaminano in modo approfondito le statistiche sulle prestazioni operative e forniscono raccomandazioni sulle aree di miglioramento.

- CAs possono essere contattati direttamente e forniscono competenze tecniche per aiutarti a ottimizzare l'uso del AWS cloud. Tra le attività di CA figurano, ad esempio, la selezione dei carichi di lavoro da migrare, l'assistenza nell'onboarding di account e carichi di lavoro aggiuntivi, il ruolo di responsabile tecnico in attività operative come giornate di gioco, test di disaster recovery, gestione dei problemi e consulenza tecnica per ottenere il massimo da AMS e. AWS CAs promuove discussioni tecniche a tutti i livelli dell'organizzazione e fornisce assistenza nella gestione degli incidenti, nell'individuazione di compromessi, nella definizione delle migliori pratiche e nella mitigazione dei rischi tecnici.

- Modalità sviluppatore:

  Questa funzionalità consente di iterare rapidamente i progetti e le implementazioni dell'infrastruttura all'interno degli account configurati con AMS [1] consentendo l'accesso diretto al servizio AWS e APIs alla console AWS oltre all'accesso al processo di gestione delle modifiche AMS. La gestione delle risorse fornite o configurate con autorizzazioni in modalità sviluppatore al di fuori del processo di gestione delle modifiche è responsabilità dell'utente (vedi «Gestione automatizzata e self-service del provisioning»). Le risorse fornite tramite il processo di gestione delle modifiche AMS sono supportate come altri carichi di lavoro forniti per la gestione delle modifiche su AMS.

- Supporto AWS:

  I clienti AMS possono scegliere il livello di AWS Support di cui hanno bisogno per completare il loro piano AMS Operations. Gli account registrati ad AMS possono essere sottoscritti a Business Support o Enterprise Support. Per ulteriori informazioni sulle differenze tra i piani di supporto, consulta AWS Support Plans.

- Account gestito dal cliente:

  Questa funzionalità ti consente di richiedere account AWS all'interno dello stesso ambiente gestito, ma le operazioni correnti dei carichi di lavoro e delle risorse AWS all'interno di tali account sono di tua responsabilità. AMS fornisce account gestiti dai clienti, ma una volta creati gli account, a tali account non vengono fornite altre funzionalità o servizi AMS. AWS non iscriverà gli account gestiti dai clienti al supporto premium di livello aziendale. Sarà tua responsabilità registrare gli account gestiti dai clienti in AWS Support alla tariffa di supporto che scegli.

- Gestione del firewall:

AMS fornisce una soluzione firewall gestita opzionale per Supported Firewall Services, che consente il filtraggio del traffico in uscita legato a Internet per le reti nell'ambiente gestito. Sono esclusi i servizi rivolti al pubblico che non utilizzano l'infrastruttura di rete AWS e il cui traffico va direttamente a Internet. La soluzione combina la tecnologia firewall leader del settore con le funzionalità di gestione dell'infrastruttura AMS per implementare, monitorare, gestire, scalare e ripristinare l'infrastruttura firewall.

Quando entri a bordo di AMS, ricevi un elenco completo della tua infrastruttura di rete AMS. Per ottenere in qualsiasi momento un elenco aggiornato dei servizi in esecuzione a supporto della tua infrastruttura AMS, invia una richiesta di servizio specificando le informazioni che desideri. Per richiedere una modifica al design della rete, crea una richiesta di servizio che descriva le modifiche che desideri apportare, ad esempio aggiungendo un VPC o richiedendo una modifica delle regole del gruppo di sicurezza.

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.

Matrice di responsabilità AMS (RACI)

> **Note**
>
> Per adempiere ai propri obblighi in modo tempestivo, AWS Managed Services (AMS) potrebbe richiederti input per decidere una linea d'azione appropriata. AMS contatterà il contatto designato per il cliente per tutti questi chiarimenti e input. AMS si aspetta una risposta a tali domande entro 24 ore lavorative. In caso di mancata risposta entro 24 ore lavorative, AMS può scegliere un'azione per conto dell'utente.

La matrice AMS responsabile, responsabile, consultata e informata, o RACI, attribuisce la responsabilità principale al cliente o ad AMS per una serie di attività.

AMS gestisce la tua infrastruttura AWS. La tabella seguente fornisce una panoramica delle responsabilità del cliente e di AMS per le attività nel ciclo di vita di un'applicazione eseguita all'interno di un ambiente gestito AMS.

AMS non è responsabile per nessuna delle seguenti attività relative agli account gestiti dal cliente o all'infrastruttura in esecuzione al loro interno; pertanto questo RACI non è applicabile.

- R sta per parte responsabile che fa il lavoro per raggiungere l'obiettivo.
- C sta per consultato; una parte i cui pareri vengono richiesti, in genere in qualità di esperti in materia, e con la quale esiste una comunicazione bilaterale.
- I sta per informato; una parte che viene informata sui progressi, spesso solo al completamento del compito o del risultato.
- Il provisioning self-service si riferisce alle risorse fornite dal cliente in modalità self-service tramite l' AWS API o la console, tra cui Developer Mode e Self-Service Provisioned Services.

> **Note**
>
> Alcune sezioni contengono «R» sia per AMS che per i clienti. Questo perché, nel modello di responsabilità AWS condivisa, sia AMS che i clienti assumono la responsabilità congiunta di rispondere ai problemi dell'infrastruttura e delle applicazioni.

Per fornire funzionalità di provisioning self-service, AMS ha creato ruoli IAM elevati con limiti di autorizzazione per limitare le modifiche non intenzionali derivanti dall'accesso diretto al servizio. AWS I ruoli non impediscono tutte le modifiche e l'utente è responsabile del rispetto dei controlli interni e della conformità e della verifica che tutti i AWS servizi utilizzati soddisfino le certificazioni richieste. La chiamiamo modalità Self-Service Provisioning. Per i dettagli sui requisiti di AWS conformità, consulta AWS Conformità.

Per le risorse fornite in modalità self-service, AMS fornisce la gestione degli incidenti, i controlli investigativi e i guardrail, 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.

Attività	Cliente	AWS Managed Services (AMS)
Ciclo di vita delle applicazioni		
Sviluppo di applicazioni	R	I

Attività	Cliente	AWS Managed Services (AMS)
analisi e progettazione dei requisiti dell'infr astruttura applicativa	R	C
Progettazione e ottimizzazione per stack AMS non standard	R	C
Progettazione e ottimizzazione dello stack standard AMS	I	R
Distribuzione delle applicazioni	R	C
Implementazione dell'infrastruttura AWS	C	R
Monitoraggio dell'applicazione	R	I
Test/ottimizzazione delle applicazioni	R	I
Linee guida per l'ottimizzazione dell'infrastruttur a AWS	I	R
Monitoraggio dell'infrastruttura AWS	I	R
Risolvi e risolvi i problemi relativi alle applicazi oni	R	C
Risolvi e risolvi i problemi di rete AWS	C	R
Risolvi e risolvi i problemi del sistema operativo e dell'infrastruttura	C	R
Provisioning self-service	R	C
Integrazione di applicazioni e ITSM		
Integrazione delle applicazioni con AWS Service Offerings	R	C

Attività	Cliente	AWS Managed Services (AMS)
Integrazione ITSM con l'interfaccia AWS Managed Services	R	C
Reti		
Ambiente gestito Configurazione e configura zione di VPC e VPC	C	R
Assegna uno spazio di indirizzamento privato per VPCs (ad esempio /16)	R	C
Configurazione e utilizzo di servizi gestiti non AWS, gestiti dal cliente Firewalls/Proxy/Ba stions/HOSTs	R	C
Configurazione e utilizzo di AWS Security Groups/NAT/Customer Bastions/NACL all'inter no dell'ambiente gestito	I	R
Configurazione e implementazione di reti (ad es. DirectConnect) all'interno della rete del cliente	R	C
Configurazione e implementazione della rete all'interno dell'ambiente gestito	C	R
Configurazione dell'ambiente gestito		
Definire le impostazioni di Auto Scaling predefinite per i modelli Stack di base	I	R
Consiglia l'ottimizzazione del RI	C	R
Acquista capacità RI e PIOP	R	C

Attività	Cliente	AWS Managed Services (AMS)
Rimuovi la capacità quando la capacità è esaurita (se supportata dall'applicazione del cliente)	C	R
Creazione/aggiornamento di informazioni specifiche sui clienti AWS per AWS Managed Services	C	R
Configurazione S3	C	R
Fornitura self-service	R	C
Configurazione Glacier	C	R
Definire la politica di archiviazione	R	C
Configurazione della politica di archiviazione	C	R
Selezione della finestra di manutenzione per i clienti	R	I
Gestione di AWS RDS		
Monitora lo stato della source/replica/RO replica	I	R
Identifica l'RCA del failover di origine	I	R
Configurazione automatica delle istantanee (backup)	C	R
Provisioning self-service	R	C
Coordina e pianifica la gestione delle patch del motore DB	C	R
Provisioning self-service	R	C

Attività	Cliente	AWS Managed Services (AMS)
Consiglia lo storage DB e la capacità PIOP	C	R
Provisioning self-service	R	C
Consiglia il dimensionamento delle istanze per l'esecuzione dei database	C	R
Provisioning self-service	R	C
Consiglia l'ottimizzazione del RI per l'ambiente gestito	C	R
Provisioning self-service	R	C
Monitoraggio delle prestazioni RDS () CloudWatch	C	R
Fornitura self-service	R	C
Configurazione dell'abbonamento agli eventi RDS (SNS)	C	R
Provisioning self-service	R	C
Configurazione del gruppo di sicurezza RDS	C	R
Fornitura self-service	R	C
Configurazione del motore RDS parameter/ option	R	C
Design della tabella DB	R	I
Indicizzazione DB	R	I
Analisi dei log DB	R	I
Gestione delle modifiche AMS		

Attività	Cliente	AWS Managed Services (AMS)
Creazione di clienti RFCs (ad esempio accesso alle risorse, creating/updating/deleting managed stacks, deploying/updating applicazioni, modifiche alla configurazione delle offerte di AWS servizi)	R	I
Approvazione del cliente RFCs	I	R
Creazione di AWS Managed Services RFCs (ad esempio accesso alle risorse, creazione di risorse per conto del cliente, applicazione di aggiornamenti al sistema operativo come parte della gestione delle patch)	I	R
Approvazione non automatizzata RFCs	R	I
Invio di una richiesta per nuovi tipi di modifica	R	C
Creazione di nuovi tipi di modifica	I	R
Manutenzione del calendario delle modifiche alle applicazioni	R	C
Avviso della prossima finestra di manutenzione	I	R
AWS Service Catalog		
Crea portafogli e prodotti	R	I
Distribuisci prodotti agli utenti finali	R	I
Crea tag e una libreria di opzioni di tag	R	C
Condivisione di portafogli e prodotti con gli utenti finali	R	I
Rivedi e aggiorna portafogli e prodotti	R	I

Attività	Cliente	AWS Managed Services (AMS)
Crea e assegna vincoli a portafogli e prodotti	R	C
Associa Service Actions ai prodotti	R	C
Aggiorna le risorse fornite con una nuova versione del prodotto	R	I
Approvvigionamento		
Aggiunte specifiche del cliente all'AMI di base di AWS Managed Services	R	C
Configura altri tipi di modifica approvati utilizzati per il provisioning dei modelli Stack	C	R
Avvia gli stack gestiti e le risorse AWS associate inviate tramite il processo di gestione delle modifiche AMS o AWS Service Catalog.	I	R
Provisioning self-service	R	I
Install/Update applicazioni personalizzate e di terze parti su istanze fornite tramite il processo di gestione delle modifiche AMS o AWS Service Catalog.	R	I
Provisioning - Architettura Stack		
Fornitura di licenze del sistema operativo (incluse le tariffe di utilizzo per i servizi AWS applicabili, ad esempio EC2 e RDS)	I	R
Provisioning self-service	R	I

Attività	Cliente	AWS Managed Services (AMS)
Definisci i modelli di infrastruttura di base (Stack) per la distribuzione delle applicazioni tramite il sistema di gestione delle modifiche AMS. Provisioning self-service	I	R
	R	I
Creazione di una linea di base approvata 8 AMIs	I	R
Valuta l'inventario delle applicazioni dei clienti e stabiliscine la compatibilità con i modelli di infrastruttura disponibili (Stacks)	R	C
Definisci stack unici che si aggiungono alle offerte di modelli di base	R	C
Registrazione, monitoraggio e gestione degli eventi		
Registrazione dei log delle modifiche dell'infr astruttura AWS	I	R
Registrazione di tutti i log delle modifiche delle applicazioni	R	C
Installazione e configurazione di agenti e script per l'applicazione di patch, sicurezza , monitoraggio, ecc. dell'infrastruttura AWS fornita tramite il processo di gestione delle modifiche AMS. Fornitura self-service	I	R
	R	C
Definisci i requisiti specifici del cliente in materia di monitoraggio e gestione degli incidenti	R	C

Attività	Cliente	AWS Managed Services (AMS)
Configurazione degli avvisi per l'ambiente gestito	I	R
Monitoraggio di tutti gli avvisi configurati da AMS	I	R
Fornitura self-service	R	C
Analisi degli avvisi dell'infrastruttura per la notifica degli incidenti	I	R
Fornitura self-service	R	C
Analisi degli allarmi delle applicazioni	R	C
Gestione degli incidenti		
Notifica in modo proattivo gli incidenti sull'infrastruttura AWS in base al monitoraggio	I	R
Fornitura self-service	R	C
Gestisci i problemi e le interruzioni delle prestazioni delle applicazioni	R	I
Categorizza la priorità degli incidenti	I	R
Fornisci una risposta agli incidenti	I	R

Attività	Cliente	AWS Managed Services (AMS)
Fornisci la risoluzione degli incidenti e il ripristino dell'infrastruttura **Note** SLAs non si applicano alle risorse basate su istanze fornite al di fuori della gestione delle modifiche di AMS, incluse quelle fornite utilizzando il provisioning self-service e la modalità sviluppatore.	C	R
Gestione dei problemi		
Identifica i problemi nell'ambiente gestito	C	R
Esegui RCA per problemi nell'ambiente gestito	C	R
Risoluzione dei problemi nell'ambiente gestito	C	R
Identifica e risolvi i problemi delle applicazioni	R	I
Gestione della sicurezza		
Sicurezza dell'infrastruttura del cliente: and/or definizione delle basi per il processo di conformità alla sicurezza, come stabilito e concordato durante l'onboarding del cliente. Fornitura self-service	C R	R C
Mantenimento di licenze valide per Managed EPS	R	C
Configurare Managed EPS Fornitura self-service	I	R

Attività	Cliente	AWS Managed Services (AMS)
	R	C
Aggiorna Managed EPS	I	R
Fornitura self-service	R	C
Monitoraggio del malware sulle istanze fornite tramite il processo AMS CM.	I	R
Fornitura self-service	R	C
Manutenzione e aggiornamento delle firme dei virus.	I	R
Provisioning self-service	R	C
Correzione delle istanze infette da malware.	C	R
Provisioning self-service	R	C
Gestione degli eventi di sicurezza	C	R
Sicurezza: gestione degli accessi		
Gestisci il ciclo di vita degli utenti e le relative autorizzazioni per i servizi di directory locali, utilizzati per accedere ad AWS Managed Services	R	I
Gestisci sistemi di autenticazione federati per l'accesso dei clienti alla console/ AWS APIs	R	C
Accetta e mantieni la fiducia di Active Directory (AD) da AWS Managed Services AD ad AD gestito dal cliente	R	C

Attività	Cliente	AWS Managed Services (AMS)
Durante l'onboarding, crea ruoli di amministratore IAM multiaccount all'interno di ciascun account gestito	R	C
Proteggi le credenziali AWS root per ogni account	I	R
Definisci le risorse IAM per l'ambiente gestito	C	R
Gestisci le credenziali privilegiate per l'accesso al sistema operativo per gli ingegneri AMS	I	R
Gestisci le credenziali privilegiate per l'accesso al sistema operativo fornite al cliente da AMS	R	I
Risposta agli incidenti di sicurezza: preparazione		
Comunicazioni		
Fornisci ad AMS i dati di contatto per la sicurezza dei clienti da utilizzare durante le notifiche di eventi di sicurezza e le escalation di sicurezza	R	I
Archivia e gestisci i dati di contatto per la sicurezza dei clienti forniti da utilizzare durante gli eventi di sicurezza e le escalation di sicurezza	CI	R
Addestramento		
Fornisci al cliente la documentazione per supportare AMS durante il processo di risposta agli incidenti	I	R

Attività	Cliente	AWS Managed Services (AMS)
Pratica la responsabilità condivisa durante i processi di risposta agli incidenti durante i Security Gamedays	RI	RC
Gestione delle risorse		
Configura la gestione della sicurezza supportat a Servizi AWS per avvisi, correlazione degli avvisi, riduzione del rumore e regole aggiuntive	I	R
Mantieni l'inventario degli asset (AWS risorse) e conosci il valore e la criticità degli asset. Queste informazioni sono utili durante la strategia di contenimento degli incidenti	R	CI
Utilizza i AWS tag per identificare risorse e carichi di lavoro	R	CI
Definisci e configura la conservazione e l'archivi azione dei log	CI	R
Elaborazione sicura delle configurazioni Account AWS, delle politiche e della gestione degli accessi	CI	RC
Risposta agli incidenti di sicurezza - Rileva		
Registrazione, indicatori e monitoraggio		
Configura la registrazione e il monitoraggio per abilitare la gestione degli eventi, ad esempio, e degli account	CI	R
Monitor supportato Servizi AWS per gli avvisi di sicurezza	I	R

Attività	Cliente	AWS Managed Services (AMS)
Implementa e gestisci gli strumenti di sicurezza degli endpoint	CI	R
Monitora il malware sulle istanze utilizzando lo strumento di sicurezza degli endpoint supportat o da AMS	I	R
Informa il cliente degli eventi rilevati tramite messaggistica in uscita	I	R
Invia la notifica e gli eventuali aggiornam enti successivi ai responsabili delle decisioni per account e carichi di lavoro specifici per migliorare i tempi di risposta agli incidenti	R	CI
Definisci, distribuisci e gestisci i servizi di rilevamento standard AMS (ad esempio, Amazon GuardDuty e AWS Config)	CI	R
Registra i registri AWS delle modifiche all'infra struttura	I	RC
Abilita e configura la registrazione e il monitoraggio per abilitare la gestione degli eventi per l'applicazione	R	C
Implementa e gestisci una lista di autorizza zioni, una lista di utenti non autorizzati e rilevamenti personalizzati sui servizi di AWS sicurezza supportati (ad esempio, Amazon) GuardDuty	RCI	R
Segnalazione eventi di sicurezza		
Notifica ad AMS un'attività sospetta o un'indagi ne di sicurezza in corso	R	CI

Attività	Cliente	AWS Managed Services (AMS)
Notifica al cliente gli eventi e gli incidenti di sicurezza rilevati	I	R
Notifica l'evento pianificato che potrebbe attivare il processo di Security Incident Response	R	CI
Security Incident Response - Analizza		
Indagine e analisi		
Esegui la risposta iniziale per l'avviso di sicurezza supportato generato da una fonte di rilevamento supportata	I	RC
Valuta false/true gli aspetti positivi utilizzando i dati disponibili	RI	RC
Genera un'istantanea delle istanze interessate da condividere con il cliente, se necessario	I	R
Esegui attività di analisi forense come la catena di custodia, l'analisi del file system, l'analisi forense della memoria e l'analisi binaria	R	CI
Raccogli i registri delle applicazioni per facilitar e le indagini	R	I
Raccogli dati e registri per facilitare le indagini sugli avvisi di sicurezza	RCI	RC
Partecipa SMEs Servizi AWS alle indagini di sicurezza	CI	R

Attività	Cliente	AWS Managed Services (AMS)
Coinvolgi fornitori di terze parti durante le indagini (ad esempio, per le indagini anti-malware EPS e interagisci con il team di supporto) TrendMicro	RCI	I
Condividi i registri delle indagini fornite dall'assistenza Servizi AWS ai clienti durante un'indagine	I	R
Comunicazione		
Invia avvisi e notifiche dalle fonti di rilevamento AMS per le risorse gestite	I	R
Gestisci avvisi e notifiche per gli eventi di sicurezza delle applicazioni	R	I
Coinvolgi il punto di contatto per la sicurezza dei clienti durante un'indagine su un incidente di sicurezza	R	I
Risposta agli incidenti di sicurezza: contiene		
Strategia ed esecuzione di contenimento		
Decidete in merito all'esecuzione della strategia di contenimento concordata e accettate le conseguenze che potrebbero influire sulla disponibilità dei servizi durante la finestra di contenimento	R	CI
Effettua un backup dei sistemi interessati per ulteriori analisi	CI	R

Attività	Cliente	AWS Managed Services (AMS)
Contenete applicazioni e carichi di lavoro (tramite attività di configurazione o risposta specifiche dell'applicazione)	R	CI
Definisci la strategia di contenimento in base all'incidente di sicurezza e alla risorsa interessa ta	CI	R
Abilita la crittografia e l'archiviazione sicura dei backup point-in-time dei sistemi interessati	CI	R
Esegui le azioni di contenimento supportate per AWS risorse tra cui EC2 istanze, rete e IAM	CI	R
Security Incident Response - Eradicate		
Strategia ed esecuzione di eradicazione		
Definisci le opzioni di eradicazione in base all'incidente di sicurezza e alla risorsa interessa ta dai carichi di lavoro delle applicazioni dei clienti	R	CI
Decidi la strategia di eradicazione concordat a, i tempi di esecuzione dell'eradicazione e le conseguenze	R	CI
Definisci le fasi di eradicazione in base all'incid ente di sicurezza e alla risorsa interessata sui carichi di lavoro gestiti da AMS	CI	R
Elimina e rafforza le AWS risorse, tra cui EC2 istanze, rete ed eliminazione dell'IAM	CI	R

Attività	Cliente	AWS Managed Services (AMS)
Elimina e rafforza le applicazioni e i carichi di lavoro (tramite attività di configurazione o risposta specifiche dell'applicazione)	R	I
Risposta agli incidenti di sicurezza: ripristino		
Preparazione ed esecuzione del ripristino		
Configura i piani e gli obiettivi di backup come richiesto dal cliente	R	I
Rivedi i piani di backup per ripristinare i carichi di lavoro gestiti da AMS	CI	R
Esegui attività di ripristino dei backup per le risorse supportate Servizi AWS	I	R
Esegui il backup dell'applicazione del cliente, della configurazione dell'APP e delle impostazioni di distribuzione e rivedi i piani di backup per ripristinare le applicazioni e i carichi di lavoro dei clienti dopo l'incidente	R	I
Ripristina le applicazioni e i carichi di lavoro dei clienti (tramite passaggi di ripristino specifici dell'applicazione)	R	I
Risposta agli incidenti di sicurezza: rapporto successivo all'incidente		
Segnalazione successiva all'incidente		
Se necessario, condividete le lezioni apprese e le azioni da intraprendere con il cliente dopo l'incidente	I	R
Gestione delle patch [9]		

Attività	Cliente	AWS Managed Services (AMS)
Monitora gli aggiornamenti applicabili al sistema operativo supportato e al software preinstallato con il sistema operativo supportato per le EC2 istanze. Provisioning self-service	I	R
	R	C
Notifica al cliente gli aggiornamenti imminenti (valido solo per AMS Standard Patch)	I	R
Escludi determinati aggiornamenti (and/or determinati stack) dalle attività di patching	R	I
Definisci le finestre di manutenzione, le pianificazioni predefinite e personalizzate e altri parametri (ad esempio la durata della finestra di manutenzione) per applicare le patch (si applica a AMS Patch) (Solo Orchestrator)	R	I
Definisci linee di base di patch personalizzate per filtrare ed escludere patch specifiche (si applica solo a AMS Patch Orchestrator)	R	I
Etichetta le istanze per associarle a finestre di manutenzione personalizzate e Patch Baseline (si applica solo ad AMS Patch Orchestrator)	R	I
Monitora lo stato delle patch delle risorse ed evidenzia i sistemi non aggiornati nella revisione aziendale mensile.	C	R

Attività	Cliente	AWS Managed Services (AMS)
Applicare una patch al sistema operativo Windows e ai pacchetti Microsoft installati sul sistema operativo che sono regolati da Windows Update	I	R
Provisioning self-service	R	-
Applicazioni installate con patch, software o dipendenze delle applicazioni non gestite da Windows Update	R	I
Provisioning self-service	R	-
Applicate una patch al sistema operativo Linux e a qualsiasi pacchetto abilitato alla gestione dal gestore di pacchetti nativo del sistema operativo (ad esempio Yum, Apt, Zypper)	I	R
Provisioning self-service	R	-
Applicate patch alle applicazioni installate, al software o alle dipendenze delle applicazioni non gestite dal gestore di pacchetti nativo del sistema operativo Linux	R	I
Provisioning self-service	R	-
Gestione della continuità		
Specificare i piani di backup	R	I
Esegui i backup in base alla pianificazione.	I	R
Provisioning self-service	R	C
Convalida dei backup	R	I

Attività	Cliente	AWS Managed Services (AMS)
Richiedi attività di ripristino dei backup	R	I
Esegui attività di ripristino dei backup.	I	R
Fornitura self-service	R	C
Ripristina gli stack interessati e. VPCs	I	R
Fornitura self-service	R	C
Ripristina l'applicazione personalizzata/di terze parti interessata	R	C
Creazione di report		
Prepara e distribuisci un rapporto di assistenza mensile	I	R
AMS attivo AWS Outposts	R	I
Configura e recupera la cronologia degli audit delle API su richiesta (CloudTrail).	I	R
Provisioning self-service	R	I
Fornisci l'accesso alla cronologia degli incidenti tramite AWS Managed Services Interface	I	R
Fornisci l'accesso alla cronologia delle modifiche tramite AWS Managed Services Interface.	I	R
Fornitura self-service	N/D	N/D
Gestione delle richieste di assistenza		
Richiedi informazioni utilizzando le richieste di servizio	R	I

Attività	Cliente	AWS Managed Services (AMS)
Rispondi alle richieste di assistenza	I	R
Firewall gestito		
Richiedi l'implementazione di un firewall gestito da AMS	R	I
Progettazione e ottimizzazione dell'architettura firewall gestita da AMS	I	R
Implementazione dell'infrastruttura AWS e dell'appliance Firewall gestita da AMS	I	R
Fornitura di licenze Firewall (incluse le tariffe di utilizzo per i servizi AWS applicabili, ad es. EC2)	R	I
Definisci l'elenco di domini consentiti predefinito	I	R
Richiesta di aggiunta, modifica ed eliminazione di elenchi di autorizzazioni e politiche di sicurezza personalizzati	R	I
Configurazione degli avvisi per AMS Managed Firewall	I	R
Monitoraggio di tutti gli avvisi configurati da AMS Managed Firewall	I	R
Esegui i backup della configurazione del firewall	I	R
Richiedi attività di ripristino dei backup	R	I
Aggiorna le risorse assegnate con una nuova versione del prodotto	I	R

Attività	Cliente	AWS Managed Services (AMS)
Registrazione dei log del firewall gestiti da AMS	I	R
Inoltra i log dal firewall gestito da AMS a CloudWatch	I	R
Richiedi modifiche alla configurazione nel firewall gestito da AMS	R	I
Approva le modifiche alla configurazione nel firewall gestito da AMS	I	R
Esegui modifiche alla configurazione nel firewall gestito da AMS	I	R

[8] AMS fornisce AMIs EC2 solo Amazon

[9] AMS è responsabile della fine del ciclo di vita OSes solo quando il cliente firma un contratto di assistenza esteso con il fornitore del sistema operativo

Componenti di base dell'ambiente AMS

Multi-Account Landing Zone

Questa è una stima dei componenti e dei costi potenziali dell'infrastruttura negli account principali. Questo non include altri costi come larghezza di banda, monitoraggio CloudWatch dettagliato, registrazione, allarmi, Route53, Amazon S3, Simple Notification Service (Amazon SNS), istantanee o istanze Amazon riservate. EC2

Paghi per i componenti richiesti dall'infrastruttura di landing zone AWS gestita da AMS. Secondo le stime, il costo di un semplice ambiente di landing zone con più account AMS ammonta a 2.450 dollari al mese e 50 dollari per un semplice account applicativo.

Per informazioni sui prezzi, consulta i prezzi di AWS.

Componenti ambientali di base

Componente	Est. Costo	Descrizione
Gestione dell'account	$60	Un account AWS Organizations Management; crea e gestisce finanziariamente gli account dei membri. Contiene il framework AWS Landing Zone (ALZ), i set di stack di configurazione degli account e le policy di controllo dei servizi AWS Organization ()SCPs. • Directory Service: $35 • CloudTrail: $7 • CloudWatch: $6 • Altri: $12
Account di servizi condivisi	2000$	Contiene l'infrastruttura e le risorse necessarie per la gestione degli accessi (ad esempio, Active Directory), la gestione della sicurezza degli endpoint (Trend Micro) e i bastioni (SSH/RDP); la stima è di 2400 USD al mese. Questa stima non include il costo delle licenze Trend Micro. • EC2: 800$ (con il numero minimo di Bastioni) • RDS: $300 (PER PERSONA) • VPC (endpoint): $400 • Servizio Directory: $300 • CloudWatch: $100 • GuardDuty : $15 • Secrets Manager: $10 • Trasferimento dati: $10 • Config: $10 • Altri: $45
Account di rete	$350	L'hub centrale per il routing di rete tra gli account AMS, la rete locale e il traffico in uscita verso Internet. Inoltre, contiene bastioni DMZ pubblici (il punto di ingresso per

Componente	Est. Costo	Descrizione
		gli ingegneri AMS per accedere agli host nell'ambiente AMS). Il prezzo può aumentare in base al traffico che attraversa Transit Gateway e Direct Connect. • EC2: $250 (Bastions) • VPC: $80 • Altri: $20
Account Log Archive	$20	Un bucket S3 con copie dei file di log di AWS CloudTrail e AWS Config da ogni account dell'ambiente AMS. I costi aumentano man mano che vengono raccolti più log. • S3: $10 • CloudWatch: $5 • Altri: $5
Account di sicurezza	$20	L'hub centrale per le operazioni relative alla sicurezza e il punto principale per l'incanalamento di notifiche e avvisi verso i servizi del piano di controllo AMS. Inoltre, ospita l'account di gestione Amazon Guard Duty. I costi aumentano man mano che più eventi vengono analizzati utilizzando Amazon GuardDuty. • CloudWatch: $15 • Altri: $5

Single-Account Landing Zone

La tabella seguente elenca i componenti di un esempio di infrastruttura gestita da AMS.

Componenti di base dell'ambiente, ultimo aggiornamento 09/07/2020

Nome	Tipo di istanza	Sistema operativo	Numero di componenti	
mc-eps-dsm	m5.large	Linux	2	
mc-management	m5.large	Windows	2	
mc-bastion-dmz-ssh	m5.large	Linux	2	
mc-bastion-customer-rdp	m5.large	Windows	2	
mc-eps-relay	m5.large	Linux	2	
servizi di directory	N/D	N/D		
componenti aggiuntivi	N/D	N/D		

Per informazioni sui prezzi, consulta la pagina dei prezzi di AWS.

Limiti dell'account AMS

Esistono tre tipi distinti di limiti da considerare all'interno della landing zone multi-account AMS: limiti delle API AMS, limiti delle risorse AMS e limiti AWS.

Esistono due tipi distinti di limiti da considerare all'interno della landing zone AMS con account singolo: i limiti delle API AMS e i limiti AWS.

Limiti delle API degli account AMS

Questa sezione descrive i limiti a livello di account dopo i quali AWS Managed Services (AMS) limita il servizio API AMS SKMS. Ciò significa che se chiami una delle chiamate elencate APIs più di 10 volte al secondo, una delle chiamate viene «limitata» (ricevi un). `ThrottleException` In rare situazioni, una dipendenza esterna o derivante potrebbe limitare l'API AMS e quindi AMS potrebbe limitare le chiamate API a una velocità probabilmente inferiore.

> **Note**
>
> Per informazioni sull'API AMS SKMS, scarica il riferimento tramite la scheda Report della console AWS Artifact.

Per ogni API AMS SKMS elencata, l'operazione viene limitata dopo 10 TPS (transazioni al secondo):

- `GetStack`
- `GetSubnet`
- `GetVpc`
- `ListAmis`
- `ListStackSummaries`
- `ListSubnetSummaries`
- `ListVpcSummaries`

Limiti delle risorse dell'account AMS multi-account landing zone

I limiti delle risorse dell'account si riferiscono agli account VPCs e alle sottoreti delle applicazioni AMS multi-account landing zone.

Limiti delle risorse dell'account dell'applicazione

È previsto un limite flessibile di 50 account applicativi per organizzazione. Se hai un caso d'uso per più di 50 account applicativi, contatta il tuo responsabile della fornitura dei servizi cloud (CSDM) per inoltrare i tuoi requisiti.

VPCs e i limiti delle risorse delle sottoreti

È previsto un limite minimo di 10 VPCs per account applicativo all'interno della regione AWS predefinita per l'organizzazione.

Ogni VPC può avere da 1 a 10 livelli di sottorete privati distribuiti su 2 o 3 zone di disponibilità. Inoltre, ogni VPC può avere da 0 a 5 livelli di sottorete pubblici distribuiti su 2 o 3 zone di disponibilità. Se hai requisiti che superano questi limiti, informa il tuo CSDM o Cloud Architect per esaminare il tuo caso d'uso.

Rapporto tra applicazione della landing zone multi-account AMS

Nella landing zone multi-account AMS è supportato un account per applicazione; tuttavia, ogni account Application ha un costo contenuto e all'utente viene addebitato il numero di connessioni al Transit Gateway all'ora e la quantità di traffico che attraversa il AWS Transit Gateway. Pertanto, maggiore è la separazione delle applicazioni negli account o maggiori sono VPCs i costi.

Per ridurre i costi e garantire comunque un'adeguata separazione delle mansioni, AMS consiglia di 1) raggruppare le candidature per team con processi aziendali strettamente collegati e 2) di non combinare applicazioni che si trovano in fasi diverse (produzione e non produzione) o gestite da team diversi. In questo modo, avrete meno account, la gestione degli accessi e la separazione delle funzioni saranno più semplici e i costi del traffico potrebbero essere mitigati.

Ad esempio: un'azienda ha in produzione un'applicazione di trading e un'applicazione di gestione del portafoglio, entrambe le applicazioni sono gestite dal team IT di Investments e scambiano molto traffico tra loro. In questo scenario, l'azienda può trarre vantaggio dal raggruppamento di entrambe le applicazioni nello stesso account e nello stesso VPC, poiché il team IT di Investments non dovrà richiedere l'accesso a più account applicativi e l'azienda risparmierà sui costi di traffico. In questo caso, l'azienda dovrebbe creare un altro account per le stesse applicazioni in fase di sviluppo e fornire l'accesso al team di sviluppo.

In un altro scenario, l'azienda ha in produzione un'applicazione Payroll e un'applicazione Accounting, gestite rispettivamente dai team IT delle risorse umane e IT per la contabilità. Sebbene l'applicazione Payroll debba scambiare informazioni con l'applicazione Accounting, consigliamo di separare entrambe le applicazioni in account diversi, uno per team, e di stabilire una connessione tra le due applicazioni VPCs utilizzando l'account Networking. In questo modo, l'azienda eviterà che il team IT delle Risorse Umane richieda modifiche che influiscano sull'infrastruttura delle applicazioni di contabilità, di cui non sarebbe a conoscenza.

Suggerimenti su come raggruppare gli account in unità organizzative (OUs). Un'unità organizzativa è un meccanismo di raggruppamento logico che consente di classificare (raggruppare) gli account e applicare politiche e configurazioni in base a tali gruppi. L'approccio consigliato per la creazione OUs consiste nel basarli su politiche che devono essere applicate a un gruppo specifico di account, non sulla gerarchia interna dei team all'interno della struttura di reporting. Un'unità organizzativa non è equivalente all'unità organizzativa di Active Directory e il tentativo di replicare la struttura dell'unità organizzativa AD AWS Organizations è sconsigliato e comporta una struttura operativa difficile da mantenere. and/or

AWS limiti dell'account

AWS i limiti degli account si applicano ai tuoi account AWS Managed Services (AMS). Il metodo più semplice per determinare i limiti predefiniti e correnti per i AWS servizi consiste nell'utilizzare AWS Service Quotas. AMS consiglia di ridimensionare correttamente i limiti dei singoli servizi alla dimensione appropriata per eseguire il/i servizio/i nell'account. I limiti agiscono come barriere protettive per proteggere gli account in termini di sicurezza e riduzione dei costi. Se desideri aumentare un limite specifico, invia una richiesta di assistenza ad AMS e AMS Operations aumenterà il limite per tuo conto. Ad esempio, il limite (o quota) predefinito per le istanze RDS è 40; se il carico di lavoro richiede 50 istanze RDS, invia una richiesta di servizio ad AMS Operations per innalzare il limite al valore necessario.

Obiettivi del livello di servizio AMS (SLOs)

La tabella seguente descrive gli obiettivi del servizio AWS Managed Services (AMS). I Service Level Agreement (SLAs) per altri aspetti del servizio AMS, inclusa la gestione degli incidenti, sono trattati nel documento SLA condiviso con te al momento della sottoscrizione ad AMS. Per ulteriori informazioni, rivolgiti al tuo CSDM.

Obiettivi del livello di servizio AMS

Funzionalità	Indicatore di prestazione (PI)	Plus (Business Days, M-F 8AM to 6PM local time)	premio (Calendar Days, 24 x 7)
Gestione delle modifiche	Tempo impiegato per programmare o rifiutare in modo automatico RFCs	<=30 min	<=30 minuti
	Ora di inizio della pianificazione RFCs rispetto all'ora di esecuzione pianificata	<=1 min	<=1 min
	Tempo impiegato per la approve/reject modalità non	<=48 ore	<=24 ore

Funzionalità	Indicatore di prestazione (PI)	Plus (Business Days, M-F 8AM to 6PM local time)	premio (Calendar Days, 24 x 7)
	automatica RFCs, disponibile nel catalogo CT		
	Tempo impiegato per la approve/reject modalità non automatica RFCs non disponibile nel catalogo CT	<=5 giorni	<=5 giorni
Gestione dei problemi	Tempo impiegato per completare l'analisi della causa principale (RCA)	<= 10 giorni	<=10 giorni
Gestione delle richieste di assistenza	Tempo di risposta per la prima risposta e per ogni risposta successiva	<=8 ore	<=4 ore

AWS Servizi supportati

AWS Managed Services (AMS) fornisce servizi di supporto alla gestione operativa per i seguenti AWS servizi. Ogni AWS servizio è distinto e, di conseguenza, il livello di gestione operativa e il supporto di AMS varia a seconda della natura e delle caratteristiche del AWS servizio sottostante. I AWS servizi specifici sono raggruppati in base alla complessità e alla portata del servizio di supporto alla gestione operativa fornito da AMS.

> **Note**
>
> I tre gruppi, A, B e C, indicano i prezzi come percentuale della spesa mensile totale per account per il servizio AMS, in base al piano di supporto (Plus o Premium), per i clienti AMS

prima del 16 marzo 2021. I clienti AMS che hanno effettuato l'onboarding dopo il 16 marzo 2021 devono inviare una richiesta di servizio per ulteriori informazioni sui prezzi. Il gruppo A non indica alcun costo aggiuntivo. Il gruppo B indica un costo aggiuntivo del 12% (Plus) o del 18% (Premium). Il gruppo C indica un costo aggiuntivo del 25% (Plus) o del 42% (Premium).
Una stella (*) indica i servizi che vengono implementati in un ambiente gestito da AMS da un cliente che utilizza la AWS console e. APIs Per ulteriori dettagli sulle responsabilità del cliente in caso di fornitura e configurazione dei servizi in AWS Managed Services (AMS) Caratteristiche del piano operativo AMS Advanced questo modo, consulta «Gestione automatizzata e self-service del provisioning».
Due stelle (**) indicano che Amazon EC2 on AWS Outposts verrà fatturato come servizio del Gruppo B; tutte le altre risorse ospitate su Amazon AWS Outposts verranno fatturate alla tariffa standard.

Servizi supportati AWS

Gruppo A	Gruppo B	Gruppo C
Amazon Alexa for Business* Amazon Managed Streaming for Apache Kafka* Amazon CloudFront Amazon Elastic File System Amazon Glacier Amazon Simple Storage Service AWS Amplify* AWS AppMesh* AWS Auto Scaling AWS Backup AWS CloudFormation AWS Compute Optimizer AWS Global Accelerator* AWS Identity and Access Management AWS License Manager* AWS Management Console AWS Marketplace AWS Lake Formation*	Amazon API Gateway* Amazon AppStream* Amazon Athena* Amazon Bedrock* Amazon CloudSearch* Amazon Cognito* Amazon Comprehend* Amazon Connect* Amazon Document DB (with MongoDB compatibility)* Amazon DynamoDB* Amazon EC2 Container Registry (ECR)* Amazon Elastic Container Service (ECS) on AWS Fargate* Amazon Elastic Kubernetes Service (EKS) on Fargate* Amazon Elemental MediaConvert* Amazon Elemental MediaPackage*	Amazon Aurora Amazon CloudWatch Amazon Elastic Block Store (EBS) Amazon Elastic Compute Cloud** Amazon Elastic Load Balancing (classic, application, and network; not gateway) Amazon ElastiCache Amazon OpenSearch Service Amazon GuardDuty Amazon Macie Amazon Redshift Amazon Relational Database Service Amazon Route 53 Amazon Route 53 Resolver DNS Firewall Amazon Simple Email Service

Gruppo A	Gruppo B	Gruppo C
AWS Well Architected Tool* VM Import/ Export*	Amazon Elemental MediaStore* Amazon Elemental MediaTailor* Amazon Elastic MapReduce* AmazonEventBridge* Amazon Forecast* Amazon FSx* Amazon Inspector* Amazon Kendra* Amazon Kinesis Analytics* Amazon Kinesis Data Stream* Amazon Kinesis Firehose* Amazon Kinesis Video Streams* Amazon Lex* Amazon Managed Service for Prometheus* Amazon MQ* Amazon Personalize** Amazon Quantum Ledger Database (QLDB)* Amazon QuickSight* Amazon Rekognition* Amazon SageMaker* Amazon SimpleDB* Amazon Simple Workflow* Amazon Textract* Amazon Transcribe* Amazon Translate* Amazon WorkSpaces* AWS AppSync* AWS Audit Manager* AWS Batch* AWS Certificate Manager* AWS CloudEndure* AWS CloudHSM*	Amazon Simple Notification Service Amazon Simple Queue Service Amazon Virtual Private Cloud (VPC) AWS CloudTrail AWS Config AWS Database Migration Service AWS Data Transfer AWS Direct Connect AWS Directory Service AWS Key Management Service AWS Systems Manager (SSM)

Gruppo A	Gruppo B	Gruppo C
	AWS CodeBuild* AWS CodeCommit* AWS CodeDeploy* AWS CodePipeline* AWS DataSync* AWS Elemental MediaLive* AWS Glue* AWS Lambda* AWS MigrationHub* AWS Outposts** AWS Resilience Hub* AWS Secrets Manager* AWS Security Hub* AWS Service Catalog AWS Service Catalog AppRegistry* AWS Transfer for SFTP* AWS Shield* AWS Snowball* AWS Step Functions* AWS Transit Gateway* AWS WAF* AWS X-Ray*	

Se richiedi ad AWS Managed Services di fornire servizi per qualsiasi software o servizio che non è espressamente indicato come supportato di seguito, qualsiasi servizio AWS Managed Services fornito per tali configurazioni richieste dal cliente verrà considerato un «servizio beta» ai sensi dei Termini di servizio.

Configurazioni supportate

Queste sono le configurazioni supportate da AWS Managed Services (AMS):

- Lingua: AMS è disponibile in inglese.
- Servizi firewall:
  - Firewall DNS Amazon Route 53 Resolver
  - Firewall di nuova generazione Palo Alto serie VM

- Software di sicurezza: Deep Security di Trend Micro (richiesto). Marketplace AWS: Trend Micro Deep Security
- Servizi di directory approvati: Microsoft Active Directory (AD)
- AWS Servizi supportati.
- AWS Regioni supportate:

  AMS opera in un sottoinsieme di tutte le AWS regioni; tuttavia, l'AMS API/CLI opera solo nella regione «Stati Uniti orientali (Virginia settentrionale)». Se si esegue l'API di gestione delle modifiche (`amscm`) o l'API di gestione della conoscenza del servizio AMS (`amsskms`)) in una regione diversa dagli Stati Uniti orientali, è necessario aggiungere `--region us-east-1` al comando.

  - 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)
- Amazon machine images (AMIs): AMS fornisce immagini di sicurezza avanzata (AMIs) basate sul benchmark CIS Level 1 per un sottoinsieme di sistemi operativi supportati da AMS. Per trovare sistemi operativi che dispongono di un'immagine di sicurezza avanzata, consulta l'AMS Security User Guide. Per accedere a questa guida AWS Artifact, filtra la scheda Report per AWS Managed Services. Per accedere AWS Artifact, contatta il tuo CSDM o consulta la sezione Getting Started with AWS Artifact.
- Sistemi operativi supportati:

Sistemi operativi supportati (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (data di fine del supporto AMS prevista per il 30 giugno 2026)
- Oracle Linux 9.x, 8.x
- Red Hat Enterprise Linux (RHEL) 9.x, 8.x
- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server per SAP 15 e versioni successive SP3
- Microsoft Windows Server 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

Sistemi operativi supportati () ARM64

- Amazon Linux 2023
- Amazon Linux 2 (data di fine del supporto AMS prevista per il 30 giugno 2026)

- Sistemi operativi End of Support (EOS) supportati:

> **Note**
>
> I sistemi operativi End of Support (EOS) non rientrano nel periodo di supporto generale del produttore del sistema operativo e presentano un rischio maggiore per la sicurezza. I sistemi operativi EOS sono considerati configurazioni supportate solo se gli agenti richiesti da AMS supportano il sistema operativo e...
>
> 1. hai un supporto esteso con il fornitore del sistema operativo che ti consente di ricevere aggiornamenti, oppure
> 2. tutte le istanze che utilizzano un sistema operativo EOS seguono i controlli di sicurezza specificati da AMS nella Advanced User Guide, oppure
> 3. rispettate tutti gli altri controlli di sicurezza compensativi richiesti da AMS.
>
> Nel caso in cui AMS non sia più in grado di supportare un sistema operativo EOS, AMS emette una raccomandazione critica per aggiornare il sistema operativo.
> Gli agenti richiesti da AMS possono includere, a titolo esemplificativo ma non esaustivo: AWS Systems Manager Amazon CloudWatch, l'agente Endpoint Security (EPS) e Active Directory (AD) Bridge (solo Linux).

- Ubuntu Linux 18.04

- SUSE Linux Enterprise Server 15 e SP3 SP4 SP5
- SUSE Linux Enterprise Server per SAP 15 SP2
- SUSE Linux Enterprise Server 12 SP5
- Servizio SUSE Linux Enterprise per SAP 12 SP5
- Microsoft Windows Server 2012/2012 R2
- Red Hat Enterprise Linux (RHEL) :7.x
- Oracle Linux 7.5-7.9

Funzionalità per sistemi operativi non supportati in AMS

Un sistema operativo non supportato è qualsiasi sistema operativo non elencato in. Configurazioni supportate AMS considera le istanze con sistemi operativi non supportati come «configurazioni richieste dal cliente» soggette ai termini del AWS servizio Betas e Previews.

Il seguente set limitato di funzionalità AMS è disponibile per le istanze con sistemi operativi non supportati:

Funzionalità	Note
Gestione degli incidenti	AMS fornisce una risposta agli incidenti.
Gestione delle richieste di assistenza	AMS risponde alle richieste di assistenza.
Richieste di modifica () RFCs	AMS valuta RFCs l'esecuzione. I sistemi operativi non supportati possono influire sulla capacità di esecuzione. RFCs
Monitoraggio	AMS monitora e risponde ai controlli dello stato EC2 del sistema Amazon e ai controlli dello stato delle istanze. I controlli dello stato del sistema includono: perdita di connettività di rete, perdita di alimentazione del sistema, problemi software sull'host fisico e problemi hardware sull'host fisico che influiscono sulla raggiungibilità della rete.

Funzionalità	Note
	I controlli dello stato delle istanze includono: configura zione di rete o di avvio errata, memoria esaurita, file system danneggiato e kernel incompatibile.
Gestione della sicurezza	AMS monitora e risponde ai risultati di Amazon EC2 GuardDuty .
Gestione del Backup	AMS offre la gestione della continuità in AMS Advanced per EC2 l'utilizzo di AWS Backup piani e vault personali zzati con AMS.

Interfacce AMS Advanced

- Console AMS Advanced: utilizzi la console AMS Advanced per creare RFCs, segnalare e rispondere agli incidenti, effettuare richieste di assistenza e trovare informazioni sugli stack esistenti VPCs e sugli stack. In caso di dubbi su cosa fare o se hai bisogno di aiuto con AMS o le tue risorse gestite, crea una richiesta di servizio utilizzando questa interfaccia.
- Console di gestione AWS: Molte AWS console possono essere utili per visualizzare le informazioni AMS, ad esempio:
  - EC2 Console Amazon: da utilizzare per visualizzare le informazioni sull'istanza, inclusi gli indirizzi IP di Bastion, i gruppi Amazon EC2 Auto Scaling e i sistemi di bilanciamento del carico.
  - Conformità AWS Config alle regole Multi-Account Landing Zone: puoi visualizzare lo stato di conformità di tutti i tuoi account e identificare le risorse non conformi.
  - AWS CloudFormation console: Utilizzala per visualizzare le informazioni sullo stack, incluso lo stack IDs (puoi trovare gli stack Amazon RDS e l' IDs istanza Amazon RDS qui e le informazioni sugli eventi).
  - Console Amazon RDS: utilizzala per visualizzare informazioni sugli eventi, ad esempio un post pubblicato su un' WordPress app su un sito nel tuo account. Tieni presente che devi disporre dell'ID dell'istanza Amazon RDS.

  A seconda della modalità del tuo ruolo di accesso, hai diversi livelli di accesso alla console di AWS gestione. Per ulteriori informazioni sulle modalità, consulta Modalità AMS.
- API di gestione avanzata delle modifiche AMS — Lettura/scrittura: utilizza l'API di gestione delle modifiche (API CM) per richiedere aggiunte e modifiche specifiche all'infrastruttura gestita, tra cui il

monitoraggio delle risorse, i log, il backup e le configurazioni delle patch. Inoltre, utilizza questa API per richiedere l'accesso alle risorse, eliminare risorse AMIs, creare e creare profili di istanze IAM. È possibile accedere all'API CM tramite la CLI AMS e. SDKs

- API AMS SKMS — Sola lettura: utilizza questa API per elencare le risorse gestite e ottenere le informazioni necessarie per la segnalazione o la preparazione delle richieste di modifica.
- Supporto API: utilizza l' Supporto API standard per creare e rispondere in modo programmatico a incidenti e richieste di assistenza. Per ulteriori informazioni, consulta Getting Started with. Supporto
- AWS APIs— Sola lettura: l'amministratore IT principale può utilizzare il file AWS APIs per visualizzare tutte le risorse gestite, visualizzare CloudTrail i registri, le informazioni di fatturazione e molte altre funzioni di lettura.

Endpoint VPC AMS

Un endpoint VPC ti consente di connettere privatamente il tuo VPC senza richiedere un gateway Internet. Servizi AWS Le istanze nel VPC non richiedono indirizzi IP pubblici per comunicare con le risorse nel servizio.

Gli endpoint sono dispositivi virtuali. Si tratta di componenti VPC ad alta disponibilità, ridondanti e dimensionati orizzontalmente che consentono la comunicazione tra istanze del VPC e servizi senza comportare alcun rischio di disponibilità o vincolo di larghezza di banda sul traffico di rete. Per saperne di più, consulta VPC Endpoints.

Esistono due tipi di endpoint VPC: endpoint di interfaccia ed endpoint gateway.

- Endpoint gateway: il VPC nell'account ha un endpoint Amazon S3 Gateway abilitato per impostazione predefinita.
- Endpoint di interfaccia: le istanze del tuo ambiente AMS possono comunicare con i servizi supportati senza uscire dalla rete Amazon. Questa opzione è facoltativa per le landing zone con account singolo e per impostazione predefinita non è abilitata nell'account; invia una richiesta di servizio a AMS operations per abilitarla. Tuttavia, per le landing zone con più account, gli endpoint di interfaccia sono abilitati per impostazione predefinita nell'account Shared Services.

  Elenco degli endpoint di interfaccia supportati da AMS:

  - AWS CloudFormation
  - AWS CloudTrail
  - AWS Config

- EC2 API Amazon
- AWS Key Management Service
- Amazon CloudWatch
- CloudWatch Eventi Amazon
- CloudWatch Registri Amazon
- AWS Secrets Manager
- Amazon SNS
- AWS Systems Manager
- AWS Security Token Service

Namespace protetti da AMS

L'elenco dei namespace protetti per AWS Managed Services (AMS). Quando lavori con AWS risorse, evita i conflitti con AMS evitando di utilizzare questi namespace. Per dettagli su altri namespace AWS di servizio, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces.

- `ams-*`(questo è lo standard di denominazione preferito per le nuove risorse)
- `/ams/*`(questo è lo standard di denominazione preferito per le risorse basate sui percorsi)
- `AWSManagedServices*`(questo è lo standard di denominazione preferito per le risorse, laddove CamelCase appropriato)
- `ams*`, `AMS*` e `Ams*`
- `AWS_*` e `aws*`
- `*/aws_reserved/*`
- `CloudTrail*` e `Cloudtrail*`
- `codedeploy_service_role`
- `customer-mc-*`
- `eps` e `EPS`
- `EPSMarketplaceSubscriptionRole`
- `EPSDB*`
- `IAMPolicy*`
- `INGEST*`
- `LandingZone*`

- `Managed_Services*`
- `managementhost`
- `mc*`, `MC*` e `Mc*`
- `MMS*`
- `ms-`
- `NewAMS*`
- `Root*`
- `sentinel*` e `Sentinel*`
- `sentinel.int.`
- `StateMachine*`
- `StackSet-ams*`
- `StackSet-AWS-Landing-Zone`
- `TemplateId*`
- `UnhealthyInServiceBastion`
- `VPC_*`

Prefissi riservati AMS

Gli attributi delle risorse AMS devono rispettare determinati modelli; ad esempio, i nomi dei profili, i nomi, BackupVault i nomi dei tag delle istanze IAM non devono iniziare con i prefissi riservati AMS. Questi prefissi riservati sono:

```
*/aws_reserved/*
ams-*
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc-*
```

```
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion
```

Finestra di manutenzione AMS

La AWS Managed Services Maintenance Window (o Maintenance Window) esegue attività di manutenzione per AWS Managed Services (AMS) e si svolge 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. Questo è per AWS Managed Services (AMS), per eseguire attività di manutenzione per infrastrutture gestite, come l'implementazione di nuovi AMS. AMIs

La finestra di manutenzione è quella in cui AMS applicherà le patch e sei tu a determinare la finestra di manutenzione al momento dell'onboarding. Puoi anche accettare la finestra di applicazione delle patch proposta fornita nella notifica del servizio di patching o suggerire una finestra diversa.

Per istruzioni sulla creazione di una finestra di manutenzione, consulta Finestra di manutenzione.

Risorse informative AMS

AMS fornisce diverse risorse informative per aiutarvi ad avere successo.

- Guida per l'utente di AMS Accelerate: aiuta a comprendere i componenti e le funzionalità forniti da AMS Accelerate e come utilizzarli. Consulta qui le informazioni di base su AMS Accelerate e i dettagli sulle impostazioni predefinite, sulla ricerca di risorse ed esempi pratici. Indice HTML, PDF
- Guida per l'utente di AMS Advanced: aiuta a comprendere i componenti e le funzionalità forniti da AMS Advanced e come utilizzarli. Consulta qui le informazioni di base su AMS Advanced e i dettagli sulle impostazioni predefinite, sulla ricerca di risorse ed esempi pratici. Indice HTML, PDF
- AMS Advanced Application Guide: descrive i passaggi per la distribuzione delle applicazioni nell'infrastruttura AWS Managed Services. Consulta questa pagina per informazioni sulle metodologie e sulle considerazioni relative alla distribuzione e alla manutenzione delle applicazioni. Indice HTML, PDF.
- AMS Advanced Onboarding Guide: descrive i passaggi iniziali per creare l'infrastruttura di base di AWS Managed Services multi-account o single-account landing zone in un account AMS. Consulta qui le informazioni di base, la convalida e le domande relative agli account AMS per prepararti all'onboarding su AMS. Indice HTML, PDF.
- AMS Advanced Change Type Reference: fornisce materiale di riferimento sugli attuali tipi di modifica forniti da AWS Managed Services, inclusi schemi di tipo di modifica ed esempi di procedure dettagliate per ogni tipo di modifica e suggerimenti. Include informazioni generali sui tipi di modifica. Consente di comprendere tutti gli aspetti delle richieste di modifica (RFCs) e dei tipi di modifica AMS (). CTs Consulta questa pagina per informazioni specifiche sui tipi di modifica, inclusi i collegamenti alle informazioni pertinenti. Indice HTML, PDF.
- Riferimento all'API AMS CM (gestione delle modifiche): descrive l'API CM di AWS Managed Services, che fornisce operazioni per la creazione e il monitoraggio delle richieste di modifica e fornisce informazioni sulle risorse gestite da Managed Services. Indice HTML.
- Guide alla sicurezza AMS: descrivi le informazioni di sicurezza proprietarie di AMS.

  Privato; disponibile nella scheda Rapporti AMS nella console AWS Artifact.
- Risorse per sviluppatori AMS: accesso alla CLI e all'SDK AMS, sia per amscm che per amsskms. Per informazioni, consulta https://console.aws.amazon.com/managedservices/.
- YouTube Video AMS: le principali operazioni dei clienti spiegate in video. Guarda i video YouTube didattici di AWS Managed Services.
- Post del blog AMS: informazioni speciali su AWS Managed Services. Consulta i blog di AWS.

Conformità AMS

AMS è stata sottoposta a controlli per i seguenti standard ed è idonea all'uso come parte di soluzioni per le quali è necessario ottenere la certificazione di conformità.

Standard di conformità supportati da AMS

AMS supporta gli standard di AWS conformità. Per ulteriori informazioni sui programmi di AWS conformità, consulta AWS Conformità.

Questi sono gli attuali standard di conformità supportati da AMS.

	FedRAMP: il governo federale degli Stati Uniti si impegna a fornire i propri servizi al popolo americano nel modo più innovativo, sicuro ed economico. Il cloud computing svolge un ruolo fondamentale nel modo in cui il governo federale può raggiungere l'efficienza operativa e innovare su richiesta per portare avanti la propria missione in tutto il paese. Ecco perché oggi molte agenzie federali utilizzano i servizi cloud AWS per elaborare, archiviare e trasmettere i dati del governo federale. Per ulteriori informazioni, consulta FedRAMP.
	HIPAA: AWS ha ampliato il suo programma di conformità all'Health Insurance Portability and Accountability Act (HIPAA) per includere AMS come servizio idoneo all'HIPAA. Se hai un Business Associate Agreement (BAA) con AWS, puoi utilizzare AMS per aiutarti a creare applicazioni conformi a HIPAA. Consulta il white paper incentrato sull'HIPAA per scoprire come sfruttare AMS per l'elaborazione e l'archiviazione di informazioni sanitarie. Per ulteriori informazioni, consulta Compliance HIPAA.
	HITRUST: The Health Information Trust Alliance Common Security Framework (HITRUST CSF) sfrutta standard e regolamenti accettati a livello nazionale e internazionale come GDPR, ISO, NIST, PCI e HIPAA per creare un set completo di controlli di base per la sicurezza e la privacy.

	Per ulteriori informazioni, vedere HITRUST CSF.
	ISO 27001: ISO/IEC 27001:2013 è uno standard di gestione della sicurezza che specifica le migliori pratiche di gestione della sicurezza e controlli di sicurezza completi seguendo le linee guida sulle migliori pratiche 27002. ISO/IEC La base di questa certificazione è lo sviluppo e l'implementazione di un rigoroso programma di sicurezza, che include lo sviluppo e l'impleme ntazione di un sistema di gestione della sicurezza delle informazi oni (ISMS) che definisce il modo in cui AWS gestisce perpetuam ente la sicurezza in modo olistico e completo. Per ulteriori informazioni, consulta 27001:2013. ISO/IEC
	ISO 27017: ISO/IEC 27017:2015 fornisce linee guida sugli aspetti della sicurezza delle informazioni del cloud computing e raccomanda l'implementazione di controlli di sicurezza delle informazioni specifici per il cloud che integrano le linee guida degli standard 27002 e 27001. ISO/IEC ISO/IEC Questo codice di condotta fornisce ulteriori linee guida all'implementazione dei controlli di sicurezza delle informazioni specifiche per i fornitori di servizi cloud. Per ulteriori informazioni, vedere Conformità ISO/IEC 27017:2015.
	ISO 27018: ISO/IEC 27018:2019 è un codice di condotta incentrato sulla protezione dei dati personali nel cloud. Si basa sullo standard di sicurezza ISO/IEC delle informazioni 27002 e fornisce linee guida per l'implementazione dei controlli ISO/IEC 27002 applicabili alle informazioni di identificazione personale (PII) nel cloud pubblico. Fornisce inoltre una serie di controlli aggiuntivi e linee guida associate destinate a soddisfare i requisiti di protezione delle PII nel cloud pubblico non soddisfatti dal set di controlli 27002 esistente. ISO/IEC Per ulteriori informazioni, vedere Conformità ISO/IEC 27018:2019.

ISO 9001: ISO 9001:2015 delinea un approccio orientato ai processi per documentare e rivedere la struttura, le responsab ilità e le procedure necessarie per ottenere un'efficace gestione della qualità all'interno di un'organizzazione. Le sezioni specifich e dello standard contengono informazioni su argomenti quali:

- Requisiti per un sistema di gestione della qualità, compresa la documentazione di un manuale di qualità, il controllo dei documenti e la determinazione delle interazioni tra i processi
- Responsabilità della gestione
- Gestione delle risorse, comprese le risorse umane e l'ambient e di lavoro dell'organizzazione
- Sviluppo dei servizi, comprese le fasi dalla progettazione alla fornitura
- La soddisfazione del cliente
- Misurazione, analisi e miglioramento del SGQ attraverso attività come audit interni e azioni correttive e preventive

Per ulteriori informazioni, consulta Conformità alla ISO 9001:2015.

	PCI: AMS dispone di un attestato di conformità allo standard di sicurezza dei dati (DSS) PCI (Payment Card Industry) versione 3.2 al livello 1 di Service Provider. I clienti che utilizzano prodotti e servizi AWS per archiviare, elaborare o trasmettere i dati dei titolari di carte possono utilizzare AMS per gestire la propria certificazione di conformità PCI DSS. Per ulteriori informazioni sullo standard PCI DSS, incluse le istruzioni su come richiedere una copia del PCI Complianc e Package di AWS, consulta PCI DSS livello 1. È importante sottolineare che è necessario configurare politiche granulari in materia di password in AMS in modo che siano coerenti con gli standard PCI DSS versione 3.2. Per dettagli su quali policy devono essere applicate, consulta Enable PCI Compliance for Your AWS Microsoft AD Directory.
	SOC: I report AMS System & Organization Control (SOC) sono rapporti di esame indipendenti di terze parti che dimostrano come AMS raggiunge i controlli e gli obiettivi chiave di conformit à. Lo scopo di questi report è aiutare te e i tuoi revisori a comprendere i controlli AMS stabiliti per supportare le operazioni e la conformità. Esistono tre tipi di report SOC AMS: • Report AWS SOC 1 - Scarica con AWS Artifact • AWS SOC 2: report su sicurezza, disponibilità e riservatezza - Scarica con AWS Artifact • AWS SOC 3: report su sicurezza, disponibilità e riservatezza Per ulteriori informazioni, consulta SOC Compliance.

Responsabilità condivisa

La sicurezza, inclusa la conformità PCI, è una responsabilità condivisa. È importante comprendere che lo stato di conformità AMS non si applica automaticamente alle applicazioni eseguite nel AWS cloud. È necessario assicurarsi che l'utilizzo dei AWS servizi sia conforme agli standard. Per

maggiori dettagli su come AMS collabora con i clienti in attività specifiche, consulta l'AMSMatrice di responsabilità AMS (RACI).

Immagini di macchine AMS Amazon (AMIs)

AMS produce Amazon Machine Images (AMIs) aggiornate ogni mese per i sistemi operativi supportati da AMS. Inoltre, AMS produce anche immagini di sicurezza avanzata (AMIs) basate sul benchmark CIS di livello 1 per un sottoinsieme di sistemi operativi supportati da AMS. Per scoprire quali sistemi operativi dispongono di un'immagine di sicurezza avanzata, consulta l'AMS Security User Guide, disponibile tramite la pagina AWS Artifact -> Reports (trova l'opzione Reports nel riquadro di navigazione a sinistra) filtrata per AWS Managed Services. Per accedere ad AWS Artifact, contatta il tuo CSDM per ricevere istruzioni o consulta la sezione Getting Started with AWS Artifact.

Per ricevere avvisi quando AMIs vengono rilasciati nuovi AMS, puoi abbonarti a un argomento di notifica di Amazon Simple Notification Service (Amazon SNS) chiamato «AMS AMI». Per maggiori dettagli, consulta Notifiche AMI AMS con SNS.

La convenzione di denominazione AMS AMI è:`customer-ams-<operating system>-<release date> - <version>`. (ad esempio,`customer-ams-rhel6-2018.11-3`)

Usa solo AMS AMIs che iniziano con`customer`.

AMS consiglia di utilizzare sempre l'AMI più recente. Puoi trovare la più recente in uno AMIs dei seguenti modi:

- Cercando nella console AMS, nella AMIspagina.
- Visualizzazione del file CSV AMI AMS più recente, disponibile dal CSDM o tramite questo file ZIP: contenuti AMI AMS 11.2024 e file CSV in un file ZIP.

  Per i file ZIP AMI precedenti, consulta la Cronologia dei documenti.
- Esecuzione di questo `SKMS` comando AMS (richiesto AMS SKMS SDK):

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?
 starts_with(Name,'customer')].[Name,AmiId,CreationTime]" --output table
```

Contenuto AMI AMS aggiunto alla base AWS AMIs, per sistema operativo (OS)

- Linux AMIs:

  - AWS Strumenti CLI
  - NTP
  - Agente del servizio Trend Micro Endpoint Protection
  - Implementazione del codice
  - PBIS/Beyond Trust AD Bridge
  - Agente SSM
  - Yum Upgrade per patch critiche
  - script e software di gestione AMS personalizzati (controllo dell'avvio, del join AD, del monitoraggio, della sicurezza e della registrazione)
- Server Windows: AMIs
  - Microsoft.NET Framework 4.5
  - PowerShell 5.1
  - AWS Strumenti per Windows PowerShell
  - PowerShell Moduli AMS che controllano l'avvio, il join AD, il monitoraggio, la sicurezza e la registrazione
  - Agente del servizio Trend Micro Endpoint Protection
  - Agente SSM
  - CloudWatch Agente
  - EC2Servizio Config (tramite Windows Server 2012 R2)
  - EC2Avvio (Windows Server 2016 e Windows Server 2019)
  - EC2LaunchV2 (Windows Server 2022 e versioni successive)

Basato AMIs su Linux:

- Amazon Linux 2023 (ultima versione secondaria) (AMI minima non supportata)
- Amazon Linux 2 (ultima versione secondaria)
- Amazon Linux (2ARM64)
- Red Hat Enterprise 7 (ultima versione secondaria)
- Red Hat Enterprise 8 (ultima versione secondaria)
- Red Hat Enterprise 9 (ultima versione secondaria)
- SUSE Linux Enterprise Server 15 SP6

- Ubuntu Linux 18.04
- Ubuntu Linux 20.04
- Ubuntu Linux 22.04
- Ubuntu Linux 24.04
- Amazon Linux: per una panoramica del prodotto, informazioni sui prezzi, informazioni sull'utilizzo e informazioni di supporto, consulta Amazon Linux AMI (HVM /64-bit) e Amazon Linux 2.

  Per ulteriori informazioni, consulta Amazon Linux 2 FAQs.
- RedHat Enterprise Linux (RHEL): per una panoramica del prodotto, informazioni sui prezzi, informazioni sull'utilizzo e informazioni di supporto, consulta Red Hat Enterprise Linux (RHEL) 7 (HVM).
- Ubuntu Linux 18.04: per una panoramica del prodotto, informazioni sui prezzi, informazioni sull'utilizzo e informazioni di supporto, consulta Ubuntu 18.04 LTS - Bionic.
- SUSE Linux Enterprise Server per applicazioni SAP 15: SP6
  - Esegui i seguenti passaggi una volta per account:
    1. Passare alla Marketplace AWS.
    2. Cerca il prodotto SUSE 15 SAP.
    3. Scegli Continua per abbonarti.
    4. Scegli Accetta i termini.
  - Completa i seguenti passaggi ogni volta che devi lanciare una nuova istanza di SUSE Linux Enterprise Server for SAP Applications 15 SP6:
    1. Nota l'ID AMI per l'AMI SUSE Linux Enterprise Server for SAP Applications 15 sottoscritta.
    2. Crea una distribuzione | Componenti stack avanzati | stack | Crea modifica di tipo EC2 ct-14027q0sjyt1h RFC. Sostituiscilo `InstanceAmiId` con l'ID Marketplace AWS AMI a cui ti sei abbonato.

Basato su Windows AMIs:

Microsoft Windows Server (2016, 2019 e 2022), basato sulla versione più recente di Windows AMIs.

Per esempi di creazione AMIs, consulta Creare AMI.

AMS per chi esce dall'imbarco: AMIs

AMS non comunica nulla AMIs all'utente durante l'offboarding per evitare ripercussioni sulle sue dipendenze. Se desideri rimuovere AMS AMIs dal tuo account, puoi utilizzare l'API per nascondere dati specifici. `cancel-image-launch-permission` AMIs Ad esempio, puoi utilizzare lo script seguente per nascondere tutti gli AMS AMIs che sono stati condivisi con il tuo account in precedenza:

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
    do
    aws ec2 cancel-image-launch-permission --image-id $ami ;
    done
```

È necessario che sia installata l'AWS CLI v2 affinché lo script possa essere eseguito senza errori. Per i passaggi di installazione dell'interfaccia a riga di comando di AWS, consulta Installazione o aggiornamento dell'ultima versione dell'interfaccia a riga di comando di AWS. Per i dettagli sul `cancel-image-launch-permission` comando, consulta. `cancel-image-launch-permission`

Sicurezza migliorata AMIs

AMS fornisce immagini di sicurezza avanzata (AMIs) basate sul benchmark CIS di livello 1 per un sottoinsieme dei sistemi operativi supportati da AMS. Per scoprire quali sistemi operativi dispongono di un'immagine di sicurezza avanzata, consulta la Guida alla sicurezza dei clienti di AWS Managed Services (AMS). Per accedere a questa guida, apri AWS Artifact, seleziona Report nel riquadro di navigazione a sinistra, quindi filtra per AWS Managed Services. Per istruzioni su come accedere AWS Artifact, contatta il tuo CSDM o consulta la sezione Getting Started with AWS Artifact per ulteriori informazioni.

Come funziona l'integrazione tra AD FS e AMS

Un trust unidirezionale tra la rete locale e il dominio AMS è il mezzo predefinito per l'accesso agli stack e. VPCs Quando vengono creati un VPC e uno stack, l'accesso viene concesso tramite gruppi di sicurezza Active Directory preconfigurati. Inoltre, l'accesso a Console di gestione AWS può essere configurato utilizzando Active Directory Federation Service (AD FS) o qualsiasi software di federazione che supporti SAML, per un single sign-on (SSO) alla console di gestione. AWS

> **Note**
>
> AMS può eseguire la federazione a molti servizi federativi, tra cui Ping, Okta e così via. Non sei limitato ad AD FS; forniamo qui un esempio di una tecnologia di federazione a tua disposizione.

Le informazioni riportate qui sono duplicate da questo post di blog: Enabling Federation to AWS Using Windows Active Directory, AD FS e SAML 2.0.

1. Il flusso viene avviato quando un utente (chiamiamolo Bob) accede al sito di esempio AD FS (https://Fully.Qualified.Domain.Name). Here/adfs/ls/IdpInitiatedSignOn.aspx) all'interno del suo dominio. Quando installi ADFS, ottieni una nuova directory virtuale denominata adfs per il tuo sito Web predefinito, che include questa pagina.
2. La pagina di accesso autentica Bob rispetto ad AD. A seconda del browser utilizzato da Bob, è possibile che gli venga richiesto di inserire il nome utente e la password di AD.
3. Il browser di Bob riceve un'asserzione SAML sotto forma di risposta di autenticazione da AD FS.
4. Il browser di Bob pubblica l'asserzione SAML nell'endpoint di AWS accesso per SAML (/saml). https://signin.aws.amazon.com Dietro le quinte, l'accesso utilizza l'API AssumeRoleWithSAML per richiedere credenziali di sicurezza temporanee e quindi crea un URL di accesso per. Console di gestione AWS
5. Il browser di Bob riceve l'URL di accesso e viene reindirizzato alla console.

Dal punto di vista di Bob, il processo avviene in modo trasparente. Inizia su un sito Web interno e finisce su Console di gestione AWS, senza mai dover fornire alcuna AWS credenziale.

> **Note**
>
> Ulteriori informazioni sulla configurazione della federazione sulla console AMS sono disponibili in:
>
> - Multi-Account Landing Zone: configurazione della federazione sulla console AMS
> - Zona di destinazione per account singolo: configurazione della federazione sulla console AMS

Inoltre, consulta l'Appendice: Regola di reclamo AD FS e impostazioni SAML. Per informazioni sull'utilizzo di AWS Microsoft AD per supportare le applicazioni compatibili con Active Directory, nel AWS cloud, soggette a requisiti di conformità, vedi Manage Microsoft AD Compliance.

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.

Implementazioni di applicazioni AMS

La guida per gli sviluppatori di applicazioni AMS fornisce descrizioni dettagliate e procedure dettagliate per le seguenti implementazioni:

- L'AMS workload ingest CT consente a te e a un partner di migrazione cloud AMS di spostare facilmente i carichi di lavoro esistenti in un VPC gestito da AMS. Utilizzando AMS workload ingest, puoi creare un AMI AMS inviando una RFC con Deployment | Ingestion | Stack from migration partner migrated instance | Create CT (ct-257p9zjk14ija). È necessario che un'istanza sia migrata dall'ambiente locale a AWS un partner di migrazione, nonché un VPC e una sottorete AMS di destinazione, in cui verrà inserita l'istanza.

  Per i dettagli, consulta la guida per sviluppatori di applicazioni AMS su Workload Ingest.
- La funzionalità CloudFormation ingest change type (ct-36cn2avfrrj9v) consente di utilizzare facilmente un modello esistente per distribuire stack personalizzati in un VPC gestito da AMS. CloudFormation

  Per i dettagli, consulta la guida per CloudFormation sviluppatori di applicazioni AMS su Template Ingest.
- Puoi importare il tuo database locale in un nuovo database nel tuo bucket Amazon S3 gestito da AMS o in un'istanza Amazon RDS. Questa operazione viene eseguita utilizzando un Deployment | Advanced stack components | Database Migration Service (DMS), tra cui Crea istanza di replica (ct-27apldkhqr0ol), Crea sottorete gruppo di replica (ct-2q5azjd8p1ag5), Crea attività di replica (ct-1d2fml15b9eth), Crea endpoint sorgente (ct-0attesnjqy2eth) cx) o Crea endpoint di origine (S3) (ct-2oxl37nphsrjz) e Crea endpoint di destinazione (ct-3gf8dolbo8x9p) o Crea endpoint di destinazione (S3) (ct-05muqzievnxk5).

  Per i dettagli, consulta la guida per sviluppatori di applicazioni AMS su Database Migration Service.
- Puoi importare il tuo database MS SQL locale in un nuovo database sull'istanza SQL RDS gestita da AMS. Puoi farlo utilizzando una varietà di tipi di modifiche AMS e l'API Amazon RDS, oltre a AWS console.

  Per i dettagli, consulta la AMS Application Guide at Database (DB) Import to MS SQL RDS.

Gestione dei servizi in AWS Managed Services

Argomenti

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.

Gestione pianificata degli eventi in AWS Managed Services

La gestione pianificata degli eventi (PEM) di AWS Managed Services (AMS) è un'offerta di servizi AMS. PEM coinvolge, coordina e assiste i clienti durante gli eventi e i progetti che utilizzano i servizi AMS. Il PEM aiuta a coordinare una serie di elementi correlati in linea con l'ambito e RFCs la tempistica concordati dell'evento o del progetto PEM.

Criteri AMS PEM

Un evento pianificato è un progetto limitato a un ambito e a una scadenza. AMS utilizza i dettagli forniti dall'utente (tra cui piano e ambito, risultati attesi e modifiche che le operazioni di AMS dovrebbero eseguire) per supportarti efficacemente durante l'attività PEM. I tuoi Cloud Architects (CAs) esaminano e valutano quindi l'attività PEM per verificarne la completezza, l'implementazione tecnica e il coinvolgimento delle operazioni AMS. Dopo la revisione da parte di CA, AMS Operations esamina i piani e si coordina con il responsabile della fornitura dei servizi cloud (CSDM) per il coinvolgimento del team operativo.

Tipi di PEM

Di seguito sono riportati i tipi di PEM disponibili:

- Giorni di gioco
  - Operational Gameday: un approccio di gioco basato su scenari alla risposta operativa, volto a convalidare l'integrazione di processi, persone e sistemi.
  - Security Gameday: una strategia di risposta agli incidenti di sicurezza che utilizza un approccio di gioco basato su scenari per valutare l'integrazione di sistemi, processi e personale.
- BYOEPS: utilizzate la funzione AMS «bring your own endpoint security» (BYOEPS) per sostituire l'agente Trend Micro Deep Security predefinito con la soluzione di sicurezza degli endpoint preferita o con una licenza Trend Micro personalizzata. Per ulteriori informazioni, consulta AMS porta il tuo EPS.
- Disaster Recovery: gli eventi di disaster recovery prevedono l'assistenza di AMS durante le attività di disaster recovery pianificate. Per ulteriori informazioni, consulta Pianificazione del disaster recovery.
- Evento di sicurezza del cliente: eventi di sicurezza pianificati. Ad esempio, attività degli utenti root e test di penetrazione.

- Supporto alla migrazione: supporto per attività di onboarding e migrazione pianificate.

Questo flusso di lavoro facilita la collaborazione con AMS per il coordinamento degli eventi pianificati e delle attività di migrazione relative al supporto AMS. Per l'esecuzione prioritaria di RFCs, è consigliabile utilizzare l'impegno Operations on Demand (OOD). Per ulteriori informazioni, consulta Operazioni su richiesta.

Il processo AMS PEM

Il processo PEM consiste nelle seguenti fasi:

- Iniziazione PEM: collaborate con il vostro CSDM per definire l'obiettivo per l'evento pianificato e determinare ciò che serve ad AMS Operations. AMS CAs esamina gli aspetti tecnici del piano PEM. La CAs collaborazione con AMS Security and Operations sulla conformità, l'ottimizzazione dell'esecuzione e l'automazione e sulla definizione delle attività e dei risultati di esecuzione pre-PEM. Quindi, il CSDM crea il ticket PEM e fornisce ad AMS le informazioni sul progetto e i dettagli tecnici. AMS richiede un lead time di 14 giorni di calendario per consentire al team AMS Operations di pianificare, fornire la revisione tecnica e assegnare le risorse.
- Revisione PEM: il team AMS Operations esamina la richiesta PEM e collabora con il CSDM per verificare che le informazioni contenute nel piano PEM siano corrette e complete.
- Accettazione PEM: AMS esamina le informazioni fornite e comunica al CSDM quale sarà il livello di supporto durante l'attività PEM. Se il PEM contiene informazioni complete e il CSDM concorda con lo scopo del lavoro, il PEM viene approvato.
- Prontezza ed esecuzione: AMS assicura che le attività necessarie prima dell'inizio del PEM siano completate e facilita le comunicazioni interne e con i clienti. AMS si assicura che il piano PEM funzioni correttamente e fornisce report sullo stato e sull'avanzamento.

PEM FAQs

Come posso coinvolgere AMS con una RFC/Service richiesta (SR) durante un evento PEM?

- Utilizza l'ID PEM condiviso dal tuo CSDM nella riga dell' RFC/SR oggetto del formato. `PEM-ID`
- Puoi anche creare una Service Request (SR) per discutere dei tuoi casi d'uso o per domande sull'evento pianificato. Se utilizzi un SR, non è necessario che il PEM sia valido.

Quali convalide vengono eseguite quando viene inviata una RFC relativa al PEM?

- Verifica che l'ID dell'account sia elencato nel PEM.
- Verifica che lo stato PEM sia approvato e attivo tra le date di inizio e fine fornite.

Esistono SLAs o sono SLOs per richieste PEM?

- PEMs non sono associati a SLAs o SLOs.
- SLAs e SLOs per gli elementi di lavoro relativi al PEM (RFC/Service Request) sono definiti da AMS. SLOs

  Per ulteriori informazioni, consulta gli obiettivi del livello di servizio AMS (). SLOs

Possiamo creare un PEM tramite una Service Request (SR)?

- No, la creazione di PEM deve essere gestita dal Cloud Service Delivery Manager (CSDM).

Architettura di rete

AWS Managed Services (AMS) offre due architetture di rete:

- Multi-account landing zone (MALZ): fornisce servizi comuni, come accesso, sicurezza degli endpoint, networking, da account condivisi per carichi di lavoro distribuiti in account membri separati.
- Single account landing zone (SALZ): fornisce account autonomi in cui servizi comuni come l'accesso, la sicurezza degli endpoint e il networking vengono implementati nello stesso account del carico di lavoro. È consigliato per carichi di lavoro che richiedono un elevato livello di isolamento in quanto comporta costi AWS più elevati.

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 rispettivamente Account di gestione | Creazione di account personalizzato OUs e di gestione | Creazione di un SCP personalizzato (revisione richiesta). 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 (revisione richiesta).

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.

Entità	Singola landing zone AMS	Zone di atterraggio multiple (due o più)
Configura bilità 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 attravers a più gateway di transito (TGWs) in ciascuna landing zone potrebbe comportare costi aggiuntivi.
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).

Entità	Singola landing zone AMS	Zone di atterraggio multiple (due o più)
Migrazione o portabilità dell'account	Sì. È possibile spostare account da un'unità organizzativa all'altra all'interno della stessa AWS Organization.	No. AMS non supporta la migrazione di un account tra zone di destinazione, ovvero tra AWS Organizations. I carichi di lavoro possono raggiungere tutte le zone di atterraggio con Transit Gateway (TGW) o peering VPC.
Gestione delle modifiche	Medio. Apportare modifiche distruttive 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 federazione 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 conformità 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

- 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. È possibile:

- 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.

Firewall Palo Alto in uscita gestito

AMS fornisce una soluzione firewall Managed Palo Alto egress, che consente il filtraggio del traffico in uscita verso Internet per tutte le reti nell'ambiente Multi-Account Landing Zone (esclusi i servizi rivolti al pubblico). Questa soluzione combina la tecnologia firewall leader del settore (Palo Alto VM-300) con le funzionalità di gestione dell'infrastruttura di AMS per implementare, monitorare, gestire, scalare e ripristinare l'infrastruttura all'interno di ambienti operativi conformi. Le terze parti, inclusa Palo Alto Networks, non hanno accesso ai firewall; sono gestiti esclusivamente dai tecnici AMS.

Controllo del traffico

La soluzione di firewall gestito in uscita gestisce un elenco di domini consentiti composto da domini richiesti da AMS per servizi come backup e patch, oltre ai domini definiti dall'utente. Quando il traffico Internet in uscita viene indirizzato al firewall, viene aperta una sessione, il traffico viene valutato e, se corrisponde a un dominio consentito, il traffico viene inoltrato alla destinazione.

Architettura

La soluzione firewall gestita in uscita segue un modello ad alta disponibilità, in cui vengono implementati da due a tre firewall a seconda del numero di zone di disponibilità (). AZs La soluzione utilizza parte dello spazio IP del VPC in uscita predefinito, ma fornisce anche un'estensione VPC (/24) per le risorse aggiuntive necessarie per la gestione dei firewall.

Flusso di rete

Ad un livello elevato, il routing del traffico pubblico in uscita rimane lo stesso, ad eccezione del modo in cui il traffico viene instradato verso Internet dal VPC in uscita:

1. Il traffico in uscita destinato a Internet viene inviato al Transit Gateway (TGW) tramite la tabella di routing VPC
2. TGW indirizza il traffico verso il VPC in uscita tramite la tabella delle rotte TGW
3. Il VPC indirizza il traffico verso Internet tramite le tabelle di routing della sottorete privata
   a. Nell'ambiente Multi-Account Landing Zone predefinito, il traffico Internet viene inviato direttamente a un gateway NAT (Network Address Translation). La soluzione firewall gestita riconfigura le tabelle di routing delle sottoreti private in modo che indirizzino invece la route predefinita (0.0.0.0/0) a un'interfaccia firewall.

I firewall stessi contengono tre interfacce:

1. Interfaccia affidabile: interfaccia privata per la ricezione del traffico da elaborare.
2. Interfaccia non affidabile: interfaccia pubblica per inviare traffico a Internet. Poiché i firewall eseguono il NAT, i server esterni accettano le richieste provenienti da questi indirizzi IP pubblici.
3. Interfaccia di gestione: interfaccia privata per l'API del firewall, gli aggiornamenti, la console e così via.

Durante tutto il routing, il traffico viene mantenuto all'interno della stessa zona di disponibilità (AZ) per ridurre il traffico inter-AZ. Il traffico attraversa solo AZs quando si verifica un failover.

Modifica dell'elenco delle autorizzazioni

Dopo l'onboarding, `ams-allowlist` viene creata una lista di autorizzazioni predefinita denominata, contenente gli endpoint pubblici richiesti da AMS e gli endpoint pubblici per l'applicazione di patch agli host Windows e Linux. Una volta operativi, è possibile creare RFC nella console AMS nella categoria Management | Managed Firewall | Outbound (Palo Alto) per creare o eliminare elenchi di autorizzazioni o modificare i domini. Tieni presente che non può essere modificato. `ams-allowlist` Le RFC vengono gestite in modo completamente automatico (non sono manuali).

Politica di sicurezza personalizzata

Le politiche di sicurezza determinano se bloccare o consentire una sessione in base agli attributi del traffico, come l'area di sicurezza di origine e destinazione, l'indirizzo IP di origine e destinazione e il servizio. Le politiche di sicurezza personalizzate sono supportate in modo completamente automatizzato RFCs. CTs per creare o eliminare una politica di sicurezza è disponibile nella categoria Management | Managed Firewall | Outbound (Palo Alto), mentre il CT per modificare una politica di sicurezza esistente è disponibile nella categoria Deployment | Managed Firewall | Outbound (Palo Alto). Potrai creare nuove politiche di sicurezza, modificare le politiche di sicurezza o eliminare le politiche di sicurezza.

> **Note**
>
> La politica di sicurezza predefinita `ams-allowlist` non può essere modificata

CloudWatch Pannelli di controllo PA in uscita

Sono disponibili due dashboard CloudWatch per fornire una visualizzazione aggregata di Palo Alto (PA). La dashboard AMS-MF-PA-Egress-Config-Config fornisce una panoramica della configurazione PA, collegamenti agli elenchi di autorizzazione e un elenco di tutte le politiche di sicurezza, inclusi i relativi attributi. La dashboard AMS-MF-PA-Egress-Dashboard può essere personalizzata per filtrare i registri di traffico. Ad esempio, per creare una dashboard per una politica di sicurezza, puoi creare un RFC con un filtro come:

```
fields @timestamp, @message
| filter @logStream like /pa-traffic-logs/
| filter @message like /<Security Policy Name>/
| parse @message
 "*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*,*
 as x1, @x2, @x3, @x4, @type, @x6, @x7, @source_ip, @destination_ip, @source_nat_ip,
 @dest_nat_ip, @rule, @x13, @x14, @application, @x16, @from_zone, @to_zone,
 @x19, @x20, @x21, @x22, @session_id, @x24, @source_port, @destination_port,
 @source_nat_port, @destination_nat_port, @x29, @protocol, @action, @bytes,
 @bytes_sent, @bytes_recieved, @packets, @x36, @x37, @category, @x39, @x40, @x41,
 @source_country, @destination_country, @x44, @packets_sent, @packets_recieved,
 @session_end_reason, @x48, @x49, @x50
| display @timestamp, @rule, @action, @session_end_reason, @protocol, @source_ip,
 @destination_ip, @source_port, @destination_port, @session_id, @from_zone,
```

```
@to_zone, @category, @bytes_sent, @bytes_recieved, @packets_sent, @packets_recieved,
@source_country, @destination_country
```

Modello di failover

La soluzione firewall include due-tre host Palo Alto (PA) (uno per AZ). Healthy check canaries funziona secondo un programma costante per valutare lo stato di salute degli host. Se un host viene identificato come non integro, AMS riceve una notifica e il traffico per quella AZ viene automaticamente spostato su un host integro in un'altra AZ modificando la tabella delle rotte. Poiché il flusso di lavoro relativo al controllo dello stato è in esecuzione costante, se l'host torna a funzionare correttamente a causa di problemi temporanei o di una correzione manuale, il traffico torna alla zona di disponibilità corretta con l'host integro.

Dimensionamento

AMS monitora il firewall per verificare la velocità di trasmissione e i limiti di scalabilità. Quando i limiti di velocità effettiva superano le soglie minime (CPU/rete), AMS riceve un avviso. Una soglia di produzione di acqua bassa indica che le risorse si stanno avvicinando alla saturazione, tanto che AMS valuterà le metriche nel tempo e suggerirà soluzioni di scalabilità.

Backup e ripristino

I backup vengono creati durante l'avvio iniziale, dopo eventuali modifiche alla configurazione e a intervalli regolari. I backup iniziali all'avvio vengono creati per ogni host, ma le modifiche alla configurazione e i backup a intervalli regolari vengono eseguiti su tutti gli host del firewall quando viene richiamato il flusso di lavoro di backup. I tecnici AMS possono creare backup aggiuntivi al di fuori di tali finestre o fornire dettagli di backup, se richiesto.

Se necessario, gli ingegneri AMS possono eseguire il ripristino dei backup di configurazione. Se è necessario un ripristino, questo verrà eseguito su tutti gli host per mantenere sincronizzata la configurazione tra gli host.

Il ripristino può avvenire anche quando un host richiede il riciclo completo di un'istanza. Il ripristino automatico del backup più recente si verifica quando viene eseguito il provisioning di una nuova EC2 istanza. In generale, gli host non vengono riciclati regolarmente e sono riservati ai guasti gravi o agli scambi AMI richiesti. I ricicli degli host vengono avviati manualmente e l'utente riceve una notifica prima che si verifichi un riciclo.

Oltre ai backup della configurazione del firewall, il backup delle regole specifiche dell'elenco di autorizzazioni viene eseguito separatamente. Un backup viene creato automaticamente quando le

regole dell'elenco di autorizzazioni definite vengono modificate. Il ripristino del backup dell'elenco delle autorizzazioni può essere eseguito da un tecnico AMS, se necessario.

Aggiornamenti

La soluzione AMS Managed Firewall richiede vari aggiornamenti nel tempo per aggiungere miglioramenti al sistema, funzionalità aggiuntive o aggiornamenti al sistema operativo (OS) o al software del firewall.

La maggior parte delle modifiche non influirà sull'ambiente in esecuzione, ad esempio l'aggiornamento dell'infrastruttura di automazione, ma altre modifiche, come la rotazione delle istanze del firewall o l'aggiornamento del sistema operativo, potrebbero causare interruzioni. Quando viene valutata una potenziale interruzione del servizio dovuta agli aggiornamenti, AMS si coordinerà con il cliente per adattare le finestre di manutenzione.

Accesso da parte dell'operatore

Gli operatori AMS utilizzano ActiveDirectory le proprie credenziali per accedere al dispositivo Palo Alto ed eseguire operazioni (ad esempio, applicare patch, rispondere a un evento, ecc.). La soluzione conserva i registri standard di autenticazione e modifica della configurazione degli operatori AMS per tenere traccia delle azioni eseguite sugli host di Palo Alto.

Registri predefiniti

Per impostazione predefinita, i log generati dal firewall risiedono nella memoria locale di ogni firewall. Nel tempo, i log locali verranno eliminati in base all'utilizzo dello storage. La soluzione AMS fornisce l'invio in tempo reale dei log dalle macchine ai CloudWatch registri; per ulteriori informazioni, vedere. CloudWatch Integrazione dei log

Gli ingegneri AMS hanno ancora la possibilità di interrogare ed esportare i log direttamente dalle macchine, se necessario. Inoltre, i registri possono essere spediti a un Panorama di proprietà del cliente; per ulteriori informazioni, vedere. Integrazione Panorama

I registri raccolti dalla soluzione sono i seguenti:

Codici di stato RFC

Tipo di log	Descrizione
Traffico	Visualizza una voce per l'inizio e la fine di ogni sessione. Ogni voce include la data e l'ora, le zone di origine e destinazione, gli indirizzi e

Tipo di log	Descrizione
	le porte, il nome dell'applicazione, il nome della regola di sicurezza applicata al flusso, l'azione della regola (consentire, negare o eliminare), l'interfaccia di ingresso e uscita, il numero di byte e il motivo della fine della sessione. La colonna Tipo indica se la voce riguarda l'inizio o la fine della sessione o se la sessione è stata negata o abbandonata. Un «drop» indica che la regola di sicurezza che ha bloccato il traffico specificava «qualsias i» applicazione, mentre un «nega» indica che la regola ha identificato un'applicazione specifica. Se il traffico viene interrotto prima che l'applicazione venga identificata, ad esempio quando una regola interrompe tutto il traffico per un servizio specifico, l'applicazione viene mostrata come «non applicabile».
Minaccia	Visualizza una voce per ogni allarme di sicurezza generato dal firewall. Ogni voce include la data e l'ora, il nome o l'URL di una minaccia, le zone di origine e destinazione, gli indirizzi e le porte, il nome dell'appl icazione, l'azione di allarme (consentire o bloccare) e la gravità. La colonna Tipo indica il tipo di minaccia, ad esempio «virus» o «spyware»; la colonna Nome è la descrizione o l'URL della minaccia; e la colonna Categoria è la categoria di minaccia (ad esempio «keylogger») o la categoria URL.
Filtraggio degli URL	Visualizza i registri dei filtri URL, che controllano l'accesso ai siti Web e se gli utenti possono inviare credenziali ai siti Web.
Configurazione	Visualizza una voce per ogni modifica alla configurazione. Ogni voce include la data e l'ora, il nome utente dell'amministratore, l'indirizzo IP da cui è stata apportata la modifica, il tipo di client (interfaccia web o CLI), il tipo di comando eseguito, se il comando è riuscito o meno, il percorso di configurazione e i valori prima e dopo la modifica.
System (Sistema)	Visualizza una voce per ogni evento di sistema. Ogni voce include la data e l'ora, la gravità dell'evento e una descrizione dell'evento.

Tipo di log	Descrizione
Allarmi	Il registro degli allarmi registra informazioni dettagliate sugli allarmi generati dal sistema. Le informazioni contenute in questo registro sono riportate anche in Allarmi. Fare riferimento a «Definizione delle impostazi oni degli allarmi».
Autenticazione	Visualizza informazioni sugli eventi di autenticazione che si verifican o quando gli utenti finali tentano di accedere a risorse di rete il cui accesso è controllato dalle regole dei criteri di autenticazione. Gli utenti possono utilizzare queste informazioni per aiutare a risolvere i problemi di accesso e per adattare la politica di autenticazione degli utenti in base alle esigenze. Oltre agli oggetti di correlazione, gli utenti possono anche utilizzare i registri di autenticazione per identificare attività sospette sulla rete degli utenti, come gli attacchi di forza bruta. Facoltativamente, gli utenti possono configurare le regole di autentica zione per registrare i timeout di autenticazione. Questi timeout si riferisco no al periodo di tempo in cui un utente deve autenticarsi per una risorsa una sola volta ma può accedervi ripetutamente. La visualizzazione delle informazioni sui timeout aiuta gli utenti a decidere se e come modificarli.
Unificato	Visualizza le ultime voci di registro relative al traffico, alle minacce, al filtro degli URL, agli WildFire invii e al filtro dei dati in un'unica visualizz azione. La visualizzazione collettiva dei log consente agli utenti di esaminare e filtrare questi diversi tipi di log insieme (invece di cercare ogni set di log separatamente). In alternativa, gli utenti possono scegliere quali tipi di log visualizzare: fai clic sulla freccia a sinistra del campo del filtro e seleziona traffico, minaccia, url, data, and/or wildfire per visualizz are solo i tipi di log selezionati.

Gestione degli eventi

AMS monitora continuamente la capacità, lo stato di integrità e la disponibilità del firewall. Le metriche generate dal firewall, così come le metriche AWS/AMS generate, vengono utilizzate per creare allarmi che vengono ricevuti dai tecnici operativi di AMS, che esamineranno e risolveranno il problema. Gli allarmi attuali coprono i seguenti casi:

Allarmi relativi agli eventi:

- Utilizzo della CPU Firewall Dataplane
  - Utilizzo della CPU - Dataplane CPU (elaborazione del traffico)
- L'utilizzo dei pacchetti Firewall Dataplane è superiore all'80%
  - Utilizzo dei pacchetti - Dataplane (elaborazione del traffico)
- Utilizzo della sessione Firewall Dataplane
- Sessione Firewall Dataplane attiva
- Utilizzo aggregato della CPU del firewall
  - Utilizzo della CPU in tutti i settori CPUs
- Failover tramite AZ
  - Avvisa quando si verifica un failover in una zona AZ
- Host Syslog non funzionante
  - L'host Syslog non supera il controllo di integrità

Gestione degli allarmi:

- Allarme di guasto del Health Check Monitor
  - Quando il flusso di lavoro del controllo dello stato di salute fallisce in modo imprevisto
  - Ciò riguarda il flusso di lavoro stesso, non se il controllo dello stato del firewall fallisce
- Allarme di errore di rotazione della password
  - Quando la rotazione della password fallisce
  - La password utente dell'API/servizio viene ruotata ogni 90 giorni

Parametri

Tutte le metriche vengono acquisite e archiviate CloudWatch nell'account di rete. Queste possono essere visualizzate accedendo dalla console all'account di rete e accedendo alla CloudWatch console. Le singole metriche possono essere visualizzate nella scheda Metriche o in un pannello di controllo a riquadro singolo di determinate metriche, mentre le metriche aggregate possono essere visualizzate accedendo alla scheda Dashboard e selezionando AMS-MF-PA-Egress-Dashboard.

Metriche personalizzate:

- Controllo dello stato

  - Spazio dei nomi: AMS/MF/PA/Egress
    - PARouteTableConnectionsByAZ
    - PAUnhealthyByInstance
    - PAUnhealthyAggregatedByAZ
    - PAHealthCheckLockState
- Firewall generato
  - Spazio dei nomi:/AMS/MF/PA/Egress<instance-id>
    - DataPlaneCPUUtilizationPct
    - DataPlanePacketBuffferUtilization
    - padella GPGateway UtilizationPct
    - panSessionActive
    - panSessionUtilization

CloudWatch Integrazione dei log

CloudWatch L'integrazione dei log inoltra i log dai firewall ai registri, riducendo così il rischio di perdita dei CloudWatch log a causa dell'utilizzo dello storage locale. I log vengono compilati in tempo reale man mano che i firewall li generano e possono essere visualizzati su richiesta tramite la console o l'API.

È possibile creare query complesse per l'analisi dei log o esportarle in formato CSV utilizzando Insights. CloudWatch Inoltre, la CloudWatch dashboard personalizzata di AMS Managed Firewall mostrerà anche una rapida visualizzazione di specifiche query relative al registro del traffico e una visualizzazione grafica del traffico e degli accessi alle politiche nel tempo. L'utilizzo dei CloudWatch log consente inoltre l'integrazione nativa con altri servizi AWS come AWS Kinesis.

> **Note**
>
> I log PA non possono essere inoltrati direttamente a un raccoglitore Syslog esistente locale o di terze parti. La soluzione AMS Managed Firewall fornisce la spedizione in tempo reale dei log dalle macchine PA ad AWS CloudWatch Logs. Puoi utilizzare la funzionalità CloudWatch Logs Insight per eseguire query ad hoc. Inoltre, i registri possono essere spediti alla soluzione di gestione Panorama di Palo Alto. CloudWatch i registri possono anche essere inoltrati ad

altre destinazioni utilizzando i filtri di abbonamento. CloudWatch Scopri di più su Panorama nella sezione seguente. Per saperne di più su Splunk, consulta Integrazione con Splunk.

Integrazione Panorama

AMS Managed Firewall può, opzionalmente, essere integrato con il tuo Panorama esistente. Ciò consente di visualizzare le configurazioni del firewall da Panorama o inoltrare i log dal firewall a Panorama. L'integrazione di Panorama con AMS Managed Firewall è di sola lettura e non sono consentite modifiche alla configurazione dei firewall da Panorama. Panorama è completamente gestito e configurato da te, AMS sarà responsabile solo della configurazione dei firewall per comunicare con esso.

Licenze

Il prezzo di AMS Managed Firewall dipende dal tipo di licenza utilizzata, oraria o BYOL (Bring Your Own License) e dalla dimensione dell'istanza in cui viene eseguita l'appliance. Devi ordinare le dimensioni delle istanze e le licenze del firewall Palo Alto che preferisci tramite AWS Marketplace.

- Licenze Marketplace: accetta i termini e le condizioni del VM-Series Next-Generation Firewall Bundle 1 dall'account di rete in MALZ.
- Licenze BYOL: accetta i termini e le condizioni del VM-Series Next-Generation Firewall (BYOL) dall'account di rete in MALZ e condividi il «codice di autenticazione BYOL» ottenuto dopo aver acquistato la licenza con AMS.

Limitazioni

Al momento, AMS supporta i firewall della serie VM-300 o della serie VM-500. Le configurazioni sono disponibili qui: modelli della serie VM su istanze AWS, EC2

> **Note**
>
> La soluzione AMS funziona in modalità Active-Active poiché ogni istanza PA nella relativa zona di disponibilità gestisce il traffico in uscita per la rispettiva AZ. Pertanto, con due istanze PA AZs, ciascuna istanza PA gestisce il traffico in uscita fino a 5 Gbps e fornisce in modo efficace un throughput complessivo di 10 Gbps su due. AZs Lo stesso vale per tutti i limiti in ogni AZ. Se il controllo dello stato dell'AMS dovesse fallire, spostiamo il traffico dalla zona di zona con PA difettosa a un'altra zona e, durante la sostituzione dell'istanza, la capacità viene ridotta ai AZs limiti rimanenti.

AMS attualmente non supporta altri bundle Palo Alto disponibili su AWS Marketplace; ad esempio, non è possibile richiedere il «VM-Series Next-Generation Firewall Bundle 2". Tieni presente che la soluzione AMS Managed Firewall che utilizza Palo Alto attualmente fornisce solo un'offerta di filtraggio del traffico in uscita, quindi l'utilizzo di pacchetti avanzati della serie VM non fornirebbe funzionalità o vantaggi aggiuntivi.

Requisiti per l'onboarding

- Devi leggere e accettare i termini e le condizioni del firewall di nuova generazione della serie VM di Palo Alto in AWS Marketplace.
- È necessario confermare la dimensione dell'istanza che si desidera utilizzare in base al carico di lavoro previsto.
- È necessario fornire un blocco CIDR /24 che non sia in conflitto con le reti nell'ambiente Multi-Account Landing Zone o On-Prem. Deve essere della stessa classe dell'Egress VPC (la Soluzione fornisce un'estensione VPC /24 al VPC Egress).

Prezzi

I costi dell'infrastruttura di base di AMS Managed Firewall sono suddivisi in tre fattori principali: l' EC2 istanza che ospita il firewall Palo Alto, la licenza software, le licenze Palo Alto VM-Series e le integrazioni. CloudWatch

I prezzi seguenti si basano sul firewall della serie VM-300.

- EC2 Istanze: il firewall Palo Alto funziona in un modello ad alta disponibilità di 2-3 EC2 istanze, in cui l'istanza si basa sui carichi di lavoro previsti. Il costo dell'istanza dipende dalla regione e dal numero di AZs
  - Ad esempio us-east-1, m5.xlarge, 3 AZs
    - 0,192 USD* 24 * 30* 3 = 414,72 USD
  - https://aws.amazon.com/ec2/prezzi/su richiesta/
- Licenze Palo Alto: il costo della licenza software di un firewall Palo Alto VM-300 di nuova generazione dipende dal numero di AZ e dal tipo di istanza.
  - Ad esempio us-east-1, m5.xlarge, 3 AZs
    - 0,87 USD* 24 * 30* 3 = 1879,20 USD

    - https://aws.amazon.com/marketplace/PP/B083M7JPKB? ref_=srh_res_product_title #pdp - prezzi
- CloudWatch Integrazione dei log: l'integrazione dei log utilizza server (- t3.medium), CloudWatch NLB e Logs. SysLog EC2 CloudWatch Il costo dei server si basa sulla regione e sul numero di AZs, mentre il costo dei log varia in base all'utilizzo del traffico. NLB/CloudWatch
    - Ad esempio us-east-1, t3.medium, 3AZ
        - 0,0416 US$ * 24 * 30 * 3 = 89,86 USD
    - https://aws.amazon.com/ec2/prezzi/su richiesta/
    - https://aws.amazon.com/cloudwatch/prezzi/

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. Si tratta del blocco CIDR principale per il 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), EC2 istanze, istanze relay e un agente presente in tutti i piani dati e EC2 le istanze dei clienti. EC2

  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 questi passaggi.

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. Usa Crea chiave KMS (auto) o Crea chiave KMS (revisione richiesta).

      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 (revisione richiesta) 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 EC2 console.

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.

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 EC2 istanze Amazon.

Configurazione di AMS

Argomenti

Alcune attività di configurazione di AMS potrebbero essere completate al momento dell'onboarding.

Per una descrizione completa dei ruoli e delle responsabilità, incluso l'AMSAWS Servizi supportati, vedi. Matrice di responsabilità AMS (RACI)

> **Note**
>
> Per richiedere che AMS fornisca un AWS servizio aggiuntivo, invia una richiesta di servizio. Per informazioni su come effettuare questa richiesta, consultaGestione delle richieste di assistenza.

Comprendere le impostazioni predefinite di AMS

La tua rete AWS Managed Services (AMS) ha una configurazione standardizzata con impostazioni predefinite per la maggior parte dei servizi.

Questa sezione descrive le impostazioni predefinite utilizzate da AMS per l'accesso, il monitoraggio e la registrazione e la gestione.

Per un esempio dei costi dell'infrastruttura per zone di atterraggio con più account o zone di atterraggio con un solo account, vedere. Componenti di base dell'ambiente AMS

Argomenti

Impostazioni di risoluzione DNS predefinite (MALZ)

Landing zone multi-account AWS Managed Services (AMS): negli ambienti AWS, la risoluzione DNS (Domain Name System) tra Route 53 Resolver e i resolver DNS in un VPC può essere integrata configurando le regole di inoltro del Resolver. Prima che queste regole possano essere utilizzate per l'inoltro delle query DNS, è necessario configurare gli endpoint resolver in entrata e in uscita a cui inoltrare queste query.

Per impostazione predefinita, le query DNS all'interno dell'account dell'applicazione VPCs nelle impostazioni multi-account in AMS vengono inoltrate ai server d'inoltro condizionali del dominio AWS Directory Service per Microsoft Active Directory (noto anche come Managed AD) presente nell'account di servizi condivisi. AMS consente facoltativamente di utilizzare il DNS, ad esempio il DNS a cui inoltrare le AmazonProvided query DNS. AmazonProvided Questo ti aiuta a utilizzare gli endpoint VPC che oggi supportano solo il DNS fornito da Amazon tramite Amazon Route 53. Di conseguenza, le regole Resolver vengono configurate automaticamente anche per gli endpoint VPC comuni che vengono distribuiti per impostazione predefinita nell'account dei servizi condivisi. Per ulteriori informazioni su questi endpoint VPC comuni, consulta. Endpoint VPC AMS

Per configurare i set di opzioni DHCP (Dynamic Host Configuration Protocol) in tutti gli account dell'applicazione VPCs per utilizzare il DNS fornito da Amazon per gli endpoint VPC e avere le regole

del Resolver Route53 che puntano agli endpoint VPC comuni nei tuoi account di servizi condivisi (con una regola Resolver opzionale per il dominio locale), crea una Gestione | Altro | Altro | Crea richiesta di modifica (RFC) specificando l'account dei servizi condivisi, e richiedendo l'abilitazione del DNS locale VPC dell'account dell'applicazione e delle regole Route 53 Resolver per gli endpoint VPC.

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
	`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.

Profilo	Policy
	`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	Consenso	Crea un gruppo di log	Consente la creazione di registri in: `aws:logs:*:*:log-group:i-*`
		Crea Log Stream	Consente lo streaming dei log su: `aws:logs:*:*:log-group:i-*`
CW per MMS	Consens	DescribeAlarms, PutMetricAlarm,	Consente di CloudWatch recuperare gli allarmi nel tuo account.

CW =. CloudWatch ARN = Amazon Resource Name. * = wildcard (qualsiasi).			
Dichiarazione delle policy	Effetto	Operazioni	Descrizione e risorse (ARN)
		PutMetricData	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)			
Azioni SSM	Consens	DescribeAssociation, GetDocument, ListAssociations, UpdateAssociationStatus, UpdateInstanceInformation	Consente una varietà di funzioni SSM nel tuo account.

CW =. CloudWatch ARN = Amazon Resource Name. * = wildcard (qualsiasi).			
Dichiarazione delle policy	Effetto	Operazioni	Descrizione e risorse (ARN)
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/*`
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}/*`

CW =. CloudWatch ARN = Amazon Resource Name. * = wildcard (qualsiasi).			
Dichiarazione delle policy	Effetto	Operazioni	Descrizione e risorse (ARN)
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-*/*` ,
Nega esplicitamente S3 CFN Bucket	Rifiuta	Elimina*	Impedisce alle applicazioni di eliminare oggetti EC2 da: `aws:s3:::cf-templates-*`
Nega esplicitamente 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.

Avvisi dal monitoraggio di base in AMS

Scopri le impostazioni predefinite di monitoraggio di AMS. Per ulteriori informazioni, consulta Monitoraggio e gestione degli eventi in AMS.

La tabella seguente mostra cosa viene monitorato e le soglie di avviso predefinite. Puoi modificare le soglie di avviso con un RFC Management | Other | Other | Update (ct-0xdawir96cy7k) dopo aver determinato le modifiche desiderate e aver sottoscritto l'argomento pertinente di Amazon SNS. CloudWatch Per informazioni sulla creazione e la sottoscrizione di argomenti, consulta Sottoscrivere un argomento. Per informazioni generali, consulta Amazon SNS FAQs. Per ricevere una notifica diretta quando gli allarmi superano la soglia, oltre alla procedura di avviso standard di AMS, segui queste istruzioni su come sovrascrivere le configurazioni degli allarmi,. Ricezione di avvisi generati da AMS

Amazon CloudWatch offre una conservazione estesa dei parametri. Per ulteriori informazioni, consulta CloudWatch Limiti.

> **Note**
>
> AMS calibra il monitoraggio di base su base periodica. L'onboarding di nuovi account viene sempre effettuato con il monitoraggio di base più recente e la tabella descrive il monitoraggio di base per un account che ha appena effettuato l'onboarding. AMS aggiorna periodicamente il monitoraggio di base negli account esistenti e potrebbe verificarsi un intervallo di tempo prima che gli aggiornamenti siano disponibili. Per ulteriori informazioni, consulta Visualizzazione della configurazione di monitoraggio per un account AMS.

> **Note**
>
> L'avviso di EC2 istanza `Non-root volume usage` è DISABILITATO per impostazione predefinita. Se si richiede la generazione di avvisi in base a questo allarme, è necessario abilitarla utilizzando il tipo di modifica RFC ct-0erkoad6uyvvg

Avvisi provenienti 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. Nel caso in cui l'automazione non riesca a risolvere il problema, AMS informa l'utente del caso in cui si è verificato l'incidente e viene assunto un tecnico AMS. Inoltre, questi avvisi possono essere inviati direttame nte alla tua e-mail (se hai scelto l'argomento Direct-Customer-Alerts SNS).			
Istanza Applicati on 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.
Obiettivo Applicati on 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.
EC2 Istanza Amazon: 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	CloudWatch allarme.

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
		> 85% per 5 minuti, 2 volte consecutive.	
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.
		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) .

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
EC2 istanza - tutte OSs	No	CPUUtilization* >= 95% per 5 minuti, 6 volte consecutive.	CloudWatch allarme. L'elevato utilizzo della CPU è un indicator e 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.	
		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.	

Servizio	Avviso di sicurezz	Nome dell'avviso e condizione di attivazione	Note
	Sì	Malware EPS Malware rilevato su esempio.	CloudWatch evento.
EC2 Istanza Amazon - 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.	
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 valori medi elevati e sostenuti sono problematici. 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 ci sono cambiamen ti nello stato degli eventi Dashboard AWS Health (AWS Health) in relazione ai servizi di base supportati da AMS. 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 potrebber o 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 l'autosca ling non è riuscito 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.

AMS intraprende azioni proattive (ridimensionamento del cluster) quando viene attivato questo avviso.

Per informazioni sulle azioni correttive, consulta. Correzione automatica degli avvisi con AMS

Guardate il video di Andrew per saperne di più (7:03)

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 a tempo indeterminato 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.

Uso delle console AMS

Le console AMS nella console di AWS gestione sono disponibili per interagire con AMS e utilizzare le risorse gestite da AMS Advanced e AMS Accelerate. Le console AMS generalmente si comportano come qualsiasi AWS console; tuttavia, poiché AMS è un'organizzazione privata, solo gli account abilitati per AMS possono accedere alla console. Una volta abilitato AMS nel tuo account, puoi accedere alla console cercando «Managed Services» nella barra di ricerca unificata.

> **Note**
>
> A seconda del ruolo dell'account, accedi alla console AMS Advanced o alla console AMS Accelerate.

Quando utilizzi le console AMS, tieni presente le seguenti avvertenze:

- La console AMS è specifica per ogni account. Pertanto, se utilizzi un account «Test» per la tua organizzazione, non potrai visualizzare le risorse nell'account «Prod» di quell'organizzazione. Allo stesso modo, devi avere un ruolo AMS Advanced per accedere alla console AMS Advanced.
- Le console AMS applicano una policy IAM al momento dell'autenticazione che determina a quale console puoi accedere e cosa puoi fare in quella sede. L'amministratore può applicare politiche aggiuntive alla politica AMS predefinita per limitare ciò che puoi vedere e fare nella console.

La console AMS Advanced ha le seguenti caratteristiche:

- Pagina di apertura: la pagina di apertura contiene riquadri informativi e link per facilitare l'accesso ai report esistenti RFCs, agli incidenti, alle richieste di assistenza e ai report.
- Pagine di funzionalità, collegamenti nel riquadro di navigazione a sinistra:
  - Dashboard: fornisce una panoramica dello stato attuale del tuo account, tra cui:
    - Richieste di modifica: scopri quante RFCs sono in attesa di risposta e vai alla pagina dell'elenco RFC con quel filtro attivo. Scopri quante RFCs sono in attesa della tua approvazione e vai alla pagina dell'elenco RFC con quel filtro attivo. Scopri quanti RFCs sono aperti e vai alla pagina dell'elenco RFC con quel filtro attivo. Apri la pagina dell'elenco RFCs facendo clic sul collegamento Visualizza tutto.
    - Incidenti: scopri quanti casi di incidenti sono in attesa di risposta e vai alla pagina dell'elenco degli incidenti con quel filtro attivo. Visualizza e quanti sono aperti e passa alla pagina dell'elenco degli incidenti con quel filtro attivo. Apri la pagina con l'elenco degli incidenti facendo clic sul collegamento Visualizza tutto.
    - Richieste di assistenza: scopri quante richieste di servizio sono in attesa di risposta e vai alla pagina dell'elenco delle richieste di assistenza con il filtro attivo. Visualizza e quante sono aperte e passa alla pagina dell'elenco delle richieste di assistenza con quel filtro attivo. Aprire la pagina dell'elenco delle richieste di assistenza facendo clic sul collegamento Visualizza tutto.
    - Aggiornato di recente RFCs: data, link ai dettagli della RFC e stato
    - Incidenti e richieste di assistenza creati di recente: data, collegamento ai dettagli del caso e tipo (incidente o richiesta di servizio)
  - RFCs: apre un elenco di quelli esistenti RFCs per l'account
  - Incidenti: apre un elenco degli incidenti aperti per l'account
  - Richieste di assistenza: apre un elenco delle richieste di servizio aperte per l'account
  - Rapporti: apre la pagina Report e i report predefiniti, Backup giornaliero e Patch giornalieri e Fatturazione mensile
  - Risorse:
    - VPCs: Apre un elenco di quelli esistenti VPCs per l'account
    - Pile: apre un elenco di pile esistenti per l'account
    - AMIs: Apre un elenco di AMS disponibili AMIs
- Funzionalità in primo piano: informazioni sugli ultimi aggiornamenti della console

- Risorse per gli sviluppatori: una pagina di file scaricabili, tra cui l'SDK AMS Advanced Change Management e altro
- Documentazione: pagina iniziale della documentazione di AWS Managed Services

Utilizzo dell'API e della CLI AMS

L'API AWS Managed Services (AMS) è simile a quella APIs per altri AWS servizi. Puoi leggere informazioni sull'API AMS nell'AMS API Reference.

Endpoint HTTP dell'API AMS per chiamate REST

Oltre alle varie opzioni SDKs, AMS fornisce una CLI; puoi anche richiamare chiamate API REST sull'endpoint AMS.

Esistono due AMS APIs (l'endpoint per entrambi risiede in us-east-1):

- Gestione delle modifiche: utilizza questa API per richiedere l'accesso o le modifiche all'infrastruttura, tra cui la creazione e l'aggiornamento, la distribuzione di nuove istanze RFCs, l'aggiornamento e l'eliminazione di istanze, l'acquisizione di informazioni e la creazione. CTs AMIs L'endpoint HTTP è:

  ```
  https://amscm.us-east-1.amazonaws.com
  ```

- SKMS: utilizza questa API per ottenere informazioni sulla tua infrastruttura, tra cui stack VPCs, sottoreti e. AMIs L'endpoint HTTP è:

  ```
  https://amsskms.us-east-1.amazonaws.com
  ```

Installazione o aggiornamento della CLI AMS

L'AMS CLI è un modo semplice per interagire con l'API AMS e viene utilizzata negli esempi di questa sezione. Per le convenzioni di utilizzo per AWS CLI e AMS CLI, vedere Uso AWS dell'interfaccia a riga di comando.

Per informazioni sull'installazione di SAML, consulta. Regola di attestazione AD FS e impostazioni SAML

Per installare o aggiornare l'AMS CLI, segui queste istruzioni:

> **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 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`

Utilizzo dell'API AMS in CLI, Ruby, Python e Java

Di seguito è riportato un elenco di frammenti di codice per il `ListChangeTypeClassificationSummaries` funzionamento dell'API AMS, in tutte le lingue disponibili.

Per Python, Ruby e Java SDKs, consulta Tools for Amazon Web Services e scorri verso il basso fino alla sezione. SDKs Ogni programma di installazione SDK contiene un README con frammenti di codice aggiuntivi.

Esempio da API AMS a CLI

Dopo aver installato l'AMS CLI (richiede la AWS CLI; vediInstallazione o aggiornamento della CLI AMS), puoi eseguire qualsiasi operazione API AMS riformando la chiamata specificando prima quale API AMS`aws amsskms`, `aws amscm` oppure eseguendo l'azione con trattini che sostituiscono camel case. Infine, fornisci credenziali, come SAML.

Per ulteriori informazioni, consulta Utilizzo dell'interfaccia a riga di AWS comando.

Esempio:

- API: `'ChangeTypeClassificationSummaries[].[Category,Subcategory,Item,Operation,ChangeTypeId]'`
- CLI: `amscm list-change-type-classification-summaries --query "ChangeTypeClassificationSummaries[*].[Category,Subcategory,Item,Operation,ChangeTypeId]" --output table`

> **Note**
>
> Se esegui l'autenticazione con SAML, aggiungi `aws --profile saml` all'inizio del comando. Ad esempio,
>
> ```
> aws --profile saml amscm list-change-type-classification-
> summaries --query "ChangeTypeClassificationSummaries[*].
> [Category,Subcategory,Item,Operation,ChangeTypeId]" --output table
> ```

Esempio da API AMS a Python

Per utilizzare l'API AMS con Python, installa la CLI AMS e installa boto3. Completare la procedura riportata di seguito.

1. Installa l'AMS CLI. Per informazioni, consulta Installazione o aggiornamento della CLI AMS.
2. Installa boto3, l' AWS SDK per Python. Per ulteriori informazioni, consulta questo post sul blog Now Available — AWS SDK For Python (Boto3).

   ```
   import boto3
   ```

3. Scarica il client AMS Change Management:

   ```
   cm = boto3.client('amscm')
   ```

4. Ottieni l'AMS CTs:

   ```
   cts = cm.list_change_type_classification_summaries()

   print(cts)
   ```

Esempi di Python

Di seguito sono riportati alcuni esempi di utilizzo di Python in AMS, per creare EC2 istanze, utilizzare and/or Lambda.

Esempio in Python per creare un EC2

Questo esempio mostra come utilizzare l' RESTFul API amscm dall'interno del codice Python per archiviare ed eseguire processi RFC.

1. Installa l'AMS CLI da qualche parte a cui hai accesso; ti servono i file che fornisce.
2. Chiama le librerie Python e crea l' EC2 istanza:

```
import boto3
import json
import time

# Create the amscm client
cm = boto3.client('amscm')

# Define the execution parameters for EC2 Create
AMSExecParams = {
    "Description": "EC2-Create",
    "VpcId": "VPC_ID",
    "Name": "My-EC2",
    "TimeoutInMinutes": 60,
    "Parameters": {
        "InstanceAmiId": "INSTANCE_ID",
        "InstanceSubnetId": "SUBNET_ID"
    }
}

# Create the AMS RFC
cts = cm.create_rfc(
    ChangeTypeId="ct-14027q0sjyt1h",
    ChangeTypeVersion="3.0",
    Title="Python Code RFC Create",
    ExecutionParameters=json.dumps(AMSExecParams)
)

# Extract the RFC ID from the response
NewRfcID = cts['RfcId']
```

```
# Submit the RFC
RFC_Submit_Return=cm.submit_rfc(RfcId=NewRfcID)

# Check the RFC status every 30 seconds
RFC_Status = cm.get_rfc(RfcId=NewRfcID)
RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']

while RFC_Status_Code != "Success":
    if RFC_Status_Code == "PendingApproval":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "InProgress":
        print(RFC_Status_Code)
        time.sleep(30)
    elif RFC_Status_Code == "Failure":
        print(RFC_Status_Code)
        break
    else:
        print(RFC_Status_Code)

    RFC_Status = cm.get_rfc(RfcId=NewRfcID)
    RFC_Status_Code = RFC_Status['Rfc']['Status']['Name']
```

Esempio di Python con Lambda

Questo esempio mostra come raggruppare i modelli AMS con il codice in modo da poterlo utilizzare con Lambda, EC2 ovvero luoghi che non si possono o non possono installare. `amscli`

> **Note**
>
> AMS non fornisce un SDK Python specifico per AMS importabile. Lo script di installazione `amscli` installa i modelli di dati del servizio AMS nel percorso normale della CLI. Per l'utilizzo della CLI e l'utilizzo del sistema Python, va bene, perché entrambi `boto3` leggono `awscli` i propri modelli di servizio dalle stesse posizioni predefinite (). `~/.aws/models` Tuttavia, quando desideri utilizzare i servizi AMS tramite boto3 in Lambda (o qualsiasi altro runtime non locale), si interrompe, perché non hai più i modelli di dati. Di seguito è riportato un metodo per risolvere questo problema impacchettando i modelli di dati con la funzione.

È possibile eseguire alcuni semplici passaggi per eseguire il codice Python integrato con AMS in Lambda o in un altro runtime come Fargate, ecc. EC2 Il seguente flusso di lavoro mostra i passaggi necessari per le funzioni Lambda integrate in AMS.

Aggiungendo i modelli di dati al pacchetto di distribuzione del codice e aggiornando il percorso di ricerca dell'SDK, puoi simulare un'esperienza SDK.

> **Important**
>
> Questo esempio e tutti i comandi non Python mostrati sono stati testati su un computer Mac.

Esempio di flusso di lavoro:

1. Installa `amscli`. Questo crea una cartella `~/.aws/models` sul tuo computer (Mac).
2. Copia i modelli in una directory locale:`cp ~/.aws/models ./models`.
3. Includi i modelli nel pacchetto di distribuzione del codice.
4. Aggiorna il codice della funzione per aggiungere i nuovi modelli al percorso SDK. Nota che questo codice deve essere eseguito prima che boto3 o botocore vengano importati!

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

> **Note**
>
> Poiché i modelli di esempio si trovano in una directory denominata`models`, li aggiungiamo a _PATH. `./models` AWS_DATA Se la directory avesse un nome`/ams/boto3models`, aggiungeremmo il seguente codice:

```
import os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
```

```
import botocore
```

Il tuo codice dovrebbe trovare correttamente i modelli AMS. Come esempio più specifico relativo al packaging, ecco il flusso di lavoro specifico per Lambda.

Esempio di flusso di lavoro AMS Lambda:

Questi passaggi applicano l'esempio generico precedente alla creazione di una funzione AWS Lambda.

1. Installa amscli. Questo crea una cartella `~/.aws/models` sul tuo computer (Mac).
2. Copia i modelli in una directory locale:

```
cp ~/.aws/models ./models
```

3. Aggiungi i modelli al file zip di distribuzione della tua funzione:

```
zip -r9 function.zip ./models
```

Important

Aggiorna il codice della funzione per aggiungere i nuovi modelli al percorso SDK. Nota che questo codice deve essere eseguito prima che boto3 o botocore vengano importati!

```
# Force Python to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore
```

Note

Poiché i modelli di esempio si trovano in una directory denominata`models`, li aggiungiamo a _PATH. `./models` AWS_DATA Se la directory avesse un nome`/ams/boto3models`, aggiungeremmo il seguente codice:

```
import os
os.environ['AWS_DATA_PATH'] = './ams/boto3models'

import boto3
import botocore
```

Ora, implementa la tua funzione:

1. Aggiungi il codice della funzione al file zip di distribuzione (se non l'hai già fatto):

```
zip -g function.zip lambda-amscm-test.py
```

2. Crea o aggiorna la tua funzione con il file zip che hai creato (console o CLI):

```
aws lambda update-function-code --function-name lambda-amscm-test --zip-file fileb://
function.zip --region us-east-1
```

La tua Python Lambda integrata con AMS dovrebbe ora funzionare.

> **Note**
>
> La tua funzione deve disporre delle autorizzazioni IAM per `amscm` altrimenti riceverai un errore di autorizzazione.

Esempio di codice della funzione Lambda per testare amscm (contenuto di .py): lambda-amscm-test

```
import json

# Force lambda to search local directory for boto3 data models
import os
os.environ['AWS_DATA_PATH'] = './models'

import boto3
import botocore


def lambda_handler(event, context):
```

```
    use_session = boto3.session.Session(region_name="us-east-1")
    try:
        cm = use_session.client("amscm")
        cts = cm.list_change_type_categories()
        print(cts)
    except botocore.exceptions.UnknownServiceError:
        print("amscm not found")

    return {
        'statusCode': 200,
        'body': json.dumps('Hello from Lambda!')
    }
```

Risultati del test (successo):

Risposta della funzione:

```
{
  "statusCode": 200,
  "body": "\"Hello from Lambda!\""
}

Request ID:
"1cea13c0-ed46-43b1-b102-a8ea28529c27"
```

Registri delle funzioni:

```
START RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27 Version: $LATEST
{'ChangeTypeCategories': ['Deployment', 'Internal Infrastructure Management',
 'Management'], 'ResponseMetadata': {'RequestId': 'e27276a0-e081-408d-
bcc2-10cf0aa19ece', 'HTTPStatusCode': 200, 'HTTPHeaders': {'x-amzn-requestid':
 'e27276a0-e081-408d-bcc2-10cf0aa19ece', 'content-type': 'application/x-amz-json-1.1',
 'content-length': '89', 'date': 'Sun, 10 May 2020 23:21:19 GMT'}, 'RetryAttempts': 0}}
END RequestId: 1cea13c0-ed46-43b1-b102-a8ea28529c27
```

Esempio da API AMS a Ruby

Per utilizzare l'API AMS con Ruby, installa AWS Ruby SDK e AMS CLI. Completare la procedura riportata di seguito.

1. Installa l'AMS CLI. Per informazioni, consulta Installazione o aggiornamento della CLI AMS.
2. Installa AWS Ruby SDK. Vedi Strumenti per Amazon Web Services.

3. Configura Ruby con questi comandi:

```
require 'aws-sdk'

config = {

 region: 'us-east-1',

 credentials: Aws::Credentials.new('ACCESS_KEY','SECRET_KEY')}
```

4. Ottieni l'AMS CTs:

```
ams_cm = Aws::amscm::Client.new(config)

cts = ams_cm.list_change_type_classification_summaries

print(cts)
```

Esempio da API AMS a Java

Per utilizzare l'API AMS con Java, installa AWS Java SDK e AMS CLI. Completare la procedura riportata di seguito.

1. Installa l'AMS CLI. Per informazioni, consulta Installazione o aggiornamento della CLI AMS.
2. Installa l'SDK AWS Java. Vedi Strumenti per Amazon Web Services.
3. Configura Java con questi comandi:

```
import com.amazonaws.auth.BasicAWSCredentials;

import com.amazonaws.services.amscm.model.AWSManagedServicesCMClient;

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesReque

import
com.amazonaws.services.amscm.model.ListChangeTypeClassificationSummariesResul

public static void getChangeTypeClassificationSummaries() {
```

4. Imposta le credenziali. Ti consigliamo di non codificarlo come codice fisso.

```
final BasicAWSCredentials awsCredsCm =
```

```
 new BasicAWSCredentials("ACCESS_KEY", "SECRET_KEY");
```

5. Crea il client AMS Change Management:

```
final AWSManagedServicesCMClient cmClient =

 new AWSManagedServicesCMClient(awsCredsCm);
```

6. Ottieni l'AMS CTs:

```
final ListChangeTypeClassificationSummariesRequest listCtsRequest = new
ListChangeTypeClassification SummariesRequest();

final ListChangeTypeClassificationSummariesResult listCtsResult =

cmClient.listChangeTypeClassificationSummaries(listCtsRequest);

System.out.println("List of CTs");

listCtsResult.getChangeTypeClassificationSummaries().stream()

.map(x -> x.getCategory() + "/" + x.getSubcategory() + "/" +
x.getItem() + "/" + x.getOperation())

.forEach(System.out::println);

}
```

AMS porta il tuo EPS

Utilizza la funzionalità AMS «bring your own end point security» (BYOEPS) per sostituire l'agente Trend Micro Deep Security predefinito con la tua soluzione di sicurezza degli endpoint o con la tua licenza Trend Micro. Se disponi già di licenze convenienti per prodotti diversi da Trend Micro Deep Security o di un team che fornisce il tuo EPS, o se desideri utilizzare uno strumento EPS specifico, utilizza BYOEPS nelle tue istanze.

BYOEPS funziona a livello di account. Le istanze nell'account utilizzano BYOEPS o l'EPS predefinito gestito da AMS:

- multi-account landing zone (MALZ): designate gli account delle applicazioni che utilizzano BYOEPS o managed EPS.

- single-account landing zone (SALZ): i tuoi account AMS utilizzano BYOEPS o managed EPS.

BYOEPS, riduce la AWS bolletta del costo di Trend Micro Deep Security. Continuate a sostenere un costo per EPS perché l'EPS gestito da AMS è ancora necessario per proteggere le EC2 istanze create e gestite da AMS e necessarie per la gestione degli accessi (bastioni e host di gestione). Per calcolare l'impatto totale sui costi, è necessario tenere conto del costo delle licenze per il nuovo strumento e del costo di gestione dell'EPS ai livelli di servizio richiesti.

L'uso di BYOEPS modifica i ruoli e le responsabilità di AMS per la gestione della sicurezza:

- R sta per parte responsabile che fa il lavoro per raggiungere l'obiettivo.
- C sta per consultato; una parte i cui pareri vengono richiesti, in genere in qualità di esperti in materia, e con la quale esiste una comunicazione bilaterale.
- I sta per informato; una parte che viene informata sui progressi, spesso solo al completamento del compito o del risultato.

Gestione della sicurezza	Customer	AWS Managed Services
Mantenimento di licenze valide di Managed EPS per EC2 le istanze di AMS Shared Services	R	C
Configura Managed EPS per le EC2 istanze di AMS Shared Services	I	R
Aggiorna Managed EPS per le EC2 istanze di AMS Shared Services	I	R
Monitoraggio del malware sulle EC2 istanze di AMS Shared Services	I	R
Manutenzione e aggiornam ento delle firme dei virus per	I	R

Gestione della sicurezza	Customer	AWS Managed Services
le EC2 istanze di AMS Shared Services		
Correzione delle istanze infette da malware per le istanze di AMS Shared EC2 Services	C	R

Quando utilizzi BYOEPS, perdi uno dei controlli di sicurezza offerti da AMS. La gestione della sicurezza è ancora fornita tramite strumenti come Amazon GuardDuty, Amazon Macie e controlli di processo, come le revisioni delle configurazioni IAM. L'uso di BYOEPS non influisce sulle certificazioni e sugli attestati di conformità AMS. Tuttavia, molti framework e certificazioni di sicurezza prevedono requisiti per la protezione da malware e codice dannoso. Per mantenere il tuo account sicuro e conforme, valuta i controlli pianificati per assicurarti che soddisfino i requisiti di sicurezza per le certificazioni di conformità del tuo carico di lavoro.

Attiva BYOEPS per il tuo account

Il processo di attivazione del BYOEPS prevede tre fasi e ne utilizza diverse. RFCs Consulta le seguenti informazioni per conoscere le tre fasi necessarie per attivare il BYOEPS. Quindi, coordinati con il tuo CSDM per attivare il BYOEPS per il tuo account.

Argomenti

Fase 1: Prerequisiti

- Il profilo di EC2 istanza Amazon predefinito è`customer-mc-ec2-instance-profile`. Se utilizzi un profilo di EC2 istanza Amazon diverso da quello predefinito, consenti l'`ssm:GetParameter`azione della `/ams/end-point-security` risorsa al tuo profilo di EC2 istanza.

Se non riesci EC2 ad aggiornare i profili delle istanze, invia una RFC che specifichi i profili di istanza da aggiornare.

- Comprendi l'ambito di questa modifica.

  Le implementazioni tramite un tipo di modifica automatica (CT) AMS consentono di specificare l'AMI utilizzata nella creazione.

  Per utilizzare BYOEPS con account che utilizzano EPS gestito da AMS, è necessario collaborare con AMS per disinstallare gli agenti Trend Micro da tali EC2 istanze e aggiornare il codice AMS (ad esempio, gli script di avvio) su tali istanze. Queste azioni potrebbero richiedere un riavvio, quindi è consigliabile eseguirle come parte di una finestra di manutenzione. Contattate il vostro CSDM per identificare una finestra di manutenzione per eseguire questa attività e per creare un piano di migrazione. Per il piano di migrazione, considera le seguenti domande:

  1. Quante istanze devi migrare? Dividi il numero totale di istanze in batch incrementali più piccoli.
  2. Come dividerai le istanze in batch? Ad esempio, potresti dividere per gruppi di risorse e creare un elenco da condividere con il team operativo AMS.
  3. Quanto tempo impiegherà ogni batch? Quanto tempo totale è necessario? Considerate che potreste voler installare i vostri utensili EPS preferiti nella stessa finestra di manutenzione. Quanto tempo ci vorrà?

- Il vostro CSDM condivide il piano di migrazione con il team operativo di AMS. Se il tuo parco istanze è superiore a 50, collabora con il CSDM per creare un evento pianificato utilizzando il processo di gestione degli eventi pianificati (PEM). Per ulteriori informazioni, consulta Gestione pianificata degli eventi in AWS Managed Services

  AMS Operations si coordina con il tuo CSDM e ti consiglia come effettuare l'invio RFCs in base alle finestre di manutenzione, in base al numero di istanze presenti nel tuo account.

- Aggiorna le automazioni o i processi di avvio delle EC2 istanze utilizzando soluzioni personalizzate o AMS AMIs per utilizzare AMIs AMS rilasciate dopo dicembre 2020.

Fase 2: abilita BYOEPS nel tuo account

Quando utilizzi BYOEPS nel tuo account, le responsabilità di AMS per la gestione della sicurezza cambiano. Consultate il vostro team addetto alla sicurezza e alla piattaforma cloud prima di abilitare BYOEPS.

Per richiedere BYOEPS per il tuo account, invia un aggiornamento «MOO» RFC (Gestione | Altro | Altro | Aggiornamento) con ct-0xdawir96cy7k, con i seguenti dettagli:

```
Please enable BYOEPS for this account/these accounts
Account IDs: IDs for the accounts for BYOEPS.
```

AMS distribuisce gli aggiornamenti del Parameter Store all'account e aggiorna il profilo dell'istanza Amazon EC2 IAM.

> **Note**
>
> - Gli account con il lancio di nuove istanze che utilizzano l'ultima versione di AMS AMIs possono ignorare l'installazione dell'agente Trend Micro. AMIs le versioni precedenti a dicembre 2020 non supportano la funzionalità BYOEPS. Aggiorna le automazioni che utilizzano le versioni precedenti AMIs per utilizzare la versione più recente di AMS AMIs con supporto per le funzionalità BYOEPS.
> - Per la gestione delle EC2 istanze esistenti, consulta Fase 3: migrazioni di istanze

Fase 3: migrazione delle istanze

Utilizza una delle seguenti opzioni per migrare le istanze, a seconda del caso d'uso. Se non siete sicuri dell'opzione da scegliere, contattate la vostra CA o il CSDM.

Account con EC2 istanze che utilizzano EPS gestito da AMS

Durante la finestra di manutenzione, in linea con la pianificazione della Fase 1, vengono eseguite le seguenti azioni su ogni istanza che deve essere inserita in BYOEPS:

- Eseguita da AMS: aggiorna il codice AMS (script di avvio, moduli e così via) alle versioni più recenti. Ciò è necessario perché i vecchi script di avvio AMS non supportano la funzionalità BYOEPS e reinstallano l'agente Trend Micro a ogni avvio. Inoltre, disinstallate Trend Micro Agent.
- Eseguita dall'utente: installa e configura lo strumento EPS preferito.

> **Important**
>
> Trend Micro Agent fornisce protezione da malware. Assicurati di installare un sostituto appropriato per proteggere le tue istanze.

Per effettuare queste modifiche, inviatele RFCs con il tipo di modifica ct-2iz9nvw8zlhst, Trend Micro DSM | Remove Trend Micro EPS Agent (è richiesta la revisione), in batch.

EC2 Account senza istanze che utilizzano EPS gestito da AMS

Gli account con il lancio di nuove istanze che utilizzano l'ultima versione di AMS AMIs possono ignorare l'installazione dell'agente Trend Micro. AMIs le versioni precedenti a dicembre 2020 non supportano la funzionalità BYOEPS. Aggiorna le automazioni che utilizzano le versioni precedenti AMIs per utilizzare la versione più recente di AMS AMIs con supporto per le funzionalità BYOEPS.

Aggiungi il tuo agente sulle istanze EC2

Puoi utilizzare AMS Patterns per implementare agenti di strumenti come CrowdStrike o Qualys, Invia una richiesta di assistenza.

Ricezione di notifiche AMS

Le comunicazioni tra l'utente e AMS avvengono per diverse ragioni:

- Una RFC creata da AMS che richiede la tua approvazione
- Un caso AMS creato per esaminare una RFC da te creata che non è riuscita
- Eventi creati dagli avvisi di monitoraggio
- Notifiche del servizio di patch che informano dell'imminente applicazione delle patch
- Richieste di assistenza e segnalazioni di incidenti
- Rapporti CRM mensili
- Annunci occasionali importanti di AWS (il CSDM ti contatta se è necessaria un'azione da parte tua)

Tutte queste notifiche vengono inviate alle informazioni di contatto predefinite (l'e-mail dell'account root) che hai fornito ad AMS al momento dell'onboarding. Poiché è difficile mantenere aggiornate le singole e-mail, ti consigliamo di utilizzare un'e-mail di gruppo che possa essere aggiornata da parte tua. Tutte le notifiche che ti vengono inviate vengono ricevute anche dalle operazioni AMS e analizzate prima di dare una risposta.

Il servizio di notifica AMS offre due modi aggiuntivi per configurare i contatti per le notifiche:

- Etichetta le tue risorse con tag di contatto (il tag Key Value rappresenta le informazioni di contatto) e fornisci il tag Key Name al tuo CSDM. Gli allarmi relativi a tali risorse verranno inviati

ai contatti indicati nel Key Value, oltre al contatto dell'account creato durante l'onboarding. Ciò è particolarmente utile per i proprietari delle applicazioni. Per ulteriori informazioni, consulta Notifica di avviso basata su tag.

- (Obbligatorio al momento dell'onboarding) Invia al tuo CSDM elenchi di contatti nominativi per notifiche non basate sulle risorse. Ad esempio, potreste avere una lista denominata "" e un'altra denominata SecurityContacts "OperationsContacts«, e così via. AMS aggiunge l'elenco al servizio di notifica e gli allarmi che si applicano al contesto di quell'elenco vengono inviati a tali contatti. Ciò è particolarmente utile per le questioni organizzative.

Questa funzionalità avanzata di routing degli avvisi è attiva per la maggior parte degli CloudWatch allarmi essenziali come il guasto delle EC2 istanze Amazon, l'utilizzo della capacità del volume di Amazon Elastic Block Store (Amazon EBS): utilizzo root, utilizzo di NonRoot Amazon EBS, utilizzo elevato della memoria, utilizzo High Swap e utilizzo elevato della CPU per Amazon. EC2

Inoltre, quando invii una richiesta di servizio o una segnalazione di incidente, hai la possibilità di aggiungere «Email CC» (altamente consigliato) e tali indirizzi e-mail ricevono notifiche sulla richiesta di servizio o sull'incidente.

> **Important**
>
> Mentre gli indirizzi e-mail CC forniti nelle richieste di servizio e nelle segnalazioni di incidenti ricevono notifiche e-mail di comunicazioni, altre notifiche, come le notifiche di patch, vengono visualizzate nell'elenco delle richieste di servizio (viene inviata anche un'e-mail al contatto predefinito), senza che venga notificata esplicitamente all'utente la presenza di una comunicazione in attesa della sua attenzione. Questo è il motivo per cui consigliamo vivamente di aggiungere un'e-mail CC, ove possibile, e di impostare l'e-mail di contatto predefinita come gruppo a cui appartengono tutti gli utenti di AMS.

Inoltre, puoi richiedere notifiche speciali per le novità AMIs, per la modifica dello stato RFC e per le modifiche alla configurazione del tuo account AMS. Questi servizi di notifica opzionali vengono discussi di seguito.

Notifiche AMI AMS con SNS

AMS fornisce un servizio di notifica AMI. Puoi usarlo per abbonarti a un argomento di Amazon Simple Notification Service (SNS) che ti avvisa quando vengono rilasciati aggiornamenti AMI AMS. Puoi

scegliere di ricevere notifiche solo per l'AMS AMIs che utilizzi oppure puoi registrarti per ricevere notifiche di aggiornamento per tutti gli AMS. AMIs Per ulteriori informazioni sugli argomenti SNS, consulta Cos'è Amazon Simple Notification Service?

Ogni volta che AMIs vengono rilasciate, inviamo notifiche agli abbonati dell'argomento corrispondente; questa sezione descrive come iscriversi alle notifiche AMI AMS.

Messaggio di esempio


```
{
  "Type" : "Notification",
  "MessageId" : "example messageId",
  "TopicArn" : "arn:aws:sns:us-east-1:591688410472:customer-ams-windows2019",
  "Subject" : "New AMS AMIs are Now Available",
  "Message" : "{"v1": {"Message": "A new version of the AMS Amazon Machine Images has
 been released. You are now able to launch new EC2 stacks from these AMIs.
  Please use this time to update any dependencies such as CloudFormation or Autoscaling
 groups. Release Notes Windows - Contains latest Windows Patches:
  Microsoft Windows Server 2008 R2 Datacenter - (KB2819745, KB3018238, KB4507004,
 KB4507437) Microsoft Windows Server 2016 Datacenter Security Enhancedn - (KB4509091,
 KB4507459)
  Microsoft Windows Server 2016 Datacentern - (KB4509091, KB4507459) Microsoft Windows
 Server 2012 R2 Security Enhancedn - (KB3191564, KB3003057, KB3013172, KB3185319,
 KB4504418,
  KB4506996, KB4507463) Microsoft Windows Server 2012 R2 Standardn - (KB3003057,
 KB3013172, KB3185319, KB4504418, KB4506996, KB4507463) Linux - Contains latest Linux
 patches -
  All AMIs now force domainjoin-cli leave before domainjoin-cli join for better
 stability in the domain join process.", "images":
  {"images": {"image_name": "customer-ams-windows2019-2021.08-1", "image_id":
 "ami-05dfa45396fddaa5e"}}, "region": "us-east-1"}}",
  "Timestamp" : "2021-09-03T19:05:57.882Z",
  "SignatureVersion" : "1",
  "Signature" : "example sig",
  "SigningCertURL" : "example url",
  "UnsubscribeURL" : "example url"
}
```


Possibili argomenti AMI AMS a cui abbonarsi:

- TUTTI: Usa`customer-ams-all-amis`. L'abbonamento a questo argomento ti avvisa quando uno degli AMS AMIs viene aggiornato.

- AMS AWS Linux AMIs: per Amazon Linux, usa `customer-ams-amazon1` `ecustomer-ams-amazon1-security-enhanced`. Per Amazon Linux 2, usa `customer-ams-amazon2` `ecustomer-ams-amazon2-security-enhanced`.
- AMS SUSE Linux AMIs: usa `customer-ams-sles12` `ocustomer-ams-sles15`.
- AMS AWS RedHat AMIs: Usa `customer-ams-rhel8``customer-ams-rhel8-security-enhanced`,,`customer-ams-rhel7`,`customer-ams-rhel7-security-enhanced`.
- AMS AWS CentOs AMIs: Usa`customer-ams-centos7`,`customer-ams-centos7-security-enhanced`.
- AMS Ubuntu AMIs: Usa`customer-ams-ubuntu18`.
- AMS AWS Windows AMIs: usa `customer-ams-windows2019``customer-ams-windows2019-security-enhanced`,`customer-ams-windows2016`,`customer-ams-windows2016-security-enhanced`,`customer-ams-windows2012`,`customer-ams-windows2012r2`,`customer-ams-windows2012r2-security-enhanced`,`customer-ams-windows2022`.

Per abbonarsi alle nuove notifiche AMI di AMS utilizzando la console Amazon SNS:

1. Apri la console Amazon SNS nella dashboard.
2. Nell'angolo in alto a destra, passa alla regione AWS per la quale AMIs ti stai abbonando.
3. Nel riquadro di navigazione a sinistra, scegli Abbonamenti, quindi scegli Crea abbonamento.
4. Inserisci le informazioni che seguono:

    a. Argomento ARN: `arn:aws:sns:{`*`REGION`*`}:287847593866:{`*`AMS_AMI_NAME`*`}` dove REGION è la regione AWS selezionata (dove è stata creata la notifica SNS) e AMS_AMI_NAME è l'AMI per cui desideri ricevere notifiche. Esempi:

    - Per iscriverti alle notifiche del nuovo AMS Amazon Linux AMIs nella regione AWS us-east-1, usa questo argomento ARN =. `arn:aws:sns:us-east-1:287847593866:customer-ams-amazon1`
    - Per iscriverti alle notifiche del nuovo AMS Window Server 2016 AMIs nella regione AWS us-west-2, usa questo argomento ARN = `arn:aws:sns:us-west-2:287847593866:customer-ams-windows2016`

    b. Per Protocollo, scegli E-mail.

    c. In Endpoint immetti l'indirizzo e-mail utilizzabile per ricevere le notifiche. Consigliamo una lista di distribuzione anziché l'e-mail di un individuo.

5. Scegli Create Subscription (Crea sottoscrizione).
6. Quando ricevi un'e-mail di conferma con l'oggetto «AWS Notification - Subscription Confirmation», apri l'e-mail e scegli Conferma abbonamento per completare l'abbonamento.

> **Note**
>
> Non sei limitato all'invio di e-mail per il Protocollo. Per informazioni su altri protocolli accettabili e su come utilizzarli, consulta subscribe.

Per annullare l'iscrizione alle nuove notifiche AMI di AMS utilizzando la console AWS SNS:

1. Apri la console Amazon SNS nella dashboard.
2. Nella barra di navigazione, passa alla regione AWS di tua scelta. È necessario utilizzare la regione AWS in cui si desidera ricevere le notifiche relative alla regione AWS corrispondente AMIs.
3. Nel pannello di navigazione, scegli Abbonamenti, seleziona l'abbonamento, quindi scegli Azioni -> Elimina abbonamenti.
4. Quando viene richiesta la conferma, seleziona Delete (Elimina).

Per abbonarsi alle notifiche AMS New AMI utilizzando Deployment | Ingestion | Stack from CloudFormation Template | Create (ct-36cn2avfrrj9v):

1. Per sottoscrivere AmazonLinuxSubscription, creare e salvare un file JSON con i parametri di esecuzione; questo esempio lo chiama .json: CreateSubscribeAmiParams

```
{
    "AWSTemplateFormatVersion": "2010-09-09",
    "Resources": {
        "AmazonLinuxSubscription":{
              "Type" : "AWS::SNS::Subscription",
              "Properties": {
                "TopicArn": "arn:aws:sns:{REGION}:287847593866:{AMS_AMI_NAME}",
                "Protocol": "email",
                "Endpoint": "username@yourdomain.com"
            }
        }
      }
```

```
}
```

2. Create e salvate il file JSON dei parametri RFC con il seguente contenuto; questo esempio lo chiama file.json: CreateSubscribeAmiRfc

```
{
   "ChangeTypeId": "ct-36cn2avfrrj9v",
   "ChangeTypeVersion": "1.0",
   "Title": "cfn-ingest-subscribe-ami"
}
```

3. Crea l'RFC, specificando il file e il file: CreateSubscribeAmiRfc CreateSubscribeAmiParams

```
aws amscm create-rfc --cli-input-json file://CreateSubscribeAmiRfc.json  --
execution-parameters file://CreateSubscribeAmiParams.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 esempi di creazione AMIs, consulta Creare AMI.

Per informazioni sul consumo AMIs programmatico, consulta EC2 stack: creating.

Notifiche di servizio

AMS invia richieste di servizio in uscita, o notifiche di servizio, quando devi agire o essere a conoscenza di qualcosa che potrebbe influire sul tuo account o sulle tue risorse, tra cui:

- Impatto sull'infrastruttura: AMS invia una notifica di servizio quando c'è un servizio AWS sottostante che influisce sull'infrastruttura e devi intervenire prima di una certa data, altrimenti potresti avere un'interruzione.
- EC2 Problemi hardware: AMS invia notifiche di servizio per problemi EC2 hardware che richiedono il riavvio di un' EC2 istanza prima di una certa data o per informarti che AMS riavvierà l'istanza automaticamente. Si tratta di un avviso importante perché il riavvio può causare un'interruzione ed è necessario rispondere con una data accettabile o creare un RFC con ct-09qbhy7kvtxqw per riavviare l'istanza autonomamente. Una notifica di servizio come questa si chiude automaticamente dopo cinque giorni se non rispondi.

Notifiche di modifica dello stato RFC

AMS offre notifiche per le modifiche dello stato RFC tramite e-mail ed CloudWatch eventi:

- E-mail tramite la console AMS: nella seconda pagina della procedura guidata di creazione RFC è disponibile un'opzione, in cui è possibile aggiungere fino a cinque indirizzi e-mail per ricevere una notifica quando lo stato RFC cambia.
- CloudWatch Eventi: puoi configurare regole e obiettivi diversi per CloudWatch Events per ricevere notifiche per ogni modifica dello stato RFC.

Notifiche e-mail

È possibile aggiungere indirizzi e-mail per ricevere le modifiche dello stato RFC a un RFC creato nella console AMS o utilizzando l'API/CLI AMS.

Nella console AMS, utilizza l'opzione Notifiche e-mail, nella seconda pagina della procedura guidata Crea RFC:

Nell'API/CLI AMS, aggiungi una riga come questa alla sezione dei parametri RFC della tua RFC (non aggiungere la riga alla sezione dei parametri di esecuzione):

```
--notification "{\"Email\": {\"EmailRecipients\" : [\"email@example.com\"]}}"
```

Il comportamento delle notifiche varia a seconda del tipo di pianificazione RFC:

- Notifiche e-mail di RFCs ricezione programmate su: Inviate, Pianificate, Completate, Rifiutate InProgress, Annullate, Rifiutate automaticamente o Annullate automaticamente.
- RFCs Ricevi al più presto una notifica e-mail su: Inviato, Completato, Rifiutato InProgress, Annullato o Annullato automaticamente. AutoRejected

> **Note**
>
> - Le notifiche e-mail vengono inviate da questo indirizzo:. `no-reply@managedservices.amazonaws.com`

- I caratteri speciali e URLs il titolo RFC sono oscurati nelle e-mail che inviamo. Si tratta di una misura di sicurezza.

CloudWatch Notifiche di eventi

AMS offre notifiche push per le modifiche dello stato RFC tramite CloudWatch Events. Per ricevere queste notifiche:

1. Crea un argomento e un abbonamento a cui verranno inviate le notifiche. Puoi assegnare all'argomento il nome che preferisci; per informazioni su questa operazione, consulta Argomento e sottoscrizione SNS: creazione.
2. Invia una RFC con Management | Other | Other | Crea un tipo di modifica e includi l'argomento e l'abbonamento SNS nella richiesta di avvisi di modifica dello stato RFC.

Quando invii la richiesta RFC Management | Other | Other per questa funzionalità, puoi specificare quali modifiche allo stato RFC ti interessa ricevere notifiche e quali tipi di modifica, e impostare altri filtri. Ad esempio, potresti voler richiedere di essere avvisato solo quando i tipi di modifica di Admin Access sono EventType = RfcSubmitted e EventType =. RfcUpdated

Questo è un modello di notifiche di CloudWatch eventi che puoi ricevere (con tutti i valori possibili):

```
{
    "source ": "aws.managedservices",
    "detail-type": "AMS RFC State Change",
    "detail": {
        "ActionState": "null | AwsActionPending | AwsOperatorAssigned |
 CustomerActionPending | NotApplicable | NoActionPending",
        "ActualExecutionTimeRange": {
            "StartTime": "null | Actual Start Time",
            "EndTime": "null | Actual End Time"
        },
        "AutomationStatus": "Automated | Manual",
        "AwsAccountId": "AWS Account ID",
        "AwsApprovalStatus": "null | SubmissionPending | NotRequired | ApprovalPending
 | Rejected | Approved",
        "ChangeTypeId": "Change_Type_ID",
        "ChangeTypeVersion": "Change_Type_Version",
        "CreatedTime": "Created_Time",
```

```
        "CustomerApprovalStatus": "null | SubmissionPending | NotRequired |
 ApprovalPending | Rejected | Approved",
        "EventType": "RfcActionStateUpdated | RfcApproved | RfcAutoRejected |
 RfcCanceled | RfcCompleted | RfcCreated | RfcInProgress | RfcRejected | RfcSubmitted |
 RfcUpdated",
        "LastModifiedTime": "Last_Updated_Time",
        "LastSubmittedTime": "null | Last_Submitted_Time",
        "RequestedExecutionTimeRange": {
            "StartTime": "null | Expected_Start_Time",
            "EndTime": "null | Expected_End_Time"
        },
        "RfcId": "RFC_ID",
        "Status": "Editing | PendingApproval | Scheduled | Rejected | Canceled |
 ExecutionLock | InProgress | Success | Failure",
        "Title": "Title"
    }
}
```

Le modifiche di stato RFC supportate (EventType), così come appaiono nella notifica effettiva degli CloudWatch eventi, sono:

- RfcActionStateUpdated (nessuna opzione della console AMS): la RFC in uno degli stati, descritti più avanti, è cambiata.
- RfcApproved (nessuna opzione console AMS): la RFC ha superato la convalida dell'operatore and/or AMS del sistema ed è stata approvata per il completamento.
- RfcAutoRejected (Rifiutato automaticamente): La RFC non ha superato la convalida del sistema o dell'operatore AMS ed è stata rifiutata.
- RfcCanceled (Annullato o annullato automaticamente): La RFC è stata annullata dal mittente o da un operatore AMS.
- RfcCompleted (Completato): I parametri di esecuzione RFC sono stati completati, inclusi. UserData
- RfcCreated (nessuna opzione della console AMS): l'RFC è stato creato correttamente (i parametri JSON e inviati erano validi).
- RfcInProgress (InProgress): L'esecuzione RFC è ancora in corso.
- RfcRejected (Rifiutato): Il sistema RFC fallito o la convalida dell'operatore AMS sono stati rifiutati.
- RfcSubmitted (Inviata): La RFC è stata inviata ed è in fase di convalida del sistema.
- RfcUpdated (nessuna opzione console AMS): la RFC è stata aggiornata manualmente da un operatore AMS.

Inoltre, puoi inviare notifiche relative CloudWatch agli eventi (CWE) a qualsiasi destinazione supportata e creare sistemi personalizzati sulla base di queste notifiche automatiche:

- EC2 Istanze Amazon
- AWS Lambda funzioni
- Flussi in Amazon Kinesis Data Streams
- Flussi di distribuzione in Amazon Data Firehose
- Gruppi di log in Amazon CloudWatch Logs
- Attività di Amazon ECS
- Run Command di Systems Manager
- Systems Manager Automation
- AWS Batch lavori
- Macchine a stati di Step Functions
- Gasdotti in CodePipeline
- CodeBuild progetti
- Modelli di valutazione di Amazon Inspector
- Argomenti di Amazon SNS
- Code Amazon SQS
- Obiettivi predefiniti: chiamata EC2 CreateSnapshot EC2 RebootInstances API, chiamata EC2 StopInstances API, chiamata EC2 TerminateInstances API e chiamata API.
- Il bus di eventi predefinito di un altro account AWS

> **Note**
>
> Inviamo notifiche CloudWatch sugli eventi per le modifiche dello stato RFC, con la massima diligenza possibile.

Configurazione di DNS privati e pubblici

Durante l'onboarding, AMS imposta un servizio DNS privato per le comunicazioni tra le risorse gestite e AMS.

È possibile utilizzare AMS Route 53 per gestire i nomi DNS interni per le risorse delle applicazioni (server Web, server delle applicazioni, database e così via) senza esporre queste informazioni alla rete Internet pubblica. Ciò aggiunge un ulteriore livello di sicurezza e consente anche di eseguire il failover da una risorsa primaria a una secondaria (spesso chiamata «flip») mappando il nome DNS su un indirizzo IP diverso.

Dopo aver creato risorse DNS private utilizzando Deployment | Advanced stack components | DNS (privato) | Creazione (ct-0c38gftq56zj6) o Deployment | Advanced stack components | DNS (pubblico) | Creazione (ct-0vzsr2nyraedl), puoi utilizzare Gestione | Componenti stack avanzati | DNS (privato) | Aggiornamento (ct-1d55pi44ff21u) e Gestione | Componenti stack avanzati | DNS (pubblico) | Aggiornamento (ct-1hzofpphabs3i), CTs per configurare set di record aggiuntivi o aggiornare set di record esistenti. Per gli account multi-account landing zone (MALZ), le risorse DNS create nell'account dell'applicazione VPCs possono essere condivise con l'account di servizi condivisi VPC per mantenere il DNS centralizzato utilizzando AMS AD.

MALZ

L'immagine seguente illustra una possibile configurazione DNS per Multi-Account Landing Zone AMS. Illustra una configurazione DNS ibrida tra AMS e una tipica rete di clienti. Un Canonical Name Record (CNAME) nel server DNS della rete del cliente viene inoltrato all'AMS AD DNS nell'account dei servizi condivisi con un inoltro condizionale in cui il CNAME del nome di dominio completo AMS viene inoltrato al record A.

SALZ

Il grafico seguente illustra una possibile configurazione DNS per single-account landing zone (SALZ). Mostra una configurazione DNS ibrida tra AMS e una tipica rete di clienti. Un CNAME nel server DNS della rete del cliente inoltra all'AMS AD DNS con un inoltro condizionale che ha il CNAME dell'FQDN AMS inoltrato al record A.

SALZ Route53 DNS

Il grafico seguente illustra una possibile configurazione DNS per single-account landing zone (SALZ). Mostra una configurazione DNS ibrida tra AMS e una tipica rete di clienti. Un CNAME nel server DNS della rete del cliente inoltra all'AMS AD DNS con un inoltro condizionale che ha il CNAME dell'FQDN AMS inoltrato al record A. Ciò sfrutta anche Route53 per il traffico di rete in uscita in modo che qualsiasi applicazione dell'account possa avere la risoluzione DNS nell'account con la massima disponibilità.

Percorsi di risoluzione abilitati per Route53:

- Istanza che tenta di risolvere il nome AMS MAD --> VPC +2 (Route53/ AmazonProvided DNS) --> Server d'inoltro condizionale valutati -> Regola d'inoltro condizionale Route53 MAD corrispondente --> Resolver Route53 in uscita --> AD DNS gestito
- Istanza che tenta di risolvere il nome locale del cliente --> VPC +2 (Route53/ AmazonProvided DNS) --> Sono stati valutati gli inoltratori condizionali --> La regola dell'inoltro condizionale locale di Route53 corrisponde -> Resolver in uscita Route53 --> DNS locale del cliente
- Istanza che tenta di risolvere il nome Internet --> VPC +2 (Route53/ AmazonProvided DNS) --> Inoltro condizionale valutato --> Nessun server d'inoltro corrispondente --> Servizio DNS Internet

Per ulteriori informazioni, consulta Utilizzo del DNS con il VPC e Utilizzo delle zone ospitate private.

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.

Implementazione di risorse IAM in AMS Advanced

AMS distribuisce le risorse IAM nell'applicazione multi-account landing zone (MALZ) e negli account single-account landing zone (SALZ) in due modi:

- Provisioning IAM automatizzato: questa funzionalità di AMS consente di inviare, creare, aggiornare o eliminare tipi di modifica per il provisioning di ruoli o policy IAM, senza la revisione dell'operatore e con IAM e AMS, i controlli di convalida vengono eseguiti automaticamente.

  Questa funzionalità deve essere abilitata esplicitamente con Management | Managed account | AMS Automated IAM Provisioning con autorizzazioni di lettura/scrittura | Enable (revisione richiesta) change type (ct-1706xvvk6j9hf). Per ulteriori informazioni, consulta Provisioning IAM automatizzato (AMS). Dopo aver abilitato AMS Automated IAM Provisioning, avrai accesso ai tipi di modifica Create, Update ed Delete per gestire le risorse IAM.

- Revisione del tipo di modifica IAM richiesto: questo tipo di modifica, Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entità o policy (revisione richiesta) (ct-3dpd8mdd9jn1r), richiede una revisione da parte dell'operatore AMS, che a volte può richiedere alcuni giorni per essere completata se sono necessari chiarimenti.

> **Note**
>
> Indipendentemente dal metodo utilizzato, viene assegnato un ruolo IAM all'account o agli account pertinenti e, una volta assegnato il ruolo, è necessario inserire il ruolo nella soluzione di federazione.

Provisioning IAM automatizzato (AMS)

AWS Managed Services (AMS) supporta la convalida e il provisioning automatizzati per le risorse IAM, inclusi ruoli e policy, utilizzando AMS Advanced requests for change (RFCs) e new change types (). CTs In precedenza, queste richieste venivano sottoposte a un processo semiautomatico che a volte comportava lunghi tempi di attesa. Ora puoi utilizzare AMS Automated IAM Provisioning per fornire risorse IAM e ottenere risultati molto più rapidamente.

Come funziona il provisioning IAM automatizzato in AMS

Il provisioning IAM automatizzato si basa su controlli automatici in fase di esecuzione per consentire a IAM di convalidare le modifiche alle risorse IAM. Questi controlli automatici, eseguiti quando vengono eseguiti i tipi di modifica Create, Update o Delete, impediscono l'implementazione di risorse IAM eccessivamente permissive o con schemi non sicuri nell'account. Ciò ti consente di abbinare il livello di rigore delle revisioni IAM all'esperienza del tuo team. Consigliamo ai team che non conoscono i servizi cloud e necessitano di controlli manuali per tutte le modifiche alle risorse IAM di utilizzare il tipo di modifica esistente obbligatorio per la revisione: Deployment | Advanced stack components | Identity and Access Management (IAM) and Access Management (IAM) | Create entità o policy (review required), (ct-3dpd8mdd9jn1r). I team con AWS esperienza e controllo dei propri ambienti possono utilizzare il provisioning IAM automatizzato per velocizzare le implementazioni. È possibile utilizzare questa funzionalità per eseguire la convalida tramite controlli automatici in fase di esecuzione o per eseguire la convalida e il provisioning delle risorse IAM dopo una convalida riuscita.

Important

AWS Managed Services ha implementato in modo proattivo un elenco di controlli di runtime di convalida che impediscono la creazione di risorse o policy IAM con determinate autorizzazioni e condizioni. Per una descrizione di questi privilegi e condizioni, consulta Implementazione delle risorse IAM in AMS Advanced. I tipi di modifica automatizzata ct-1n9gfnog5x7fl, ct-1e0xmuy1diafq e ct-17cj84y7632o6 consentono agli utenti esperti nella gestione delle risorse IAM di fornire ruoli e policy IAM che consentono azioni oltre i privilegi di sola lettura.

Inoltre, è possibile utilizzare i ruoli creati tramite i tipi di modifica automatizzata ct-1n9gfnog5x7fl, ct-1e0xmuy1diafq e ct-17cj84y7632o6 per creare le nuove risorse. Tuttavia, le risorse non possono seguire lo standard di denominazione AMS e non fanno parte dello stack AMS standard. AMS fornisce il supporto operativo e di sicurezza di tali risorse specifiche con il massimo impegno.

Sebbene sia i processi manuali che quelli automatizzati mirino a rispettare i nostri standard di sicurezza, è importante notare che esistono differenze nei controlli tra i due. Il provisioning automatizzato consente una maggiore flessibilità nella creazione e nell'aggiornamento di ruoli e policy, pertanto non sono la stessa cosa. Si consiglia all'organizzazione di esaminare attentamente i controlli del runtime di convalida elencati nella Guida per l'utente AMS per assicurarsi che siano in linea con le aspettative e i requisiti dell'organizzazione.

Flusso di convalida

Flusso di convalida e approvvigionamento

Note

Questa funzionalità è adatta ai team che hanno esperienza con le risorse IAM AWS e non la consigliamo ai team alle prime armi. AWS Il processo di convalida automatizzato è progettato per catturare la maggior parte degli errori ed è utile ai team per ottenere revisioni rapide delle modifiche a IAM, quando comprendono le autorizzazioni di cui hanno bisogno. Per utilizzare i nuovi tipi di modifica in modo sicuro ed efficace, ti consigliamo di avere una buona conoscenza di AWS IAM e dei controlli in fase di esecuzione offerti dai tipi di modifica per determinare se sono adatti al tuo team.

Introduzione al provisioning IAM automatizzato di AMS in AMS

Per utilizzare i nuovi tipi di modifica, abilita innanzitutto AMS Automated IAM Provisioning inviando una RFC utilizzando il seguente tipo di modifica: Gestione | Account gestito | AMS Automated IAM Provisioning con autorizzazioni di lettura/scrittura | Abilita (è richiesta la revisione) (ct-1706xvvk6j9hf). AWS richiede che l'organizzazione si sottoponga a un processo di gestione dei rischi di sicurezza dei clienti (CSRM) per garantire che l'uso di questi tipi di modifiche sia allineato alle politiche organizzative. Il team AWS operativo collabora con voi per ottenere l'approvazione esplicita dal vostro referente del team di sicurezza sotto forma di accettazione del rischio nell'ambito della revisione richiesta. Per ulteriori informazioni, consulta il processo di gestione del rischio dei clienti (CSRM) di RFC.

Una volta completata la richiesta di attivazione della funzionalità AMS Automated IAM Provisioning con autorizzazioni di lettura/scrittura, AMS abilita i tipi di modifica di AMS Automated IAM Provisioning nell'account utilizzato per inviare la RFC di abilitazione. Per confermare che AMS Automated IAM Provisioning sia attivato su un account, controlla il ruolo nella console IAM. `AWSManagedServicesIAMProvisionAdminRole`

Come parte dell'onboarding, AMS fornisce IAM Access Analyzer nella stessa regione AWS dell'account per sfruttare la sua funzionalità di anteprima degli accessi. IAM Access Analyzer aiuta a identificare le risorse dell'organizzazione e gli account condivisi con un'entità esterna, convalida le politiche IAM rispetto alla grammatica e alle best practice delle policy e genera policy IAM basate sull'attività di accesso nei log. AWS CloudTrail Per ulteriori informazioni, consulta Using. AWS Identity and Access Management Access Analyzer

Una volta effettuato l'onboarding, `AWSManagedServicesIAMProvisionAdminRole` viene distribuito agli account abilitati. Se scegli di utilizzare questo ruolo tramite la federazione SAML, devi inserire il ruolo nella tua soluzione di federazione.

Come parte dell'onboarding, puoi richiedere di aggiornare la policy di fiducia IAMProvision AdminRole di AWSManaged Services per concedere un altro ruolo IAM utilizzando ARN per assumere questo ruolo. AWS Security Token Service

Utilizzo del provisioning IAM automatizzato di AMS in AMS

Puoi creare RFCs con i seguenti tipi di modifica di AMS Automated IAM Provisioning.

Note

- È supportato solo il provisioning in base a ruoli e policy.

  Durante l'aggiornamento dei ruoli, l'Update CT sostituisce l'elenco esistente di Amazon resource names (ARNs) con policy gestite e il documento relativo alla policy «assume role», con l'elenco fornito di policy gestite ARNs e il documento di policy «assume role». In un aggiornamento parziale, ad esempio, l'aggiunta o la rimozione di un ARN nell'elenco esistente di policy gestite ARNs, non è consentito aggiungere o rimuovere singole dichiarazioni di policy al documento di policy «assumi ruolo». Analogamente, durante l'aggiornamento delle politiche, l'Update CT sostituisce il documento di policy esistente e non consente di aggiungere o rimuovere singole dichiarazioni politiche nel documento politico esistente.
- Quando è selezionata l'opzione «convalida solo», i controlli in fase di esecuzione vengono eseguiti senza fornire alcuna entità o policy IAM. Indipendentemente dai risultati, lo stato RFC è «riuscito». Lo stato «successo» indica una convalida riuscita rispetto all'entità o alla policy IAM fornita.

- Distribuzione | Advanced Stack Components | Identity and Access Management (IAM) | Crea entità o policy (autorizzazioni di lettura/scrittura) (ct-1n9gfnog5x7fl): una nuova entità o policy IAM viene convalidata e fornita automaticamente.
- Gestione | Advanced Stack Components | Identity and Access Management (IAM) | Aggiorna entità o policy (autorizzazioni di lettura/scrittura) (ct-1e0xmuy1diafq): un'entità o policy IAM esistente viene aggiornata e convalidata automaticamente.
- Gestione | Advanced Stack Components | Identity and Access Management (IAM) | Elimina entità o policy (autorizzazioni di lettura/scrittura) (ct-17cj84y7632o6): viene eliminata un'entità o policy IAM esistente il cui provisioning utilizza il tipo di modifica automatica dell'entità o della policy di creazione.

Puoi chiamare solo i tre precedenti utilizzando un ruolo IAM dedicato:. CTs `AWSManagedServicesIAMProvisionAdminRole` Questo ruolo è disponibile solo negli account che sono stati inseriti nella funzionalità utilizzando le autorizzazioni di lettura/scrittura Gestione | Account gestito | AMS Automated IAM Provisioning | Abilita (è richiesta la revisione) (ct-1706xvvk6j9hf).

> **Important**
>
> I tipi di modifica Crea, Aggiorna ed Elimina sono sempre visibili nel tuo account, ma non sono attivati per impostazione predefinita. Se provi a inviare una RFC utilizzando uno di questi tipi di modifica senza prima abilitare la funzionalità AMS Automated IAM Provisioning, viene visualizzato un errore «non autorizzato».

Limitazioni:

- Il Create CT potrebbe consentire di creare un ruolo o una policy IAM con l'autorizzazione a creare risorse. AWS Tuttavia, AWS le risorse create da questi ruoli e politiche non sono gestite da AMS. È consigliabile attenersi al controllo organizzativo per limitare la creazione di tali ruoli o politiche.
- L'Update CT non può modificare i ruoli e le politiche IAM creati con CFN Ingest, Direct Change Mode, Developer Mode o, in alcuni casi, tramite AMS Advanced esistente in modo manuale o automatizzato. CTs
- Il Delete CT non può eliminare ruoli o politiche esistenti che non sono stati creati con AMS Automated IAM Provisioning Create CT.
- La funzionalità AMS Automated IAM Provisioning con autorizzazioni di lettura/scrittura non è supportata nei ruoli in modalità Direct Change. Ciò significa che non è possibile fornire o aggiornare ruoli e policy IAM con autorizzazioni di lettura/scrittura utilizzando questi ruoli.
- I tipi di modifica Create, Update ed Delete di AMS Automated IAM con autorizzazioni di lettura/scrittura non sono compatibili con il Connector. ServiceNow

Controlli di runtime per AMS Automated IAM Provisioning in AMS

Automated IAM Provisioning sfrutta i controlli ed esegue controlli e convalide aggiuntivi rispetto alla policy limite di AMS. AWS Identity and Access Management Access Analyzer AMS ha definito i controlli e le convalide aggiuntivi sulla base delle migliori pratiche IAM, dell'esperienza di gestione del carico di lavoro dei clienti nel cloud e dell'esperienza collettiva di valutazione manuale AMS IAM.

È possibile visualizzare i risultati del controllo in fase di esecuzione delle politiche nell'output della richiesta di modifica (RFC). I risultati includono l'identificatore della risorsa, la posizione all'interno della and/or policy del ruolo che ha generato i risultati e un messaggio che illustra il controllo che l'entità o la risorsa IAM non è riuscita a superare. Questi risultati aiutano a creare policy funzionali e conformi alle migliori pratiche di sicurezza.

> **Note**
>
> L'IAM Provisioning automatizzato tenta di specificare la posizione all'interno della definizione di entità o policy che non supera il controllo. A seconda del tipo, la posizione può includere il nome della risorsa o l'ARN o l'indice all'interno di un array. Ad esempio, una dichiarazione per aiutarti a modificare l'entità o la politica per un esito positivo.

Per un'esperienza fluida di AMS Automated IAM Provisioning, è consigliabile utilizzare l'opzione «validate only» per eseguire i controlli di convalida fino a quando non ci sono risultati dai controlli di convalida riportati negli output RFC. Se i controlli di convalida non riportano alcun risultato, scegli Crea copia dalla console AMS per creare rapidamente una copia della RFC esistente. Quando sei pronto per il provisioning, nella sezione Parametri, cambia il valore Validate only da Sì a No, quindi procedi.

Questi sono i controlli in fase di esecuzione eseguiti da AMS Automated IAM Provisioning per garantire la sicurezza delle risorse IAM:

> **Note**
>
> Per effettuare il provisioning delle policy IAM che contengono azioni negate da questi tipi di modifiche automatizzate, è necessario seguire il processo RFC Customer Security Risk Management (CSRM). Utilizza il seguente tipo di modifica: Deployment | Advanced stack components | Identity and Access Management (IAM) and Access Management (IAM) | Crea entità o policy (revisione richiesta) (ct-3dpd8mdd9jn1r).

- Verifica e convalida delle policy di IAM Access Analyzer: consulta anche il riferimento per il controllo delle policy di Access Analyzer e la convalida delle policy di IAM Access Analyzer.
- Controlli della politica dei limiti delle autorizzazioni AMS: azioni su una serie di servizi che vengono negate per impostazione predefinita. Per ulteriori informazioni, consulta Controllo dei limiti delle autorizzazioni di Automated IAM Provisioning.
- Controlli delle politiche relative ai limiti delle autorizzazioni definite dal cliente: ulteriori azioni limitate su una serie di servizi che vengono negate. Per ulteriori informazioni, consulta Controllo dei limiti delle autorizzazioni di IAM Provisioning automatizzato.

- Controlli personalizzati definiti da AMS: controlli che identificano varie policy o modelli di accesso non sicuri ed eccessivamente permissivi all'interno di un'entità o policy IAM richiesta e negano la richiesta se ne trova una. Per informazioni, consulta JSON policy elements: Principal.AWS

Risultato	Descrizione
È possibile accedere al ruolo da un account esterno che non rientra nella propria zona di fiducia.	Questo risultato si riferisce a un responsab ile elencato nella politica sulla fiducia dei ruoli che non rientra nella zona di fiducia dell'utente. Una zona di fiducia è definita come l'account a cui viene creato il ruolo o l' AWS organizza zione a cui appartiene l'account. Un'entità che non appartiene all'account o alla stessa AWS organizzazione è un'entità esterna. Per risolvere il problema, controlla l'ID dell'account nell'account principale ARNs e assicurati che appartenga a te e che sia un account registrato da AMS.
Al ruolo può accedere un'entità esterna di proprietà di un account *External_Account_ID* che non è di proprietà dell'account proprietario del cliente AMS. *Account_ID*	Questo risultato viene generato se la policy di trust dei ruoli include un ARN principale con un ID account non di tua proprietà e un account integrato da AMS. Per risolvere questo problema, rimuovi qualsiasi principio di questo tipo dalla politica di fiducia dei ruoli.
L'ID utente canonico non è un principio supportato nella policy di fiducia IAM.	I principi canonici non IDs sono supportati nella policy di fiducia IAM. Per risolvere il problema, rimuovi qualsiasi principio di questo tipo dalla policy di fiducia dei ruoli.
È possibile accedere al ruolo tramite un'identità web esterna che non rientra nella propria zona di fiducia.	Questo risultato viene generato se la policy di trust del ruolo consente un provider di identità Web (IdP) esterno diverso da SAML IdP. Per risolvere questo problema, esamina la policy sulla fiducia dei ruoli e rimuovi le dichiaraz

Risultato	Descrizione
	ioni che consentono l'operazione. `sts:AssumeRoleWithWebIdentity`
È possibile accedere al ruolo tramite la federazione SAML; tuttavia, il provider di identità SAML (IdP) fornito non esiste.	Questo risultato viene generato se la policy di attendibilità dei ruoli contiene un IdP SAML che non esiste nel tuo account. Per risolvere il problema, assicurati che tutti gli IdP SAML elencati siano presenti nel tuo account.
La policy contiene azioni privilegiate equivalenti all'accesso da amministratore o utente esperto. Valuta la possibilità di ridurre l'ambito delle autorizzazioni a un servizio, un'azione o una risorsa specifici. Se NotResourcevengono utilizzati elementi di policy avanzati come NotActiono, assicurati che non garantiscano un accesso maggiore di quello previsto, in particolare nelle istruzioni Allow.	La migliore pratica di sicurezza consiste nel AWS Identity and Access Management concedere solo le autorizzazioni necessarie per eseguire un'attività quando si impostano le autorizzazioni con le politiche IAM. A tale scopo, definisci le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Questo risultato viene generato quando l'automazione rileva che la politica concede autorizzazioni ampie e non rispetta il principio del privilegio minimo. Per risolvere il problema, rivedi e riduci le autorizzazioni.

Risultato	Descrizione
L'informativa contiene azioni privilegiate per. *Service_Name* Valuta la possibilità di escludere queste azioni con una dichiaraz ione di rifiuto. Fai riferimento al riferimento alla politica dei confini nella documentazione AMS per un elenco di azioni privilegiate.	AMS ha identificato alcune azioni per un determinato servizio come rischiose e richiedon o un'ulteriore revisione e accettazione del rischio da parte del team di sicurezza del cliente. Questo risultato viene generato quando l'automazione rileva la determinata politica che concede tali autorizzazioni. Per risolvere questo problema, nega queste azioni nella tua politica. Per un elenco di azioni, consulta la politica dei confini di AMS. Per i dettagli sulla politica dei confini di AMS, vedere. Controllo dei limiti di autorizzazione AMS Automated IAM Provision ing
La dichiarazione consente l'accesso ai tipi di modifica RFC privilegiati: ct-1n9gfnog5x7fl, ct-1e0xmuy1diafq e ct-17cj84y7632o6 per il servizio. *Service_Name* Valuta la possibilità di definire l'ambito delle autorizzazioni per tipi di modifica specifici o di escludere questi tipi di modifica con una dichiarazione di negazione.	Questo risultato viene generato se la policy concede le autorizzazioni per eseguire azioni relative a RFC utilizzando i tipi di modifica di Automated IAM Provisioning (). CTs CTs Sono soggetti all'accettazione del rischio e devono essere utilizzati solo tramite ruoli integrati . Quindi, non puoi concedere il permesso a questi. CTs Per risolvere questo problema, nega le azioni RFC che li utilizzano. CTs

Risultato	Descrizione
L'informativa contiene azioni privilegiate che non rientrano nell'ambito delle risorse di servizio. *Service_Name* Valuta la possibilità di assegnare le azioni a risorse specifiche o di escludere le risorse con prefissi dello spazio dei nomi AMS. Se vengono utilizzati caratteri jolly, assicurati che limitino l'ambito alle tue risorse.	Questo risultato viene generato se la politica concede azioni privilegiate che non rientrano nell'ambito delle risorse del servizio specificato. Le wild card spesso creano politiche eccessiva mente permissive che includono un'ampia gamma di risorse o azioni nell'ambito dell'auto rizzazione. Per risolvere il problema, riduci l'ambito delle autorizzazioni alle risorse di tua proprietà o escludi le risorse che si trovano nel namespace AMS. Per un elenco dei prefissi dello spazio dei nomi AMS, consulta la politica dei limiti nella documentazione di AMS. Tieni presente che non tutti i prefissi si applicano a tutti i servizi. Per i dettagli sulla politica dei confini di AMS, vedere. Controllo dei limiti di autorizzazione AMS Automated IAM Provision ing
ID account o Amazon Resource Name (ARN) non valido.	Questo risultato viene generato se un ARN o un ID account specificato nella policy o nella policy di attendibilità del ruolo non è valido. Per esaminare le risorse ARN valide relative ai servizi, consulta il Service Authorization Reference. Assicurati che l'ID dell'account sia un numero di 12 cifre e che l'account sia attivo in. AWS
L'uso della wildcard (*) per l'ID dell'account in ARN è limitato.	Questo risultato viene generato se nel campo ID account di un ARN viene specificata una wild card (*). Una wild card nel campo ID dell'account corrisponde a qualsiasi account e potenzialmente concede autorizzazioni involontarie alle risorse. Per risolvere il problema, sostituisci la wild card con un ID account specifico.

Risultato	Descrizione
Account di risorse specificato non di proprietà dello stesso account *Account_ID* proprieta rio del cliente AMS.	Questo risultato viene generato se un ID account specificato nell'ARN di una risorsa non appartiene all'utente e non è gestito da AMS. Per risolvere questo problema, assicurati che tutte le risorse (come specificato dal relativo ARN nella policy) appartengano ai tuoi account gestiti da AMS.
Il nome del ruolo si trova nello spazio dei nomi con restrizioni AMS.	Questo risultato viene generato se si tenta di creare un ruolo con un nome che inizia con un prefisso riservato AMS. Per risolvere questo problema, utilizzate un nome per il ruolo specifico per il vostro caso d'uso. Per un elenco di prefissi riservati AMS, consulta Prefissi riservati AMS
Il nome della policy si trova nello spazio dei nomi con restrizioni AMS.	Questo risultato viene generato se si tenta di creare una policy con un nome che inizia con un prefisso riservato AMS. Per risolvere questo problema, utilizzate un nome per la policy specifico per il vostro caso d'uso. Per un elenco di prefissi riservati AMS, consulta Prefissi riservati AMS.
L'ID della risorsa nell'ARN si trova nello spazio dei nomi con restrizioni AMS.	Questo risultato viene generato se si tenta di creare una politica che conceda l'autoriz zazione a risorse denominate presenti nello spazio dei nomi AMS. Per risolvere questo problema, assicurati di definire l'ambito delle autorizzazioni per le tue risorse o di negare le autorizzazioni alle risorse che si trovano nello spazio dei nomi AMS. Per ulteriori informazi oni sugli spazi dei nomi AMS, consulta AMS Restricted namespaces.

Risultato	Descrizione
Caso di variabile di policy non valido. Aggiorna la variabile a. *Variable_Names*	Questo risultato viene generato se si tenta di creare una policy che contenga una variabile di policy globale IAM nel caso errato. Per risolvere questo problema, utilizza la maiuscola/minuscola corretta per le variabili globali nella tua policy. Per un elenco di variabili globali, consulta AWS Global Condition Context keys. Per ulteriori informazioni sulle variabili di policy, consulta IAM policy elements: Variables and tags
L'istruzione contiene azioni privilegiate che non rientrano nell'ambito delle chiavi KMS. Valuta la possibilità di assegnare queste autorizzazioni a chiavi specifiche o di escludere le chiavi di proprietà di AMS.	Questo risultato viene generato se la policy contiene autorizzazioni che non rientrano nell'ambito di specifiche chiavi KMS di tua proprietà. Per risolvere questo problema, concedi l'autorizzazione a chiavi specifiche o escludi le chiavi di proprietà di AMS. Le chiavi di proprietà di AMS hanno set di alias specifici . Per un elenco degli alias chiave di proprietà di AMS, vedere. Controllo dei limiti di autorizzazione AMS Automated IAM Provisioning
L'istruzione contiene azioni privilegiate che non rientrano nell'ambito degli alias delle chiavi KMS. Valuta la possibilità di assegnare queste autorizzazioni alle tue chiavi o alias oppure escludi gli alias chiave di proprietà di AMS.	Questo risultato viene generato se la policy contiene autorizzazioni che non rientrano nell'ambito di alias di chiavi KMS specifici di tua proprietà. Per risolvere questo problema, concedi l'autorizzazione a chiavi specifiche o escludi le chiavi di proprietà di AMS. Le chiavi di proprietà di AMS hanno set di alias specifici . Per un elenco degli alias chiave di proprietà di AMS, vedere. Controllo dei limiti di autorizzazione AMS Automated IAM Provisioning

Risultato	Descrizione
L'informativa contiene azioni privilegiate che non rientrano in modo adeguato nell'ambito delle chiavi KMS utilizzando il. `kms:ResourceAliases condition` Prendi in considerazione l'utilizzo di alias specifici insieme all'operatore di set appropriato per la chiave di condizione. Se vengono utilizzati caratteri jolly nei nomi degli alias, assicurati che limitino l'ambito a un set limitato di chiavi KMS.	Questo risultato viene generato se stai definendo l'ambito delle autorizzazioni per le tue chiavi KMS utilizzando le condizioni e non utilizzando gli alias `kms:ResourceAliases` per le tue chiavi KMS. Oppure, se la chiave di `kms:ResourceAliases` condizione ha un valore che include anche gli alias delle chiavi KMS di proprietà di AMS. Per risolvere questo problema, aggiorna la condizione in modo da limitare l'autorizzazione solo agli alias delle tue chiavi KMS o escludi gli alias per le chiavi KMS di proprietà di AMS. Per un elenco degli alias delle chiavi di proprietà di AMS, vedi. Controllo dei limiti di autorizzazione AMS Automated IAM Provisioning
Al ruolo deve essere allegato customer_deny_policy. Includi l'ARN della policy nell'elenco delle policy gestite. ARNs	Questo risultato viene generato se il ruolo che si sta creando non è `customer_deny_policy` associato. Per risolvere il problema, includetelo `customer_deny_policy` nell' ARNs elenco delle policy gestite.
La politica AWS gestita è eccessivamente permissiva o concede autorizzazioni limitate dalla politica dei confini di AMS.	Questo risultato viene generato se il ManagedPolicyArnsvalore del ruolo contiene una politica gestita da AMS che fornisce l'accesso completo o a livello di amministratore al servizio pertinente. Per risolvere questo problema, esamina l'utilizzo della politica AWS gestita e utilizza una politica che fornisca l'autorizzazione di ripartizione dell'ambito o definisci una politica personalizzata che segua il principio del privilegio minimo.

Risultato	Descrizione
La policy gestita dai clienti si trova in un namespace AMS limitato.	Questo risultato viene generato se al ruolo è associata una politica gestita dal cliente con il nome come prefisso nel AWS namespace. Per risolvere questo problema, rimuovi la policy dall'ManagedPolicyArnelenco per il ruolo.
La customer_deny_policy non può essere scollegata dal ruolo. Includi l'ARN della policy nell'elenco delle policy gestite. ARNs	Questo risultato viene generato se `customer_deny_policy` viene rimosso dal ruolo durante un aggiornamento. Per risolvere il problema, aggiungi il `customer_deny_policy` al ManagedPolicyArnscampo del ruolo e riprova.
Le politiche gestite dal cliente sono state fornite al di fuori del servizio AMS Change Management o senza previa convalida.	Questo risultato viene generato se una o più politiche gestite dai clienti esistenti ARNs sono associate a un ruolo e le politiche non vengono fornite tramite il servizio AMS Change Management (tramite una RFC). Ad esempio, Developer Mode o Direct Change Mode consentono ai clienti di fornire policy IAM senza una RFC. Per risolvere questo problema, rimuovi la policy gestita ARNs dal cliente dall'ManagedPolicyArnselenco per il ruolo.
Il numero di policy gestite fornite ARNs supera la policy allegata per quota di ruolo.	Questo risultato viene generato se il numero totale di policy gestite associate al ruolo supera la quota di policy per ruolo. Per ulteriori informazioni sulle quote IAM, consulta Quote IAM e AWS STS, requisiti dei nomi e limiti di caratteri. Utilizza queste informazioni per ridurre il numero di policy da associare al ruolo.

Risultato	Descrizione
La dimensione della policy di trust ({trust_policy}) supera la quota di {size} relativa alle dimensioni della policy di assunzione del ruolo.	Questo risultato viene generato se la dimensione del documento relativo alla politica di assunzione del ruolo supera la quota relativa alla dimensione della policy. Per ulteriori informazioni sulle quote IAM, consulta Quote IAM e AWS STS, requisiti dei nomi e limiti di caratteri.
L'informativa contiene tutte le azioni mutative per Amazon S3. Valuta la possibilità di estendere queste autorizzazioni solo alle azioni obbligatorie. Se vengono utilizzate delle wild card, assicuratevi che coprano un insieme limitato di azioni mutative.	Questo risultato viene generato se la policy specificata concede tutte le autorizzazioni mutative di Amazon Simple Storage Service indipendentemente da una o più risorse. Per risolvere questo problema, includi solo le azioni mutative richieste di Amazon S3 sui tuoi bucket.
L'istruzione contiene azioni privilegiate che non sono consentite su nessun bucket in Amazon S3. Valuta la possibilità di aggiungere una dichiarazione che neghi queste azioni.	Questo risultato viene generato se la politica concede azioni privilegiate su qualsiasi bucket. Per un elenco delle azioni privilegiate, consulta Controllo dei limiti di autorizzazione AMS Automated IAM Provisioning Per risolvere questo problema, rimuovi o nega queste azioni nella tua politica.
L'informativa contiene azioni privilegiate che non rientrano nell'ambito dei tuoi bucket in Amazon S3. Valuta la possibilità di includere o escludere i bucket con prefissi dei namespace AMS. Se vengono utilizzate delle wild card, assicuratevi che corrispondano ai bucket all'interno dei vostri namespace.	Questo risultato viene generato se la policy concede ad Amazon S3 azioni che non rientrano solo nell'ambito dei tuoi bucket. Ciò si verifica spesso se si utilizzano delle wild card per specificare le risorse del bucket. Per risolvere questo problema, specifica i nomi dei bucket o quelli di ARNs cui sei proprietario o escludi i bucket con prefissi dello spazio dei nomi AMS.

Risultato	Descrizione
L'informativa contiene azioni privilegiate che non rientrano nell'ambito dei tuoi bucket in Amazon S3. Valuta la possibilità di evitare l'uso di wild card (*) che coprono tutti i bucket dell'account.	Questo risultato viene generato se la policy concede ad Amazon S3 azioni che non rientrano nell'ambito del tuo bucket. Ciò si verifica spesso se si utilizzano delle wild card per specificare le risorse del bucket. Per risolvere questo problema, specifica i nomi dei bucket o quelli di ARNs cui sei proprietario o escludi i bucket con prefissi dello spazio dei nomi AMS.
L'istruzione contiene una wildcard di risorse valida per tutti i bucket Amazon S3, inclusi i bucket inesistenti e i bucket di cui non sei proprietario. Valuta la possibilità di definire l'ambito delle autorizzazioni utilizzando una condizione e una chiave di condizione. `s3:ResourceAccount`	Questo risultato viene generato se la policy concede l'autorizzazione ai bucket specificati utilizzando le wild card. L'uso delle wild card spesso rientra nell'ambito di applicazione dei bucket non esistenti o di cui non è proprietario. Per risolvere questo problema, usa condition e `aws:ResourceAccount` condition key per definire l'ambito dell'autorizzazione solo per i bucket all'interno dell'account corrente. Per ulteriori dettagli, consulta Limitare l'accesso ai bucket Amazon S3 di proprietà di account specifici. AWS
L'informativa contiene un elemento di `NotResource` policy, che può essere applicato a un gran numero di bucket, inclusi bucket inesistenti e bucket di cui non sei proprietario. Valuta la possibilità di definire l'ambito delle autorizzazioni utilizzando una condizione e una chiave di condizione. `s3:ResourceAccount`	Questo risultato viene generato se la policy utilizza l'elemento `NotResources` policy per specificare le risorse del bucket. L'utilizz o dell'`NotResource` elemento potrebbe riguardare un gran numero di bucket, inclusi bucket inesistenti o non proprietari. Per risolvere questo problema, utilizza le condizion i e la chiave di `aws:ResourceAccount` condizione per limitare l'autorizzazione ai bucket solo all'interno dell'account corrente.

Risultato	Descrizione
L'istruzione contiene azioni di Amazon S3 sui bucket *Bucket_Name* che non esistono, non appartengono all'account *Account_ID* o il nome contiene una wild card che potrebbe essere applicata a un gran numero di bucket, inclusi quelli inesistenti e quelli che non possiedi. Valuta la possibilità di definire l'ambito delle autorizzazioni utilizzando una condizione e la chiave di condizione `s3:ResourceAccount`	Questo risultato viene generato se la policy concede l'autorizzazione a bucket che non esistono, non sono di tua proprietà o contengono wild card nei nomi dei bucket che coprono un gran numero di bucket e l'accesso non è limitato solo all'account corrente. Per risolvere il problema, utilizza condition e `aws:ResourceAccount` condition key per definire l'ambito dell'autorizzazione solo per i bucket all'interno dell'account corrente.
L'istruzione contiene azioni di Amazon S3 su bucket *Bucket_Name* che non esistono, non sono di proprietà dell'account *Account_ID* oppure il nome contiene una wild card che potrebbe essere applicata a un gran numero di bucket, inclusi bucket inesistenti e bucket di cui non sei proprietario. L'accesso non è limitato all'utilizzo `s3:ResourceAccount` o all'account di risorse specificato nella condizione che non ti appartiene.	Questo risultato viene generato se la politica concede l'autorizzazione a bucket che non esistono, non sono di tua proprietà o contengono wild card nei nomi dei bucket che coprono un gran numero di bucket e l'accesso è limitato solo a un account specifico. Tuttavia, l'account specificato nella chiave di `aws:ResourceAccount` condizione non appartiene all'utente ed è gestito da AMS. Per risolvere questo problema, aggiorna la chiave `aws:ResourceAccount` condizionale e imposta l'ID dell'account appropriato che possiedi e che è gestito da AMS.
L'informativa contiene azioni privilegiate che non rientrano nell'ambito delle tue istanze per Amazon. EC2 Valuta la possibilità di assegnare le azioni a un'istanza specifica ARNs o di escludere le istanze che hanno la chiave Name tag con valore nei prefissi dello spazio dei nomi AMS. Se vengono utilizzate delle wild card, assicuratevi che corrispondano ai namespace di cui siete proprietari.	Questo risultato viene generato se la policy concede azioni privilegiate contro le EC2 istanze Amazon di proprietà di AMS. Le istanze AMS sono etichettate con la chiave Name tag con valori nello spazio dei nomi AMS. Per risolvere questo problema, specifica le tue risorse o escludi le istanze AMS con una condizione la cui `aws:ResourceTag/Name` chiave esclude i valori nello spazio dei nomi AMS utilizzando l'operatore `StringNotLike`

Risultato	Descrizione
L'istruzione contiene azioni privilegiate che non rientrano nell'ambito delle risorse nell'archivio dei parametri. AWS Systems Manager Valuta la possibilità ARNs di specificare i parametri o di escludere i parametri con i prefissi dello spazio dei nomi AMS. Se vengono utilizzate delle wild card, assicuratevi che includano solo i vostri parametri.	Questo risultato viene generato se la politica concede autorizzazioni per parametri di cui non sei proprietario. Di solito si tratta di quando vengono utilizzate wild card o quando i parametri con prefissi dello spazio dei nomi AMS sono elencati tra le risorse di una dichiarazione politica. Per risolvere questo problema, specificate i parametri che rientrano nel vostro namespace o escludete i parametri AMS con un'istruzione deny.
L'informativa contiene azioni privilegiate contro le risorse in. AWS Systems Manager Valuta la possibilità di definire l'ambito delle autorizza zioni per azioni di sola lettura o azioni contro le tue risorse.	Questo risultato viene generato se la policy concede autorizzazioni diverse dall'archivio dei parametri o dalle azioni di sola lettura sulle risorse di Systems Manager. Per risolvere questo problema, riduci le autorizzazioni alle azioni di sola lettura o alla sola memorizzazione dei parametri.
L'istruzione contiene azioni privilegiate che non rientrano nell'*`Service_Name`* ambito di {message} di tua proprietà. Valuta la possibili tà di assegnare queste autorizzazioni a tipi di risorse specifici, a seconda dei casi, o di escludere le risorse di proprietà di AMS. Se vengono utilizzate delle wild card, assicuratevi che corrispondano. *`Resources`*	Questo risultato viene generato se la politica consente azioni privilegiate che non sono concesse sulle risorse, in particolare per le risorse denominate. Per risolvere questo problema, esamina l'elenco delle risorse e verifica se riguardano solo le risorse che si trovano nel tuo spazio dei nomi. In alternativa, escludi le risorse che si trovano nello spazio dei nomi AMS.

Risultato	Descrizione
L'istruzione contiene azioni di etichettatura di {*Service_Name* } che non sono limitate a valori specifici per la chiave Name tag. Prendi in considerazione la possibilità di definire l'ambito di queste azioni impostando la chiave di `aws:RequestTag/Name` condizion e con i valori nel tuo spazio dei nomi o di limitare queste azioni impostando la chiave di `aws:RequestTag/Name` condizione con l'`StringNotLike` operatore con i valori nei prefissi dello spazio dei nomi AMS.	Questo risultato viene generato se la politica concede l'autorizzazione di etichettatura per un determinato servizio e l'autorizzazione non è limitata a chiavi/valori di tag specifici. Per definire quale chiave o valore può essere utilizzato nelle azioni dei tag, ad esempio, quando si richiede di eseguire le azioni, utilizza la condizione. `aws:RequestTag/tag key` Quindi, per risolvere questo problema, usa questa chiave condizionale per limitare la chiave o i valori nello spazio dei nomi. Oppure, nega il `Name` tag key (`aws:RequestTag/Nam e`) con valori nello spazio dei nomi AMS.
Errore interno durante la convalida della policy di fiducia dei ruoli IAM.	Questo risultato viene generato quando CT automation rileva un errore durante la convalida della policy di trust dei ruoli IAM tramite il servizio IAM Access Analyzer. Per risolvere il problema, invia nuovamente la RFC. Se l'errore persiste, contatta AMS Operations per risolvere l'errore.
Errore interno durante la convalida della politica gestita dal cliente.	Questo risultato viene generato quando CT Automation rileva un errore durante la convalida della policy gestita dal cliente tramite il servizio IAM Access Analyzer. Per risolvere il problema, invia nuovamente la RFC. Se l'errore persiste, contatta AMS Operations per risolvere l'errore.
Analizzatore di accesso non trovato in. *Regione AWS* Impossibile eseguire il controllo di anteprima dell'accesso per la politica di attendibilità dei ruoli.	Questo risultato viene generato quando la risorsa IAM Access Analyzer non viene trovata in. Regione AWS Contatta AMS Operations per risolvere i problemi e creare una risorsa IAM Access Analyzer nella regione AWS.

Risultato	Descrizione
Policy di fiducia non valida per il ruolo *Role_Name*	Questo risultato viene generato quando il ruolo IAM fornito contiene una policy di fiducia non valida. Per risolvere, rivedi la politica di fiducia per verificare che sia valida.
IAM Access Analyzer ha riscontrato un errore interno. Impossibile creare l'anteprima di accesso per il ruolo *Role_Name*	Questo risultato viene generato quando l'automazione riscontra un errore durante la creazione di un'anteprima di accesso per un ruolo tramite IAM Access Analyzer. Per risolvere il problema, invia nuovamente la RFC. Se l'errore persiste, contatta AMS Operations per risolvere l'errore.
Impossibile creare l'anteprima di accesso per la politica di attendibilità del ruolo *Role_Name*	Questo risultato viene generato quando l'automazione rileva un errore durante la creazione di un'anteprima di accesso per un ruolo tramite IAM Access Analyzer. Per risolvere il problema, invia nuovamente la RFC. Se l'errore persiste, contatta AMS Operations per risolvere l'errore.
Errore interno durante la convalida dell'IdP SAML elencato.	Questo risultato viene generato quando l'automazione riscontra un errore durante la convalida del SAML IdPs fornito elencato nella policy di attendibilità dei ruoli. Per risolvere il problema, invia nuovamente la RFC. Se l'errore persiste, contatta AMS Operations per risolvere l'errore.
Errore interno relativo alla convalida delle autorizzazioni. AWS Key Management Service	Questo risultato viene generato quando l'automazione riscontra un errore durante la convalida delle autorizzazioni AWS KMS chiave nella politica fornita. Per risolvere il problema, invia nuovamente la RFC. Se l'errore persiste, contatta AMS Operations per risolvere l'errore.

Risultato	Descrizione
Errore interno durante la convalida della politica gestita elencata. ARNs	Questo risultato viene generato quando l'automazione riscontra un errore durante la convalida della policy gestita elencata. ARNs Per risolvere il problema, invia nuovament e la RFC. Se l'errore persiste, contatta AMS Operations per risolvere l'errore.
Errore interno durante la convalida dell'allegato predefinito. `customer_deny_policy`	Questo risultato viene generato quando l'automazione riscontra un errore durante la convalida dell'associazione al `customer_ deny_policy` ruolo. Per risolvere il problema, invia nuovamente la RFC. Se l'errore persiste, contatta AMS Operations per risolvere l'errore.
Errore interno durante la convalida delle policy gestite relative al ruolo *`Role_Name`*	Questo risultato viene generato quando l'automazione rileva un errore durante la convalida della politica gestita per il ruolo. ARNs Per risolvere il problema, invia nuovamente la RFC. Se l'errore persiste, contatta AMS Operations per risolvere l'errore.
Errore interno durante la convalida *`Policy_na me`* rispetto alla politica dei limiti definita dal cliente `AWSManagedServicesIAMProvis ionCustomerBoundaryPolicy`	Questo risultato viene generato quando l'automazione rileva un errore durante la convalida della policy che contiene l'elenco di rifiuto personalizzato. Per risolvere il problema, invia nuovamente la RFC. Se l'errore persiste, contatta AMS Operations per risolvere l'errore.

Risultato	Descrizione
Nell'account esiste una politica dei limiti definita dal cliente. `AWSManagedServices IAMProvisionCustomerBoundaryPolicy` Tuttavia, la politica contiene istruzioni di autorizzazione che concedono autorizzazioni. La policy deve contenere solo dichiarazioni di rifiuto.	Questo risultato viene generato quando la politica che contiene l'elenco di rifiuto personalizzato include una dichiarazione che concede l'autorizzazione. Sebbene la lista di rifiuto personalizzata esista all'interno del tuo account come policy gestita da IAM, non può essere utilizzata per la gestione delle autorizzazioni. La policy deve contenere solo dichiarazioni di rifiuto che indicano che desideri che AMS Automated IAM Provisioning convalidi e neghi le azioni nelle policy IAM create da AMS Automated IAM Provisioning.
L'informativa contiene azioni privilegiate definite dall'organizzazione per. *`Service_Name`* Valuta la possibilità di escludere queste azioni con una dichiarazione di rifiuto. Fai riferimento alla politica indicata nel tuo account per fare riferimento all'elenco di azioni riservate.	Questo risultato viene generato quando l'automazione rileva qualsiasi azione nella politica definita nell'elenco di rifiuto personalizzato. Per risolvere il problema, rivedi l'informativa sulla politica e rimuovi tutte le azioni definite nell'elenco di rifiuto personalizzato o aggiungi una dichiarazione di rifiuto che neghi tali azioni.
Il ruolo deve essere allegato. *`POLICY_ARN`* Includi l'ARN della policy nell'elenco delle policy gestite. ARNs	Questo risultato viene generato se il ruolo che stai creando non è *`POLICY_ARN`* associato . Per risolvere il problema, includi il ruolo ManagedPolicyArnsnel campo del ruolo e riprova. *`POLICY_ARN`*
Non *`POLICY_ARN`* può essere distaccato dal ruolo. Includi l'ARN della policy nell'elenco delle policy gestite. ARNs	Questo risultato viene generato se *`POLICY_ARN`* viene rimosso dal ruolo durante un aggiornamento. Per risolvere il problema, aggiungi il *`POLICY_ARN`* al ManagedPolicyArnscampo del ruolo e riprova.

Controllo dei limiti di autorizzazione AMS Automated IAM Provisioning

I controlli dei limiti di autorizzazione AMS ti aiutano a rispettare la politica dei limiti di autorizzazione predefinita fornita da AMS. Questa policy è un elenco di azioni negate da AMS Automated IAM Provisioning. Le politiche di provisioning che contengono queste azioni limitate richiedono un'ulteriore accettazione esplicita del rischio. Scarica la policy qui: boundary-policy.zip.

Utilizza i controlli della politica dei limiti di autorizzazione definiti dal cliente per personalizzare le azioni di negazione oltre i valori predefiniti della politica dei limiti di autorizzazione AMS. Quando effettui l'onboarding ad AMS Automated IAM Provisioning utilizzando il seguente tipo di modifica: Gestione | Account gestito | AMS Automated IAM Provisioning con autorizzazioni di lettura/scrittura | Abilita (revisione richiesta) (ct-1706xvvk6j9hf), puoi includere un elenco di azioni di rifiuto personalizzate che specificano azioni limitate aggiuntive.

Puoi aggiornare l'elenco delle azioni di negazione utilizzando il tipo di modifica: Gestione | Account gestito | Provisioning IAM automatizzato con autorizzazioni di lettura/scrittura | Aggiorna elenco di negazioni personalizzato (ct-2r9xvd3sdsic0). È necessario utilizzare il ruolo IAM dedicato per eseguire questo tipo di modifica. `AWSManagedServicesIAMProvisionAdminRole`

> **Note**
>
> - È necessario fornire un elenco completo di azioni di negazione per ogni aggiornamento. L'elenco precedente viene sostituito dal nuovo elenco.
> - L'elenco delle azioni di rifiuto deve contenere solo le azioni da negare. Le azioni di autorizzazione non sono supportate.
> - L'elenco delle azioni di negazione si trova all'interno dell'account sotto forma di policy gestita da IAM. `AWSManagedServicesIAMProvisionCustomerBoundaryPolicy` La policy non deve essere associata a nessun ruolo.
> - Il termine limite di autorizzazione utilizzato per indicare le azioni negate in AMS Automated IAM Provisioning ha un significato contestuale diverso rispetto al limite di autorizzazione IAM. Il limite di autorizzazione IAM imposta l'autorizzazione massima che una policy può concedere in fase di esecuzione a un'entità IAM. Per ulteriori informazioni sui limiti delle autorizzazioni IAM, consulta Tipi di policy nella Guida per l'AWS Identity and Access Management utente. Il limite di autorizzazione in AMS Automated IAM Provisioning impedisce di fornire una policy IAM che contenga un determinato set di autorizzazioni, ad esempio un elenco di azioni negate.

Risoluzione dei problemi relativi ai risultati e agli errori di AMS Automated IAM Provisioning

Esistono tre modi in cui potresti riscontrare problemi quando utilizzi AMS Automated IAM Provisioning:

- Errori RFC: possono verificarsi per una serie di motivi, ad esempio un inserimento errato. Per ulteriori informazioni, consulta Risoluzione degli errori RFC in AMS.
- Errori SSM: possono verificarsi per diversi motivi, ad esempio una formattazione scadente. Per ulteriori informazioni, vedere Troubleshooting Systems Manager Automation.
- Risultati del controllo di convalida: si verificano quando uno dei numerosi controlli di convalida eseguiti da Automated IAM Provisioning rileva un problema. Per un elenco dei controlli di convalida e delle azioni consigliate da correggere, consulta. Controlli di runtime per AMS Automated IAM Provisioning in AMS

Impostazione delle autorizzazioni in AMS con ruoli e profili IAM

AMS utilizza AWS Identity and Access Management (IAM) per gestire gli utenti, le credenziali di sicurezza come le chiavi di accesso e le autorizzazioni che controllano le AWS risorse a cui possono accedere utenti e applicazioni. AMS fornisce un ruolo utente IAM predefinito e un profilo di EC2 istanza Amazon predefinito (che include un'istruzione che consente l'accesso delle risorse al ruolo utente IAM predefinito).

Richiesta di un nuovo ruolo utente o profilo di istanza IAM

AMS utilizza un ruolo IAM per impostare le autorizzazioni degli utenti tramite il servizio federativo e un profilo di istanza IAM come contenitore per quel ruolo IAM.

Puoi richiedere un ruolo IAM personalizzato con Deployment | Advanced stack components | Identity and Access Management (IAM) | Create Entity o Policy (revisione obbligatoria), tipo di modifica (ct-3dpd8mdd9jn1r) o un profilo di istanza IAM con Management | Applications | Profilo istanza IAM | Create Management | Applications | IAM instance profile | Create (revisione richiesta) change type (ct-0ixp4ch2ti2c (04). Vedi le descrizioni di ciascuno di essi in questa sezione.

> **Note**
>
> AMS ha una politica IAM `customer_deny_policy` che blocca i namespace e le azioni pericolosi. Questa politica è associata a tutti i ruoli dei clienti AMS per impostazione

predefinita e raramente rappresenta un problema per gli utenti. Le tue richieste di utenti e ruoli IAM non includono questa policy, ma l'inclusione automatica di essa `customer_deny_policy` nelle richieste per i ruoli IAM aiuta AMS a implementare nuovi profili di istanze IAM più rapidamente. Puoi richiedere l'esclusione della `customer_deny_policy` policy. Tuttavia, questa richiesta sarà sottoposta a un'approfondita revisione di sicurezza ed è probabile che venga rifiutata per motivi di sicurezza.

Limita le autorizzazioni con le dichiarazioni sulle policy dei ruoli IAM

AMS utilizza un ruolo IAM per impostare le autorizzazioni degli utenti tramite il servizio di federazione.

Landing Zone AMS per account singolo: vedi SALZ: Ruoli utente IAM predefiniti.

Multi-Account Landing Zone AMS: vedi MALZ: Ruoli utente IAM predefiniti.

Un ruolo IAM è un'entità IAM che definisce un insieme di autorizzazioni per effettuare AWS richieste di servizio. I ruoli IAM non sono associati a un utente o gruppo specifico. Invece, le entità attendibili assumono ruoli, come utenti IAM, applicazioni o AWS servizi come Amazon EC2. Per ulteriori informazioni, consulta IAM Roles (Ruoli IAM).

Puoi definire la policy desiderata per un utente che assume il ruolo utente AMS IAM utilizzando l'operazione API AWS Security Token Service (STS) AssumeRoleinserendo una policy IAM più restrittiva nel campo di `Policy` richiesta.

Di seguito vengono fornite istruzioni politiche di esempio che è possibile utilizzare per limitare l'accesso CT.

Utilizzando i gruppi Active Directory (AD) configurati e l'operazione API AWS Security Token Service (STS) AssumeRole, puoi impostare le autorizzazioni per determinati utenti o gruppi, inclusa la limitazione dell'accesso a determinati tipi di modifiche ()CTs. Puoi utilizzare le dichiarazioni politiche mostrate di seguito per limitare l'accesso CT in vari modi.

Dichiarazione AMS change type nel profilo di istanza IAM predefinito che consente l'accesso a tutte le chiamate API AMS (amscm e amsskms) e a tutti i tipi di modifica:

```
{
    "Sid": "AWSManagedServicesFullAccess",
    "Effect": "Allow",
    "Action": [
```

```
        "amscm:*",
        "amsskms:*"
    ],
    "Resource": [
        "*"
    ]
}
```

1. Dichiarazione per consentire l'accesso e tutte le azioni solo per due operazioni specificate CTs, dove «Azione» indica le operazioni dell'API AMS (una `amscm` o l'altra`amsskms`) e «Resource» rappresenta il tipo di modifica e il numero di versione esistenti: IDs

   JSON

   ```
   {
       "Version":"2012-10-17",
       "Statement": [
           {
               "Effect": "Allow",
               "Action": "amscm:*",
               "Resource": [
                   "arn:aws:amscm:*:*:changetype/ct-ID1:1.0",
                   "arn:aws:amscm:*:*:changetype/ct-ID2:1.0"
               ]
           }
       ]
   }
   ```

2. Dichiarazione per CreateRfc consentire l'accesso a e solo SubmitRfc su due specificate CTs: UpdateRfc
3. Dichiarazione per CreateRfc consentire l'accesso a e SubmitRfc su tutti i dispositivi disponibili CTs: UpdateRfc
4. Dichiarazione per negare l'accesso a tutte le azioni relative alla TAC con restrizioni e consentire ad altre CTs:

Limita le autorizzazioni con i profili di istanza Amazon EC2 IAM

Un profilo di istanza IAM è un contenitore per un ruolo IAM che puoi utilizzare per passare informazioni sul ruolo a un' EC2 istanza Amazon all'avvio dell'istanza.

Attualmente esiste un profilo di istanza predefinito di AWS Managed Services (AMS) che concede le autorizzazioni alle applicazioni in esecuzione sull'istanza, non agli utenti che accedono all'istanza. `customer-mc-ec2-instance-profile` Potresti voler modificare il profilo predefinito dell'istanza o crearne uno nuovo, se desideri consentire a un'istanza di accedere a qualcosa, senza concedere l'accesso anche ad altre istanze. Puoi richiedere un nuovo profilo di istanza IAM con Management | Applications | IAM instance profile | Create change type (ct-0ixp4ch2tiu04). Quando invii la RFC, puoi creare il tuo profilo di istanza e includerlo come InstanceProfileDescription, oppure puoi semplicemente informare AMS (utilizzando lo stesso campo) delle modifiche che desideri. Poiché si tratta di un CT manuale, AMS deve approvare la modifica e si metterà in contatto con l'utente in merito.

Se non conosci le politiche di Amazon IAM, consulta Panoramica delle politiche IAM per informazioni importanti. C'è anche un buon post sul blog, Demystifying EC2 Amazon Resource-Level Permissions. Tieni presente che attualmente AMS non supporta il controllo degli accessi basato sulle risorse, ma supporta i controlli a livello di risorsa utilizzando le policy dei ruoli IAM (per una spiegazione della differenza, consulta Servizi che funzionano con IAM).AWS

Landing Zone AMS per account singolo:

Per visualizzare una tabella delle autorizzazioni concesse dal profilo di istanza AMS IAM predefinito, vai a EC2 IAM Instance Profile.

Regola di attestazione AD FS e impostazioni SAML

ActiveDirectory Regola di reclamo Federation Services (AD FS) e impostazioni SAML per AWS Managed Services (AMS)

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 rivendicazione 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 degli 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 seguenti riguardano i 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

Limita con ACL di rete

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, in AMS Managed Multi-Account Landing Zone, 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 Multi-Account Landing Zone Core, ossia Account di gestione, Networking, Shared-Services, Logging e Security.
- NACLs sono supportati negli account Multi-Account Landing Zone Application, a condizione che vengano utilizzati solo come elenco «Deny» e abbiano la funzione «Allow All» per consentire le operazioni di monitoraggio e gestione di AMS.

In ambienti multi-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 in AMS Multi-Account Landing Zone per separare il traffico di rete. VPCs

AMS su Outposts

AWS Outpostsè una soluzione hardware gestita che estende le zone di atterraggio gestite da AMS ai data center dei clienti. Con il supporto AMS attivo AWS Outposts, i clienti che cercano l'esperienza nel cloud, il risparmio sui costi e la piattaforma standardizzata offerta da AMS non si limitano più a ospitare risorse interne Regioni AWS. Con AMS attivo AWS Outposts, i clienti con esigenze locali possono ora modernizzarsi e usufruire al contempo dei AWS servizi di patching, backup, provisioning, gestione degli incidenti, continuità operativa e ottimizzazione dei costi offerti da AMS.

Una volta attivato un AWS Outposts account AMS Multi-Account Landing Zone o Single-Account Landing Zone, puoi seguire i processi di gestione delle modifiche AMS esistenti per fornire e gestire le risorse. AWS L'infrastruttura ospitata da AMS può essere gestita specificando una sottorete specifica. AWS Outposts AWS Outposts i cicli di vita possono essere gestiti direttamente nella console utilizzando il ruolo dei servizi di self-provisioning. AWS Outposts AWS Outposts

Per informazioni sul ruolo, vedere. AWS Outposts

AWS Outposts installazione e gestione operativa

Il AWS Outposts processo di onboarding verso AMS comprende:

1. Pianificazione Outposts
2. Convalida dell'ordine
3. Outposts Onboarding verso AMS
4. Gestione del ciclo di vita

AWS Outposts pianificazione

Durante la AWS Outposts pianificazione, identificate AMS in base ai casi AWS Outposts d'uso e coinvolgete le principali parti interessate, tra cui il team addetto all'account e AWS Outposts i rappresentanti di AMS, per allineare la strategia di capacità.

1. Una volta identificati i casi d'uso che richiedono AMS on, AWS Outposts contattate il vostro account team AMS per discutere della pianificazione della capacità.

2. Una volta determinati i requisiti di AWS Outposts capacità, l'account team di AMS coinvolge il team di AWS Outposts assistenza per discutere del piano di AWS Outposts onboarding, dei ruoli e delle responsabilità. Durante questo periodo vi viene AWS Outposts assegnato un unico punto di contatto (SPOC). Lo AWS Outposts SPOC aiuta a AWS Outposts finalizzare i requisiti di dimensionamento.

AWS Outposts convalida dell'ordine

Durante la convalida dell'ordine, crei un AWS Outposts sito e ordini la capacità richiesta direttamente nella AWS Outposts console o tramite il rappresentante del tuo AWS Outposts account.

Una volta che il team dell'account AMS avrà allineato il AWS Outposts team, potrai richiedere il ruolo di servizio che ti AWS Outposts viene assegnato autonomamente utilizzando l'ID di modifica ct-3qe6io8t6jtny, per creare il tuo sito e ordinare direttamente nella console. AWS Outposts AWS Outposts

In alternativa, puoi utilizzare lo SPOC per creare siti e ordini Outpost. AWS Outposts Il tuo AWS Outposts SPOC continuerà a fornire aggiornamenti sullo stato a te e al team dell'account AMS durante la convalida del sito e dell'ordine e l'installazione. AWS Outposts

AWS Outposts onboarding su AMS

Una volta attivata AWS Outposts l'unità nel tuo VPC gestito da AMS, puoi richiedere la creazione di monitor per tenere traccia della disponibilità, della capacità, delle eccezioni e della connettività di rete per il tuo hardware Outposts. Seguendo le fasi di implementazione del monitoraggio descritte di seguito, l' AWS Outposts hardware viene monitorato attivamente da AMS.

1. Una volta installato e attivato, AWS Outposts è possibile richiedere un monitoraggio AWS Outposts specifico inviando il seguente modello con una RFC utilizzando il tipo di modifica Management | Other | Other | Create (ct-1e1xtak34nx76). Le operazioni AMS assicurano che la sottorete sia tracciata negli strumenti interni di AMS. AWS Outposts
   - AWS Outposts ID
   - CIDR sottorete
   - AWS Outposts Allarmi consigliati:
     - InstanceFamilyCapacityAvailabilityAlert
     - InstanceTypeCapacityAvailabilityAlert
     - EBSVolumeTypeCapacityAvailabilityAlert

- CapacityExceptionsAlert
- Connect diretto ConnectionAlert

- Per ciascuno degli avvisi precedenti, specificare i seguenti parametri:
  - La statistica («Media») è consigliata. Altre opzioni includono somma, valore massimo, minimo, numero di campioni e p90)
  - Periodo («5 minuti») è consigliato. Le altre opzioni includono 10 e 30 secondi, 1, 5 e 15 minuti, 1 e 6 ore e 1 giorno)
  - Il tipo di soglia («Statico») è consigliato. Anche le «Anomalie» sono opzioni.)
  - Condizione (sono disponibili anche le opzioni «Ogni volta che il numero di chiamate è maggiore di», «uguale a», «minore di»).
  - Il valore della condizione (» 25% ") è configurato per impostazione predefinita. È consentito un altro numero intero positivo.)
  - Argomento di notifica (gli argomenti relativi alle operazioni AMS vengono assegnati automaticamente. Tuttavia, è possibile aggiungere anche qualsiasi altro argomento o argomento personalizzato.)

2. Supporto al monitoraggio e alle operazioni
   - Le operazioni AMS monitorano le AWS Outposts metriche relative alla disconnessione della rete o ai guasti dei componenti. AMS Operations fornisce servizi di prima risposta in caso di AWS Outposts problemi e, se necessario, passa al supporto o al supporto Premium. EC2
   - Le operazioni AMS sono disponibili per risolvere i problemi relativi all'unità. AWS Outposts
3. Quando i controlli dello stato dell' EC2 istanza o dello stato del sistema falliscono, le operazioni AMS seguono i processi esistenti per riportare l'istanza online. Se il riavvio fallisce o la AWS Outposts capacità è insufficiente, un membro del team operativo AMS ti avvisa direttamente per determinare i passaggi successivi.

AWS Outposts gestione del ciclo di vita

Una AWS Outposts volta effettuato l'accesso al tuo account AMS, riceverai una notifica in caso di eccezioni di disponibilità, capacità o rete. È possibile disattivare AWS Outposts direttamente la AWS Outposts console o lo SPOC. AWS Outposts

È possibile eseguire la gestione AWS Outposts direttamente nella AWS Outposts console utilizzando il ruolo del servizio di provisioning AWS Outposts self-service o la modalità sviluppatore. Puoi anche richiedere AWS Outposts tramite il tuo CSDM o il punto di contatto AWS Outposts unico (SPOC).

AWS Outposts È possibile ottenere un'elevata disponibilità su installandone due o più. AWS Outposts La configurazione di due o più AWS Outposts abilita l'opzione della zona a disponibilità multipla per le istanze di Amazon Relational Database Service.

Fornitura di risorse gestite da AMS su AWS Outposts

AWS Le risorse di provisioning ospitate su AWS Outposts (ad esempio Amazon, Amazon EMR EC2, Amazon EKS, Amazon ECS, Amazon EBS e Amazon S3) negli account AMS (account Single-Account Landing Zone, Multi-Account Landing Zone e Accelerate) sono soggetti agli stessi livelli di supporto AMS delle risorse in. Regioni AWS Puoi utilizzare la gestione delle modifiche AMS, i servizi di provisioning self-service o la modalità sviluppatore per creare e modificare le risorse create su. AWS Outposts

Attualmente sono disponibili tutti i tipi di istanze (M5/M5d, C5/C5d, R5/R5d, i3en, G4dn), Amazon Elastic Block Store, Amazon Elastic Container Service, Amazon Elastic Kubernetes Service, Amazon EMR, Amazon Relational Database Service, Application Load Balancers e il proxy App Mesh Envoy sono disponibili direttamente su. DBs AWS Outposts Queste risorse sono idonee per lo stesso supporto operativo AMS delle risorse nelle regioni esistenti.

Limitazioni di AMS su AWS Outposts

- Il supporto operativo per le risorse AWS Outposts ospitate dipende dalla connettività di rete coerente. AWS Outposts la disconnessione della rete impedisce alle operazioni AMS di risolvere eventuali incidenti o problemi che si verificano sull'unità disconnessa. AWS Outposts Per informazioni su AMS in caso AWS Outposts di emergenza a livello di servizio, consulta i Service Level Agreement aggiornati ().AWS SLAs
- Servizio Amazon Relational Database:
  - Il tipo di modifica RDS di creazione (ct-2z60dyvto9g6c), per impostazione predefinita, abilita Multi-AZ e richiede un gruppo di sottoreti DB. I gruppi di sottoreti DB richiedono due sottoreti in due zone di disponibilità (AZ) separate. Se ne hai solo uno AWS Outposts, la creazione di un gruppo di sottoreti DB è un problema poiché AWS Outposts vengono assegnati solo a una singola AZ. Per aggirare questa limitazione, segui queste istruzioni:
    1. Richiedi un gruppo di sottoreti DB tramite una RFC con un CT Management | Other | Other e specifica la sottorete su. AWS Outposts
    2. Crea un modello CFN personalizzato su cui distribuire RDS e specifica il gruppo di sottoreti creato nel passaggio precedente. AWS OutpostsPer ulteriori informazioni su questa operazione, consulta Risorse personalizzate.

3. Richiedi che AMS distribuisca il modello CFN contenente l'istanza RDS di destinazione tramite AMS CFN ingest CT (ct-36cn2avfrrj9v).
4. Tieni presente che attualmente, RDS for non fornisce metriche e log a causa di una limitazione del servizio RDS. AWS Outposts

- Workload ingest (WIGs): Linux funziona WIGs solo se l'WIGs EC2 istanza preliminare si trova su una sottorete.AWS Outposts Il motivo è che Linux WIGs crea un WIGs nodo nella sottorete della prima EC2 istanza utilizzando m4.large, per impostazione predefinita. Poiché AWS Outposts non ha quel tipo di istanza, non WIGs è in grado di avviare il suo nodo di lavoro. La soluzione alternativa consiste nel creare l' EC2 istanza iniziale in una non AWS Outposts sottorete, quindi è possibile creare l'istanza di destinazione su. AWS Outposts Inoltre, attualmente sono supportati solo i tipi di EC2 istanze basati su Nitro, tra cui C5, C5d, M5d, R5, R5d, G4 e I3en. AWS Outposts
- Amazon Elastic Block Store (EBS): Create EBS Volume CT (ct-16xg8qguovg2w) non funziona, poiché i volumi vengono creati al posto di AWS Outposts non fornire l'Amazon Resource Number (ARN) AWS come parametro di input per il CT. AWS Outposts
- Connettività di rete AWS Outposts : la connettività di rete è una tua responsabilità nei confronti del team.
- Brownfield e acquisizione dell'account: l' AWS Outposts attivazione su account non AMS non può essere trasferita ad AMS, a causa della natura della AWS Outposts fatturazione e dei requisiti di supporto aziendale.

AMS sulla conformità AWS Outposts

AMS sull'attestazione di AWS Outposts conformità

AWS Outposts il piano di controllo è stato certificato idoneo all'HIPAA, conforme agli standard PCI e ISO. Tuttavia, l'AMS sul piano AWS Outposts di controllo non è stato attestato. AWS Outposts Per questo motivo, i clienti sono incoraggiati a richiedere l'attestazione di conformità AMS sull' AWS Outposts ambiente.

Per controllare la creazione di risorse sull'unità Outpost, i clienti sono incoraggiati a separare l'accesso degli sviluppatori all'Outpost, per evitare un accesso eccessivo degli sviluppatori negli account gestiti AMS standard.

Carichi di lavoro gestiti da AMS che richiedono la conformità FedRAMP

Innanzitutto, gli account di gestione AMS devono prima essere valutati per verificarne la conformità alle normative, poiché i dati del piano di controllo confluirebbero dagli account di gestione AMS. AWS Outposts

Se è richiesta la certificazione FedRAMP e la struttura degli account AMS è conforme, si consiglia di utilizzare un fornitore di data center che disponga già della certificazione richiesta e possieda tutta l'appliance service link (o che già crittografa i dati in uscita).

Infine, è possibile implementare una protezione aggiuntiva dei dati collaborando con il team dell'account per implementare un SCP che limiti i dati AWS Outposts e impedisca la creazione di risorse locali nell'account che ospita Outpost.

Impatto sulla conformità esistente per gli account AMS

AWS Outposts Non è necessario ripetere il test di conformità di un account che utilizza, purché non vengano utilizzati dati regolamentati e l'account sia separato logicamente. Gli account di gestione AMS possono gestire conti non regolamentati e conti regolamentati purché i flussi di dati tra account authentication/authorization e in ingresso/uscita siano separati. VPCs Pertanto, anche se l'account Outpost non conforme e gli account delle applicazioni conformi esistenti appartengono alla stessa organizzazione (inclusi servizi condivisi, networking, registrazione, master e servizi AMS di sicurezza), l'account dell'applicazione di conformità mantiene la conformità poiché i dati sono separati logicamente.

AMS attivo AWS Outposts FAQs

Per quali casi d'uso è possibile usufruire del supporto AMS? AWS Outposts

AMS on AWS Outposts può essere utilizzato dalle aziende che necessitano di un modello operativo cloud collaudato, con carichi di lavoro che richiedono bassa latenza (ad esempio, gestione dei robot di fabbrica e migrazione del mainframe), edge computing (ad esempio, workstation remote e semplificazione dei dati edge) e grandi carichi di trasferimento di dati.

Qual è il vantaggio di utilizzare questa funzionalità?

AMS fornisce il monitoraggio dell' AWS Outposts hardware e la prima risposta a qualsiasi problema hardware. AWS Outposts Inoltre, le seguenti funzionalità di supporto per tutte le risorse gestite ospitate su AWS Outposts:

- Registrazione, monitoraggio, guardrail e gestione degli eventi

- Gestione della continuità
- Gestione della sicurezza e degli accessi
- Gestione delle patch
- Gestione delle modifiche
- Gestione automatizzata e self-service del provisioning
- Gestione degli incidenti e dei problemi
- Segnalazione (la generazione di report per AWS Outposts l'hardware non sarà inizialmente supportata con AMS attivo AWS Outposts)
- Gestione delle richieste di assistenza
- Modalità sviluppatore
- Supporto aziendale

Come posso usare questa funzionalità?

AWS Outposts pianificazione: durante la AWS Outposts pianificazione, avete identificato i casi AWS Outposts d'uso di AMS e coinvolgerete le principali parti interessate, tra cui il team addetto all'account e AWS Outposts i rappresentanti di AMS, per allineare la strategia in materia di capacità.

Convalida dell'ordine: durante la convalida dell'ordine, crei un AWS Outposts sito e ordini la capacità richiesta direttamente nella AWS Outposts console o tramite il rappresentante del tuo AWS Outposts account.

AWS Outposts onboarding su AMS: una volta attivata AWS Outposts l'unità nel tuo VPC gestito da AMS, puoi richiedere l'onboarding sul tuo AWS Outposts account AMS inviando una richiesta di modifica (RFC) utilizzando il modello nella Guida per l'utente AMS (). AWS Outposts AMS operations crea quindi una sottorete e monitora Outpost utilizzando gli input forniti nella RFC.

Gestione del ciclo di vita: una volta effettuato AWS Outposts l'onboarding sul tuo account AMS, riceverai una notifica di eventuali eccezioni di disponibilità, capacità o rete. Puoi disattivare AWS Outposts direttamente la AWS Outposts console o il tuo AWS Outposts unico punto di contatto (SPOC).

Quali sono le limitazioni di AMS? AWS Outposts

I casi d'uso relativi alla residenza dei dati (ad esempio, leggi sulla localizzazione dei dati specifiche del paese, ecc.) non sono ancora stati convalidati per AMS on. AWS Outposts

AWS Outposts l'attivazione in account diversi da AMS non può essere trasferita ad AMS, a causa della natura della AWS Outposts fatturazione e dei requisiti di Enterprise Support.

AWS Outposts il piano di controllo è stato certificato idoneo agli standard HIPAA e conforme agli standard PCI e ISO. Tuttavia, l'AMS sul piano AWS Outposts di controllo non è stato attestato. AWS Outposts Per questo motivo, i clienti sono incoraggiati a richiedere l'attestazione di conformità AMS sull' AWS Outposts ambiente.

Posso disattivare questa funzionalità?

Il provisioning AWS Outposts nell'ambiente AMS è facoltativo. Una volta implementato nell'account AMS, AWS Outposts può essere eseguito il deprovisioning tramite la AWS Outposts console in qualsiasi momento, se non è più necessario.

Come verrà fatturato AMS on AWS Outposts ?

L'aumento delle AWS Outposts tariffe da parte di AMS verrà applicato a livello del Gruppo B.

In che modo verrà AWS Outposts adattato il Service Level Agreement di AMS?

La gestione degli incidenti dipenderà dalla disponibilità. AWS Outposts AWS Outposts la disponibilità è soggetta alla disponibilità della rete del cliente, che è responsabilità del cliente. AWS Outposts la disponibilità è inoltre soggetta all'operatività AWS Outposts dell'hardware, che dipende dai AWS Outposts Service Level Agreement.

Consulta anche AWS Outposts FAQs.

Utilizzo dei tag in AMS

Argomenti

Fornire tag può essere di grande utilità. Per informazioni approfondite, leggi Tagging Your Amazon EC2 Resources.

RFCs che creano istanze, come un bucket Amazon S3 o un Elastic Load AWS Balancer (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 un Management | Advanced stack

components | Amazon S3 storage | Update CT. Amazon EC2, Amazon EFS, Amazon 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

Quando si utilizza la console AMS, è necessario abilitare la visualizzazione 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 si sta creando. Alcuni schemi offrono un parametro per denominare la risorsa che si sta creando, altri no. Ad esempio, lo schema CT per lo EC2 stack Create Amazon non offre un parametro per denominare l' EC2 istanza Amazon. 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 Amazon viene visualizzata nella EC2 console Amazon senza un attributo name.

Esistono restrizioni relative ai tag? Sì:

- I tag rispettano la distinzione tra maiuscole e minuscole.
- La lunghezza massima della chiave è di 128 caratteri Unicode.
- La lunghezza massima del valore è di 256 caratteri Unicode.
- Il numero massimo di tag per risorsa è 50.
- Il prefisso riservato è `aws:`.
- I nomi e i valori dei tag generati da AWS vengono contrassegnati automaticamente con il prefisso `aws:`, che tu non puoi assegnare. I nomi dei tag definiti dall'utente hanno il prefisso `user:` nel report di allocazione dei costi.
- Utilizza ciascuna chiave una sola volta per ciascuna risorsa. Se si tenta di utilizzare la stessa chiave due volte sulla stessa risorsa, la richiesta viene rifiutata.
- I caratteri consentiti sono lettere Unicode, spazi bianchi, numeri e i seguenti caratteri speciali: + - =. _:/

Quali tipi di AWS risorse supportano i tag? Vedi Ora organizza AWS le tue risorse utilizzando fino a 50 tag per risorsa.

Etichettatura automatica dell'infrastruttura AMS

AMS può etichettare tutte le risorse create da AMS per scopi di gestione, negli account multi-account landing zone (MALZ) e single-account landing zone (SALZ) tramite una richiesta di modifica (RFC) con il tipo di modifica Deployment | Advanced stack components | Tag | Create (review required) change (ct-0176f0n99vcps). Questo può aiutarti a identificare le risorse create da AMS per scopi di gestione.

AMS è in grado di identificare automaticamente le risorse create da AMS in base agli standard di denominazione e verificare se la risorsa presenta le seguenti chiavi e valori di tag: "AppNameAppId«," AMSResource «e"». EnvironmentType Se la chiave del tag non esiste o il valore è vuoto, tali chiavi di tag possono essere create automaticamente da AMS con tag-value "». AMSInfrastructure

Puoi personalizzare i tag che desideri sulle risorse create da AMS in base agli standard di etichettatura della tua organizzazione. Puoi includere le tue chiavi e i tuoi valori di tag quando invii la richiesta ad AMS. Segui questi standard di denominazione dei AWS tag: Tagging Best Practices

> **Note**
>
> Per gli account MALZ, l'etichettatura personalizzata dell'infrastruttura AMS è supportata solo sugli account delle applicazioni. L'etichettatura personalizzata sugli account principali non è attualmente supportata.
> Se il nome della chiave del tag fornito nella RFC esiste già nella risorsa, il valore del tag viene sostituito con il nuovo valore del tag fornito nella RFC.
> La lunghezza totale delle coppie di tag chiave:valore non deve superare i 256 caratteri.

Includi le seguenti informazioni nella tua RFC con Deployment | Advanced stack components | Tag | Create (review required) change type (ct-0176f0n99vcps) per etichettare le risorse create da AMS.

1. Elenco di account di landing zone con più account o di landing zone con account singolo in cui desideri etichettare le risorse create da AMS per scopi di gestione.
2. Nome della chiave e valore del tag richiesti (se necessario). Per impostazione predefinita, AMS può etichettare con il nome della chiave del tag come "" e il valore del tag come EnvironmentType "». AMSInfrastructure Se hai bisogno di un nome chiave e di un valore per il tag personalizzati, segui gli standard di denominazione dei tag: Tagging Best Practices AWS

Queste risorse sono attualmente supportate dal tagging dell'infrastruttura AMS:

```
   API Gateway
   Amazon CloudFront
   Amazon DynamoDB
   Amazon EBS
   Amazon EC2
   Amazon OpenSearch Service
   Amazon Quantum Ledger Database (QLDB)
   Amazon Redshift
   Amazon RDS
   Amazon S3 (specific buckets only*)
   Amazon Simple Queue Service (SQS)
   Amazon Simple Notification Service (SNS)
   Amazon VPC AWS Certificate Manager AWS CloudFormation AWS CloudTrail AWS CodeBuild
AWS CodePipeline AWS Elastic Beanstalk AWS Lambda AWS Secrets Manager AWS Service
Catalog AWS Systems Manager AWS WAF Regional
   Elastic Load Balancing
```

* «arn:aws:s3: ::awsms-a*-patch-data-*», «arn:aws:s3: ::ams-a*-log-management-*», «arn:aws:s3: :cf-templates-*», «arn:aws:s3: ::mc-a*», «arn:aws:s3: ::ams-a** -backup-reports-*», «arn:aws:s3: ::ams-a*- -*», «arn:aws:s3: ::ams-a*- -*», «arn:aws:s3: ::ams-a*- -*», «arn:aws:s3: ::ams-a*-release-assets-*», «arn:aws:s3: :ams-a*-release-assets-*», «arn:aws:s3: :ams-a*-release-assets-*», «arn:aws:s3: :ams-a*-release-assets-*», «arn:aws:s3: :ams-a*-release-assets-*», «arn:aws:s3: :s3::: -*», «arn:aws:s3::: *» patch-data-customer-reports patch-data-raw patch-data-reporting ams-cfn-drift-remediation ams-reporting-data-a

Tag consigliati da AMS

AMS consiglia i seguenti tag sulle risorse supportate. I tag con asterisco (*) sono altamente consigliati.

> **Note**
>
> È possibile utilizzare i tag per pianificare l'applicazione delle patch. Per informazioni, consulta AMS Advanced Patch Orchestrator: un modello di patching basato su tag.

Prefissi riservati AMS

Gli attributi delle risorse AMS devono rispettare determinati modelli; ad esempio, i nomi dei profili, i nomi, BackupVault i nomi dei tag delle istanze IAM non devono iniziare con i prefissi riservati AMS. Questi prefissi riservati sono:

```
*/aws_reserved/*
ams-*
/ams/*
ams*
AMS*
Ams*
aws*
AWS*
AWS_*
AWSManagedServices*
codedeploy_service_role
CloudTrail*
Cloudtrail*
customer-mc-*
eps
EPSDB*
IAMPolicy*
INGEST*
LandingZone*
Managed_Services*
managementhost
mc*
MC*
Mc*
MMS*
ms-
NewAMS*
Root*
sentinel*
Sentinel*
sentinel.int.
StackSet-ams*
StackSet-AWS-Landing-Zone
StateMachine*
TemplateId*
VPC_*
UnhealthyInServiceBastion
```

Tag consigliati da AMS

Chiave tag	Valori supportati	Note
`AppName*`	Senza vincoli.	Identifica le applicazioni che risiederanno sulla risorsa o che richiederanno l'accesso alla stessa. Ciò facilita il tracciamento e le comunicazioni tra AMS e l'utente.
`AppId*`		
`EnvironmentType *`		Distinguete tra infrastruttura di sviluppo, test e produzione come ambiente per la risorsa.
`OwnerTeamEmail *`	Indirizzo e-mail della lista di distribuzione	Identifica l'indirizzo e-mail della lista di distribuzione per il team responsabile della risorsa. L'e-mail non deve essere un'e-mail personale; deve essere un'e-mail anonima come una lista di distribuzione.
`ComplianceFramework`	Non vincolato	Identifica quali controlli e politiche devono essere applicati alla risorsa.
`CostCenter`		Identifica il centro di costo o l'unità aziendale associata a una risorsa (in genere per l'allocazione e il monitoraggio dei costi).
`Customer`		Utilizzato dai clienti AMS che dispongono di risorse provenienti da più clienti (sottoclienti AMS). Per raggruppare le risorse nell'ambiente gestito in base allo specifico cliente che servono. Identifica un cliente specifico su un particolare gruppo di risorse o servizi.

Chiave tag	Valori supportati	Note
`DataClassification`		Identifica lo specifico livello di riservatezza dei dati supportato da una risorsa. Identifica quali controlli e politiche devono essere applicati alla risorsa.
`HoursOfOperation`		Identifica la data o l'ora in cui una risorsa deve essere avviata, interrotta, eliminata o ruotata.
`OwnerTeam`		Identifica il team responsabile della risorsa. Facilita la comunicazione con il team responsabile della risorsa.
`Patch Group`	Sono disponibili due opzioni: • Puoi inviare una richiesta di servizio con le informazioni descritte in AMS Advanced Patch Orchestrator: un modello di patching basato su tag, e AMS crea un tag per te sulle risorse specificate e, utilizzando le informazioni fornite, un tag per te. `Patch Group` • Se avete già creato un `Patch Group` tag sulle vostre risorse, i valori supportati non sono vincolati.	Quali risorse includere in una finestra di manutenzione automatica delle patch.

Chiave tag	Valori supportati	Note
`ProjectId`	Non vincolato	Identifica i progetti supportati dalla risorsa.
`SupportPriority`	Uno dei sei possibili acronimi per Riservatezza, Integrità o Disponibilità; l'ordine dell'acronimo indica la priorità. Ad esempio, I.C.A. significherebbe che l'ordine è Integrità, Riservatezza, Disponibilità. Altri valori accettabili sono C.I.A., C.A.I., I.A.C., A.C.I. e A.I.C.	Identifica quale tipo di supporto deve essere prioritario: riservatezza, integrità o disponibilità.

Aggiungi tag alle note di aggiornamento collettivo

Queste note possono essere utilizzate con le procedure dettagliate di esempio relative al tipo di modifica Tag | Bulk Update e Tag | Bulk Update (Review Required).

Note sull'aggiornamento collettivo dei tag:

- Servizi supportati:
  - Per Tag | Aggiornamento in blocco (revisione richiesta): Tutti.
  - Per Tag | Aggiornamento in blocco:
    - Auto Scaling
    - Amazon EC2
    - Elastic Load Balancing
    - Amazon RDS
    - Bucket Amazon S3

- Per generare il file con valori separati da virgole (CSV), accedi a Resource Groups > Tag Editor nella AWS console, trova le risorse che desideri taggare ed esportale in un file CSV. Per ulteriori informazioni, consulta Esportazione dei risultati in formato CSV.

  NOTA: ti consigliamo di utilizzare un URL S3 prefirmato per fornire la posizione dell'oggetto CSV.
- Devono esserci colonne con le intestazioni Service, Type e Identifier. Queste colonne sono obbligatorie.
- Rinomina l'identificatore della colonna in ID.
- I valori per le colonne Service, Type e Identifier (modificati in ID) sono quelli forniti dal Tag Editor in Resource Groups.
- Se una risorsa da etichettare non è disponibile nel Tag Editor, utilizza l'Amazon Resource Name (ARN) della risorsa per l'identificatore di colonna (modificato in ID) e lascia vuoti Service e Type.
- Le intestazioni delle colonne dei tag da aggiungere o modificare devono avere il formato Tag:. ***`TagKey`***
- Le intestazioni di colonna dei tag da eliminare devono avere il formato Untag:. *`TagKey`*
- Ogni riga serve per etichettare o rimuovere i tag di una risorsa.
- Se dovete aggiungere un tag a una risorsa, specificate il valore del tag nella colonna Tag: ***`TagKey`*** appropriata.
- Se un tag deve essere eliminato da una risorsa, specificate True nella *`TagKey`* colonna Untag: appropriata.
- Se un Tag: ***`TagKey`*** o Untag: non *`TagKey`* è applicabile a una risorsa, aggiungete un trattino (-) alla rispettiva colonna o lasciatelo vuoto.

  NOTA: Untag sostituisce il Tag, perché, a differenza di Tag, Untag deve essere aggiunto manualmente al file CSV, quindi supponiamo che l'intenzione fosse quella di rimuovere, non modificare, il tag.
- Tutte le colonne aggiuntive che non soddisfano i criteri vengono ignorate.

> **Important**
>
> L'esportazione di Tag Editor compila una matrice di tutti i tag rispetto a tutte le risorse, i tag mancanti vengono compilati con il valore «non taggato». Il riutilizzo di questo file CSV di esportazione come input per la RFC comporta la creazione di tutti i tag precedentemente mancanti, con il valore letterale «non taggato».

> **Note**
>
> Per informazioni sull'esportazione dei tag in un file CSV, consulta Trova risorse da etichettare -> Esporta risultati in CSV.

AWS Managed Services Resource Scheduler

Usa AWS Managed Services (AMS) Resource Scheduler per pianificare l'avvio e l'arresto automatici di AutoScaling gruppi, EC2 istanze Amazon e istanze RDS nel tuo account. Questo aiuta a ridurre i costi di infrastruttura laddove le risorse non sono destinate a funzionare 24 ore su 24, 7 giorni su 7. La soluzione si basa su Instance Scheduler on AWS, ma contiene funzionalità e personalizzazioni aggiuntive specifiche per le esigenze di AMS.

> **Note**
>
> Per impostazione predefinita, AMS Resource Scheduler non interagisce con risorse che non fanno parte di uno stack. AWS CloudFormation La risorsa deve far parte di uno stack che inizia con «stack-», «sc-» o «SC-». Per pianificare le risorse che non fanno parte di uno CloudFormation stack, puoi aggiornare il parametro dello stack Resource Scheduler a. `ScheduleNonStackResources` `Yes`

AMS Resource Scheduler utilizza periodi e pianificazioni:

- I periodi definiscono gli orari di esecuzione di Resource Scheduler, ad esempio l'ora di inizio, l'ora di fine e i giorni del mese.
- Le pianificazioni contengono i periodi definiti, insieme a configurazioni aggiuntive, come la finestra di manutenzione SSM, il fuso orario, l'impostazione di ibernazione e così via; e specificano quando le risorse devono essere eseguite, in base alle regole del periodo configurate.

È possibile configurare questi periodi e pianificazioni utilizzando i tipi di modifica automatici di AMS Resource Scheduler (). CTs

Per tutti i dettagli sulle impostazioni disponibili per AMS Resource Scheduler, consulta la documentazione corrispondente di AWS Instance Scheduler in Solution components. Per una

visione dell'architettura della soluzione, consulta la documentazione corrispondente di AWS Instance Scheduler in Architecture overview.html.

Installazione di AMS Resource Scheduler

Per implementare AMS Resource Scheduler, utilizza il tipo di modifica automatica (CT): Deployment | AMS Resource Scheduler | Solution | Deploy (ct-0ywnhc8e5k9z5) per generare una RFC che poi distribuisca la soluzione nel tuo account. Una volta eseguita la RFC, nel tuo account viene automaticamente fornito uno stack contenente le risorse AMS Resource Scheduler con configurazione predefinita. CloudFormation Per ulteriori informazioni sui tipi di modifica del Resource Scheduler, consulta AMS Resource Scheduler.

> **Note**
>
> Per scoprire se AMS Resource Scheduler è già distribuito nel tuo account, controlla la console AWS Lambda per quell'account e cerca la funzione Scheduler. AMSResource

Dopo aver installato AMS Resource Scheduler nel tuo account, ti consigliamo di rivedere la configurazione predefinita e, se necessario, personalizzare configurazioni come tag key, fuso orario, servizi pianificati e così via, in base alle tue preferenze. Per i dettagli sulle personalizzazioni consigliate, consulta la sezione successiva. Personalizzazione di AMS Resource Scheduler

Per effettuare le configurazioni personalizzate o semplicemente confermare la configurazione del Resource Scheduler,

Personalizzazione di AMS Resource Scheduler

Ti consigliamo di personalizzare le seguenti proprietà di AMS Resource Scheduler utilizzando i tipi di modifica di AMS Resource Scheduler aggiornati, vedi AMS Resource Scheduler.

- Nome tag: il nome del tag che Resource Scheduler utilizzerà per associare le pianificazioni delle istanze alle risorse. Il valore predefinito è Schedule.
- Servizi pianificati: un elenco separato da virgole di servizi che Resource Scheduler può gestire. Il valore predefinito è «ec2, rds, autoscaling». I valori validi sono «ec2", «rds» e «autoscaling»
- Fuso orario predefinito: Specificare il fuso orario predefinito da utilizzare per Resource Scheduler. Il valore predefinito è UTC.

- Usa CMK: un elenco separato da virgole di Amazon KMS Customer Managed Key (CMK) ARNs a cui è possibile concedere le autorizzazioni a Resource Scheduler.
- Utilizzo LicenseManager: è possibile concedere le autorizzazioni a un elenco separato da virgole di AWS Licence Manager per quel Resource Scheduler. ARNs

> **Note**
>
> Di tanto in tanto, AMS può rilasciare funzionalità e correzioni per mantenere aggiornato AMS Resource Scheduler nell'account dell'utente. Quando ciò accade, tutte le personalizzazioni apportate all'AMS Resource Scheduler vengono mantenute.

Utilizzo di AMS Resource Scheduler

Per configurare AMS Resource Scheduler dopo l'implementazione della soluzione, utilizza il Resource Scheduler automatizzato CTs per creare, eliminare, aggiornare e descrivere (ottenere dettagli sui) periodi di AMS Resource Scheduler (gli orari in cui viene eseguito Resource Scheduler) e pianificazioni (i periodi configurati e altre opzioni). Per un esempio di utilizzo dei tipi di modifica di AMS Resource Scheduler, consulta AMS Resource Scheduler.

Per selezionare le risorse da gestire con AMS Resource Scheduler, dopo la distribuzione e la creazione della pianificazione, utilizzi AMS Tag Create CTs per etichettare i gruppi di Auto Scaling, gli stack Amazon RDS e le risorse EC2 Amazon con la chiave di tag che hai fornito durante la distribuzione e la pianificazione definita come valore del tag. Dopo aver taggato le risorse, viene pianificato l'avvio o l'arresto delle risorse in base alla pianificazione del Resource Scheduler definita.

L'utilizzo di AMS Resource Scheduler non comporta costi aggiuntivi. Tuttavia, la soluzione ne utilizza diverse Servizi AWS e queste risorse ti verranno addebitate man mano che vengono utilizzate. Per ulteriori dettagli, consulta Panoramica dell'architettura.

Per disattivare AMS Resource Scheduler:

- Per la disattivazione o la disattivazione temporanea: invia una RFC utilizzando il tipo di modifica automatizzato Management | AMS Resource Scheduler | State | Disable change type (ct-14v49adibs4db)
- Per la rimozione permanente: invia una richiesta RFC di gestione | Altro | Altro | Aggiornamento (revisione richiesta) (ct-0xdawir96cy7k) che richiede la rimozione dal sistema di automazione delle versioni di Resource Scheduler

Stima dei costi di AMS Resource Scheduler

Per tenere traccia dei risparmi sui costi, AMS Resource Scheduler presenta un componente che calcola ogni ora i risparmi sui costi stimati per le risorse Amazon EC2 e RDS gestite dallo scheduler. Questi dati sui risparmi sui costi vengono quindi pubblicati come CloudWatch metrica (`AMS/ResourceScheduler`) per aiutarti a tenerne traccia. Lo strumento di stima dei costi stima i risparmi solo sulle ore di funzionamento delle istanze. Non tiene conto di altri costi, come i costi di trasferimento dei dati associati a una risorsa.

Lo strumento di stima del risparmio sui costi è abilitato con Resource Scheduler. Funziona ogni ora e recupera i dati sui costi e sull'utilizzo da. AWS Cost Explorer In base a questi dati, calcola il costo orario medio per ogni tipo di istanza e quindi proietta il costo per un'intera giornata se l'istanza era in esecuzione senza pianificazione. Il risparmio sui costi è la differenza tra il costo previsto e il costo effettivo riportato da Cost Explorer per un determinato giorno.

Ad esempio, se l'istanza A è configurata con Resource Scheduler per essere eseguita dalle 9:00 alle 17:00, ovvero otto ore in un determinato giorno. Cost Explorer riporta il costo pari a $1 e l'utilizzo a 8. Il costo orario medio è quindi di 0,125 USD. Se l'istanza non è stata pianificata con Resource Scheduler, l'istanza verrà eseguita 24 ore su 24 in quel giorno. In tal caso, il costo sarebbe stato 24x0,125 = 3 USD. Resource Scheduler ti ha aiutato a ottenere un risparmio sui costi di 2$.

Affinché lo strumento di stima del risparmio dei costi recuperi i costi e l'utilizzo solo per le risorse gestite da Resource Scheduler da Cost Explorer, la chiave tag utilizzata da Resource Scheduler per indirizzare le risorse deve essere attivata come tag di allocazione dei costi nella dashboard di fatturazione. Se l'account appartiene a un'organizzazione, la chiave del tag deve essere attivata nell'account di gestione dell'organizzazione. Per informazioni su questa operazione, vedere Attivazione dei tag di allocazione dei costi definiti dall'utente e dei tag di allocazione dei costi definiti dall'utente

Dopo l'attivazione della chiave del tag come tag di allocazione dei costi, la AWS fatturazione inizia a tenere traccia dei costi e dell'utilizzo delle risorse gestite da Resource Scheduler e, una volta che i dati sono disponibili, lo strumento di stima dei costi inizia a calcolare i risparmi sui costi e a pubblicare i dati nello spazio dei nomi delle metriche in. `AMS/ResourceScheduler` CloudWatch

Suggerimenti per la stima dei costi

Cost Savings Estimator non prende in considerazione sconti come istanze riservate, piani di risparmio e così via, nel calcolo. L'Estimator prende i costi di utilizzo da Cost Explorer e calcola il

costo medio orario per le risorse. Per maggiori dettagli, consulta Understanding your AWS Cost Datasets: A Cheat Sheet

Affinché lo strumento di stima del risparmio sui costi recuperi i costi e l'utilizzo solo per le risorse gestite da Resource Scheduler da Cost Explorer, la chiave tag utilizzata da Resource Scheduler per indirizzare le risorse deve essere attivata come tag di allocazione dei costi nella dashboard di fatturazione. Se l'account appartiene a un'organizzazione, la chiave del tag deve essere attivata nell'account di gestione dell'organizzazione. Per informazioni su questa operazione, consulta Tag di allocazione dei costi definiti dall'utente. Se il tag di allocazione dei costi non è attivato, lo stimatore non è in grado di calcolare i risparmi e pubblicare la metrica, anche se è abilitata.

Le migliori pratiche di AMS Resource Scheduler

Pianificazione delle istanze Amazon EC2

- Il comportamento di chiusura dell'istanza deve essere impostato su `stop` e non su. `terminate` È preimpostato `stop` per le istanze create con il tipo di modifica automatica AMS Amazon EC2 Create (ct-14027q0sjyt1h) e può essere impostato per le istanze EC2 Amazon create con l'ingestione, impostando la proprietà su. AWS CloudFormation `InstanceInitiatedShutdownBehavior` `stop` Se il comportamento di chiusura delle istanze è impostato su`terminate`, le istanze termineranno quando Resource Scheduler le arresta e lo scheduler non sarà in grado di riavviarle.
- Le EC2 istanze Amazon che fanno parte di un gruppo Auto Scaling non vengono elaborate singolarmente da AMS Resource Scheduler, anche se sono contrassegnate.
- Se il volume root dell'istanza di destinazione è crittografato con una chiave master del cliente (CMK) KMS, è necessario aggiungere un'`kms:CreateGrant`autorizzazione aggiuntiva al ruolo IAM di Resource Scheduler, affinché lo scheduler possa avviare tali istanze. Per impostazione predefinita, questa autorizzazione non viene aggiunta al ruolo per una maggiore sicurezza. Se richiedi questa autorizzazione, invia una RFC con il tipo di modifica Management | AMS Resource Scheduler | Solution | Update e specifica un elenco separato da virgole ARNs del KMS. CMKs

Pianificazione dei gruppi di Auto Scaling

- AMS Resource Scheduler avvia o arresta la scalabilità automatica dei gruppi di Auto Scaling, non delle singole istanze del gruppo. Cioè, lo scheduler ripristina la dimensione del gruppo Auto Scaling (inizio) o imposta la dimensione su 0 (arresto).
- AutoScaling Gruppo di tag con il tag specificato e non le istanze all'interno del gruppo.

- Durante l'arresto, AMS Resource Scheduler memorizza i valori di capacità minima, desiderata e massima del gruppo Auto Scaling e imposta la capacità minima e desiderata su 0. Durante l'avvio, lo scheduler ripristina la dimensione del gruppo Auto Scaling com'era durante l'arresto. Pertanto, le istanze del gruppo Auto Scaling devono utilizzare una configurazione di capacità appropriata in modo che la chiusura e il riavvio delle istanze non influiscano su alcuna applicazione in esecuzione nel gruppo Auto Scaling.
- Se il gruppo Auto Scaling viene modificato (la capacità minima o massima) durante un periodo di esecuzione, lo scheduler memorizza la nuova dimensione del gruppo Auto Scaling e la utilizza per ripristinare il gruppo al termine di una pianificazione di interruzioni.

Pianificazione delle istanze Amazon RDS

- Lo scheduler può scattare un'istantanea prima di arrestare le istanze RDS (non si applica al cluster Aurora DB). Questa funzionalità è attivata per impostazione predefinita con il parametro del modello Create RDS Instance Snapshot impostato su true. CloudFormation Lo snapshot viene conservato fino alla successiva interruzione dell'istanza Amazon RDS e alla creazione di una nuova istantanea.

  Scheduler può utilizzare istanze start/stop Amazon RDS che fanno parte di un cluster o di un database Amazon RDS Aurora o in una configurazione con più zone di disponibilità (Multi-AZ). Tuttavia, verifica la limitazione di Amazon RDS quando lo scheduler non sarà in grado di interrompere l'istanza Amazon RDS, in particolare le istanze Multi-AZ. Per pianificare l'avvio o l'arresto di Aurora Cluster, usa il parametro del modello Schedule Aurora Clusters (l'impostazione predefinita è true). Il cluster Aurora (non le singole istanze all'interno del cluster) deve essere etichettato con la chiave tag definita durante la configurazione iniziale e il nome della pianificazione come valore del tag per pianificare quel cluster.

  Ogni istanza Amazon RDS ha una finestra di manutenzione settimanale durante la quale vengono applicate eventuali modifiche al sistema. Durante la finestra di manutenzione, Amazon RDS avvierà automaticamente le istanze che sono state interrotte per più di sette giorni per applicare la manutenzione. Tieni presente che Amazon RDS non interromperà l'istanza una volta completato l'evento di manutenzione.

  Lo scheduler consente di specificare se aggiungere la finestra di manutenzione preferita di un'istanza Amazon RDS come periodo di esecuzione alla sua pianificazione. La soluzione avvierà l'istanza all'inizio della finestra di manutenzione e la interromperà al termine della finestra di

manutenzione se nessun altro periodo di esecuzione specifica che l'istanza deve essere eseguita e se l'evento di manutenzione è completato.

Se l'evento di manutenzione non viene completato entro la fine della finestra di manutenzione, l'istanza verrà eseguita fino all'intervallo di pianificazione successivo al completamento dell'evento di manutenzione.

> **Note**
>
> Lo Scheduler non verifica che una risorsa sia avviata o interrotta. Effettua la chiamata API e va avanti. Se la chiamata API fallisce, registra l'errore per consentirne l'analisi.

AWS Systems Manager in AMS Advanced

Un AWS Systems Manager documento (documento SSM) definisce le azioni che Systems Manager esegue sulle AWS risorse. Systems Manager include più di una dozzina di documenti preconfigurati che è possibile utilizzare specificando i parametri in fase di esecuzione. I documenti utilizzano JavaScript Object Notation (JSON) o YAML e includono passaggi e parametri specificati dall'utente.

AWS Managed Services (AMS) è un editore affidabile per documenti SSM. I documenti SSM di proprietà di AMS sono condivisi solo con account AMS integrati, iniziano sempre con un prefisso riservato (AWSManagedServices-*) e vengono visualizzati nella console Systems Manager, come di proprietà di. AWS Il processo AMS per lo sviluppo e la pubblicazione di documenti SSM segue le AWS migliori pratiche e richiede diverse revisioni tra pari durante l'intero ciclo di vita del documento. Per ulteriori informazioni sulle AWS migliori pratiche per la condivisione di documenti SSM, consulta Best practice for shared SSM documents.

Documenti AMS Advanced SSM disponibili

I documenti AMS Advanced SSM sono disponibili esclusivamente per i clienti AMS Advanced e vengono utilizzati per automatizzare il flusso di lavoro operativo per la gestione dell'account.

Per visualizzare i documenti AMS Advanced SSM disponibili su: Console di gestione AWS

1. Aprire la console di Systems Manager dalla console.AWS Systems Manager
2. Scegli Condiviso con me.

3. Nella barra di ricerca, filtra per prefisso del nome del documento, quindi Uguale e imposta il valore su Services-. AWSManaged

   Per le istruzioni AWS CLI, consulta Utilizzo di documenti SSM condivisi.

Versioni dei documenti AMS Advanced SSM

I documenti SSM supportano il controllo delle versioni. I documenti AMS Advanced SSM non possono essere modificati dall'account del cliente e non possono essere ricondivisi. Sono gestiti e mantenuti centralmente da AMS Advanced per la gestione dell'account.

I numeri di versione vengono incrementati con ogni aggiornamento del documento in uno specifico Regione AWS. Man mano che diventano disponibili nuove regioni, lo stesso contenuto del documento in due aree può avere numeri di versione diversi; questo è tipico e non significa che il loro comportamento sarà diverso. Se desideri confrontare due documenti AMS Advanced SSM, ti consigliamo di confrontare i loro hash con la CLI AWS :

```
aws ssm describe-document \
--name AWSManagedServices-DOCUMENTNAME \
--output text --query "Document.Hash"
```

Due documenti SSM sono identici se i loro hash corrispondono.

Prezzi di Systems Manager in AMS

L'accesso ai documenti AMS Advanced SSM è gratuito. Il costo di runtime varia in base al tipo di documento SSM, ai relativi passaggi e alla durata del runtime. Per ulteriori informazioni, consulta i AWS Systems Manager prezzi.

Account AMS fuori bordo

AMS offre assistenza all'off-boarding per account di landing zone con account singolo e landing zone con più account.

AMS non comunica nulla all'utente durante l'offboarding per evitare ripercussioni sulle sue dipendenze. AMIs Se desideri rimuovere AMS AMIs dal tuo account, puoi utilizzare l'API per nascondere dati specifici. `cancel-image-launch-permission` AMIs Ad esempio, puoi utilizzare

lo script seguente per nascondere tutti gli AMS AMIs che sono stati condivisi con il tuo account in precedenza:

```
for ami in $(aws ec2 describe-images --executable-users self --owners 027415890775 --
query 'Images[].ImageId' --output text) ;
    do
    aws ec2 cancel-image-launch-permission --image-id $ami ;
    done
```

È necessario che sia installata l'AWS CLI v2 affinché lo script possa essere eseguito senza errori. Per i passaggi di installazione dell'interfaccia a riga di comando di AWS, consulta Installazione o aggiornamento dell'ultima versione dell'interfaccia a riga di comando di AWS. Per i dettagli sul `cancel-image-launch-permission` comando, consulta. `cancel-image-launch-permission`

> **Note**
>
> La data di cessazione del servizio è l'ultimo giorno del mese di calendario successivo alla fine del periodo di preavviso di risoluzione 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.

Argomenti

Fuori bordo dagli account di landing zone con account singolo AMS

AMS offre assistenza per lo sbarco entro 30 giorni prima della cessazione di AMS.

È necessario richiedere l'assistenza per la partenza dall'imbarco almeno 7 giorni prima che tale assistenza possa essere fornita. L'assistenza per lo sbarco può essere offerta in due forme:

- Trasferimento del controllo: AMS ti restituisce il controllo dell'account insieme alle credenziali di accesso per tutte le applicazioni gestite da AMS, oppure
- Chiusura delle risorse per la chiusura dell'account: AMS elimina tutti i dati presenti nell'ambiente gestito da AMS e sfornisce tutte le risorse attive presenti nell'account. Quando inviano la richiesta di offboarding, i clienti possono richiedere che AMS:
  - Eliminare o conservare gli oggetti di dati (compresi i log) archiviati nei bucket Amazon S3
  - Rimuovere o conservare i bucket Amazon S3
  - Rimuovi o conserva AWS Backup i punti di ripristino

> **Important**
>
> Qualsiasi altra richiesta specifica (soggetta a plausibilità) deve essere comunicata ad AMS prima dell'inizializzazione dell'offboarding.

Prerequisiti opzionali (se richiesti):

> **Note**
>
> Prima della richiesta di offboarding, i clienti possono richiedere l'assistenza di AMS per trasferire i dati nel formato esistente utilizzando AWS Snowball Edge qualsiasi altro supporto con cui AWS si interfaccia.

Oltre ai backup dei dati, è possibile fornire i seguenti dati dei clienti come parte dell'assistenza durante l'offboarding:

- Dati archiviati nei servizi di archiviazione, compresi i registri
- Schemi dei tipi di modifica specifici del cliente
- CloudFormation modelli per schemi di modifica dei tipi di modifica

Se le attività di offboarding non vengono completate al momento della cessazione di AMS, trasferiamo i controlli degli account per consentire all'utente di completare qualsiasi attività in sospeso.

Funzione	Cosa è stato rimosso	Impatto	Azioni necessarie
Monitoraggio, registrazione, avvisi	AMS Monitoring rimosso MMS (Managed Monitoring System) annullata la sottoscrizione Resource Tagger e Alarm Manager rimossi CloudWatch Gli avvisi di base rimangono relativi alle risorse esistenti GuardDuty e Macie: La proprietà torna a te	AMS non ha più accesso o visibilità sulle risorse e sull'ambiente dell'utente.	Gli imprevisti per i servizi rimossi e annullati sono di tua proprietà.
Gestione del Backup	L'automazione di AMS Backup viene rimossa sebbene il AWS Backup servizio rimanga disponibile per l'uso. Gli archivi e i dati di backup vengono conservati a meno che non venga richiesta l'eliminazione.	AMS non monitora più i processi di backup né esegue azioni di ripristino durante gli incidenti. Gli allarmi e gli avvisi sono disattivati. L'eliminazione del ruolo di backup IAM e delle chiavi KMS rende i backup AMS inutilizzabili.	I piani di Backup AMS devono essere riconfigurati. Tutta la responsabilità del monitoraggio e della riparazione rientra nelle tue mani.
Automazioni AMS per la gestione dei servizi	I runbook di automazione AWS SSM curati da AMS,	Nessun accesso AMS ai tuoi account.	Tutte le funzioni di automazione, incluse SSM, SNS

Funzione	Cosa è stato rimosso	Impatto	Azioni necessarie
	le funzioni Amazon Simple Notification Service (SNS) e Lambda non sono più disponibili. AWS	Tutta l'automazione è disattivata.	e Lambda, devono essere ricreate, se necessario.
Conformità	Visibilità e monitoraggio di AMS per tutti GuardDuty e AWS Config regole rimosse, sebbene queste regole rimangano sugli account.	Tutto il monitoraggio, il reporting e la correzione di Amazon GuardDuty and AWS Config Rules non sono più gestiti da AMS.	Il monitoraggio e la correzione di tutti gli strumenti di sicurezza e conformità sono a carico dell'utente.
Agenti in istanza	L'accesso a Resource Scheduler, Resource Tagger o alla configurazione automatica dell'istanza per installare gli agenti richiesti nelle EC2 istanze viene rimosso.	CloudWatch e gli agenti SSM sulle istanze rimangono invariati con le configurazioni esistenti, tuttavia AMS non fornisce più assistenza in queste configurazioni.	Gestisci l'etichettatura e le configurazioni su istanza e degli agenti SSM. CloudWatch

Funzione	Cosa è stato rimosso	Impatto	Azioni necessarie
Infrastruttura di patch e reportistica	AMS non gestisce più le attività pre e successive all'appli cazione delle patch e l'accesso e la visibilit à a questi servizi vengono rimossi.	AMS non crea più un'istantanea dell'istanza prima dell'applicazione delle patch, non installa e monitora più l'install azione della patch e non notifica più all'utente il risultato . I report e i bucket S3 di «verifica» vengono lasciati nei tuoi account su tua richiesta. AMS non genera più report sulle metriche di servizio.	Conservate le linee di base e le istantane e delle patch create in passato. Inoltre, la configurazione delle finestre di manutenzione delle patch rimane invariata , ma le patch non vengono più installat e o corrette da AMS. Tutti i report sulle metriche operative dell'infrastruttura sono ora sotto la tua responsabilità.
Gestione dei processi	Tutti gli account vengono esclusi dalla gestione del servizio fornito per gli incidenti, inclusa la gestione delle richieste di assistenz a, dei problemi e delle modifiche.	Tutte le interruzioni del servizio precedent emente risolte da AMS mediante incidenti e richieste di assistenza e modifiche all'ambie nte, nonché le indagini sulle cause principali, vengono gestite più a lungo da AMS.	L'utente riacquista la piena proprietà di tutta la gestione dei processi.

Fuori bordo dagli account AMS con più account landing zone

Esistono due tipi di AWS account che puoi deimbarcare dalla landing zone multi-account AMS Advanced:

- Account applicativi
- Account principali

Per effettuare l'offboard di tutti gli account dalla landing zone con più account AMS, devi effettuare l'offboard di tutti gli account Application prima di eliminare gli account Core.

Per rilevare e continuare a gestire i carichi di lavoro negli account Application o Core trasferiti fuori bordo, assicurati di consultare questa documentazione con il team addetto all'account AMS. Questa documentazione descrive le modifiche apportate da AMS durante il processo offboard.

Attività da completare per il funzionamento continuo degli account trasferiti fuori bordo

Le seguenti attività sono necessarie per continuare a gestire gli account che hai trasferito dalla landing zone multi-account AMS:

- Attiva la modalità Sviluppatore: per ottenere maggiori autorizzazioni per i tuoi account, attiva la modalità Sviluppatore prima di eliminare gli account delle applicazioni da AMS. Quando attivi la modalità Sviluppatore, puoi apportare più facilmente le modifiche necessarie per prepararti all'offboarding. Non cercare di rimuovere o modificare le risorse dell'infrastruttura AMS. Se elimini le risorse dell'infrastruttura AMS, AMS potrebbe non riuscire a trasferire correttamente il tuo account. Per informazioni su come abilitare la modalità Sviluppatore, consultaGuida introduttiva alla modalità AMS Advanced Developer.

  Se non riesci a completare le modifiche necessarie per prepararti all'offboarding dopo aver attivato la modalità Sviluppatore, contatta il team del tuo account AMS per discutere delle tue esigenze.
- Scegli un metodo alternativo per l'accesso EC2 allo stack: dopo aver disattivato gli account Application da AMS, non potrai più utilizzarli RFCs per accedere alle risorse dello stack. Modifiche all'offboardingEsamina e scegli un metodo di accesso alternativo in modo da mantenere l'accesso ai tuoi stack. Per ulteriori informazioni, consulta Accedi alle alternative.

Account applicativi AMS Offboard

Per eliminare gli account dell'Applicazione dal tuo ambiente di landing zone con più account, completa i seguenti passaggi per ciascun account:

1. Verifica che non ci siano posti aperti RFCs nell'account. Per ulteriori informazioni, consulta Crea, clona, aggiorna, trova e annulla RFCs.
2. Verifica di poter accedere all'indirizzo e-mail dell'utente principale o root dell'account.

3. Dall'account dell'applicazione, invia una RFC con il tipo di modifica Account dell'applicazione | Confirm offboarding (ct-2wlfo2jxj2rkj). Nella RFC, specifica l'account dell'Applicazione da offboard.
4. Dall'account di gestione, invia una RFC con il tipo di modifica Account di gestione | Offboard Application Account (ct-0vdiy51oyrhhm). Nella RFC, specifica l'account dell'applicazione da offboard. Inoltre, indica se desideri eliminare o mantenere l'allegato del gateway di transito alla landing zone.
5. Per assicurarti che la fatturazione con AMS venga interrotta, comunica al CSDM che hai effettuato l'offboarding dell'account.

Dopo l'offboarding dell'account dell'Applicazione si verifica quanto segue:

- Tutti i componenti non sono associati ai servizi AMS, ma le risorse create rimangono nell'account. Puoi scegliere di mantenere o chiudere l'account AMS offboarding.
- Gli account principali e gli altri account Application rimanenti funzionano normalmente dopo l'offboarding di un account Application.
- La fatturazione AMS viene interrotta, ma la AWS fatturazione non viene interrotta fino alla chiusura dell'account. Per ulteriori informazioni, consulta Cosa devi sapere prima di chiudere l'account.
- Se un account viene chiuso, l'account è visibile nell'organizzazione dello `suspended` stato per 90 giorni. Dopo 90 giorni, l'account chiuso viene rimosso definitivamente e non è più visibile nell'organizzazione.
- Dopo la chiusura dell'account, puoi comunque accedere e presentare una richiesta di assistenza o un contatto Supporto per 90 giorni.
- Dopo 90 giorni, tutti i contenuti che rimangono nell'account vengono eliminati definitivamente e i AWS servizi rimanenti vengono interrotti.

Domande frequenti sull'offboarding di un account applicativo

D: Posso usare i miei ruoli IAM federati per continuare ad accedere a un account Application che ho trasferito dalla mia landing zone con più account AMS?

Sì. I ruoli predefiniti AWS Identity and Access Management (IAM) creati da AMS rimangono disponibili nell'account dopo l'offboarding di AMS. Tuttavia, questi ruoli e politiche sono progettati per essere utilizzati con la gestione degli accessi AMS. Per fornire l'accesso necessario agli utenti, potrebbe essere necessario distribuire le proprie risorse IAM.

D: Come posso ottenere l'accesso completo a un account dell'applicazione che ho trasferito dalla mia landing zone con più account AMS?

Gli account delle applicazioni fuori bordo vengono spostati nell'unità organizzativa (OU) obsoleta nella struttura degli account. AWS Organizations Questa mossa elimina le restrizioni di accesso SCP che in precedenza bloccavano l'accesso degli utenti root. Per informazioni su come reimpostare le credenziali dell'utente root, vedere Reimpostazione di una password utente root persa o dimenticata.

D: Quali modifiche vengono apportate durante l'offboarding dell'account dell'Applicazione?

Per informazioni sulle azioni intraprese da AMS quando il servizio esclude gli account, consulta. Modifiche all'offboarding

D: Posso effettuare l'offboard di un account Application senza scollegarlo dal gateway di transito?

Sì. Utilizzate il tipo di modifica dell'account di gestione | Offboard Application Account (ct-0vdiy51oyrhhm) per inviare la RFC e specificate il parametro come. `DeleteTransitGatewayAttachment` `False`

D: Quanto tempo occorre per trasferire un account Application?

Quando utilizzi l'account di gestione | Offboard Application Account (ct-0vdiy51oyrhhm), cambia il tipo di modifica entro 1 ora. RFCs

D: È obbligatorio chiudere l'account offboarding?

No. La chiusura dell'account dopo l'offboarding con AMS non è obbligatoria. Durante il processo di offboarding, AMS rimuove l'accesso e la gestione del tuo AWS account, ma il tuo account e le tue risorse all'interno dell'account rimangono. È importante notare che dopo l'offboarding di AMS, sei l'unico responsabile della gestione e della manutenzione del tuo account e delle tue AWS risorse. AMS non è responsabile per eventuali problemi, incidenti o interruzioni del servizio che potrebbero verificarsi nel tuo account dopo il completamento del processo di offboarding. Per ulteriori informazioni, consulta Come posso chiudere il mio account? AWS .

D: Se invio una richiesta di chiusura dell'account, tutte le risorse esistenti vengono eliminate immediatamente?

No. La chiusura dell'account non comporta l'interruzione delle tue risorse. Le risorse dell'account terminano automaticamente 90 giorni dopo la richiesta di chiusura. La fatturazione AMS si interrompe, ma la fatturazione AWS delle risorse non si interrompe finché non chiudi l'account. Per ulteriori informazioni, consulta Cosa devi sapere prima di chiudere l'account.

D: Posso programmare l'offboarding di un account Application?

Sì. È possibile programmarne RFCs l'esecuzione in un momento specifico. Tuttavia, l'Application Account | Confirm offboarding RFC deve essere completato prima di poter pianificare l'account di gestione | Offboard Application Account RFC. Per ulteriori informazioni, vedere Pianificazione RFC.

Account applicativo per l'offboarding di RACI

- R: Parte responsabile. La parte responsabile del completamento dell'attività elencata.
- A: Parte responsabile. La parte che approva l'attività completata.
- C: Parte consultata. Una parte le cui opinioni vengono richieste, in genere in qualità di esperti in materia, e con la quale esiste una comunicazione bilaterale.
- I: Parte informata. Una parte che viene informata sui progressi, spesso solo al completamento dell'attività o del risultato.

Attività	Custon	AWS Managed Services (AMS)
Prerequisiti		
Verifica l'accesso all'indirizzo e-mail principale per ogni ID di AWS accou nt che verrà trasferito	R	C
Consulta la documentazione AMS sulle azioni consigliate ai clienti e prepara gli account per l'offboarding con AMS	R	C
Se necessario, invia una RFC per abilitare la modalità Sviluppatore per preparare gli account per l'offboarding AMS	R	I
Se necessario, scegli un metodo alternativo per l'accesso allo stack. EC2	R	I
Offboarding		

Attività	Custon	AWS Managed Services (AMS)
Invia RFCs per confermare e richiedere la cancellazione degli account Application	R	I
Estrai i componenti AMS dagli account applicativi	I	R
Notifica ad AMS CSDM la presenza di account fuori bordo per interromp ere la fatturazione AMS	R	I
Post-imbarco		
Reimposta la password dell'account utente root e verifica l'accesso root negli account esterni	R	C
Chiudi l'account o segui le indicazioni di AMS sulle azioni consigliate ai clienti nella documentazione sull'offboarding di AMS per continuare a utilizzare gli account	R	C

Account Offboard Core

Per eliminare gli account core con più account landing zone, completa i seguenti passaggi:

1. Verifica che tutti gli account dell'Applicazione nella landing zone siano stati trasferiti da AMS.
2. Verifica di non avere conti aperti RFCs . Per ulteriori informazioni, consulta Crea, clona, aggiorna, trova e annulla RFCs.
3. Verifica di poter accedere all'indirizzo e-mail dell'utente principale o root per tutti gli account Core. Per ulteriori informazioni, consulta Account Multi-Account Landing Zone.
4. Verifica di poter accedere al numero di telefono dell'utente principale o root dell'account di gestione. Utilizza il ruolo `AWSManagedServicesBillingRole` IAM per aggiornare il numero di telefono. Per ulteriori informazioni, vedi Come posso aggiornare il mio numero di telefono associato al mio AWS account? .
5. Accedi al tuo account di gestione delle landing zone AMS e invia una richiesta di servizio AMS. Nella richiesta di servizio, specifica di lasciare l'intera landing zone fuori bordo.

Dopo l'offboarding degli account Core si verifica quanto segue:

- Tutti i componenti non sono associati ai servizi AMS, ma alcune AWS risorse rimangono nell'account. Puoi scegliere di mantenere o chiudere gli account Core trasferiti da AMS.
- La fatturazione AMS viene interrotta, ma la AWS fatturazione non viene interrotta fino alla chiusura dell'account. Per ulteriori informazioni, consulta Cosa devi sapere prima di chiudere l'account.
- Se un account viene chiuso, l'account è visibile nell'organizzazione dello `suspended` stato per 90 giorni. Dopo 90 giorni, l'account membro chiuso viene rimosso definitivamente e non è più visibile nell'organizzazione.
- Dopo la chiusura dell'account, puoi comunque accedere e presentare una richiesta di assistenza o contattare l'assistenza Supporto per 90 giorni.
- Dopo la chiusura dell'account per 90 giorni, qualsiasi contenuto rimasto nell'account viene eliminato definitivamente e i AWS servizi rimanenti vengono interrotti.

Domande frequenti sull'offboarding dell'account principale

D: Posso usare i miei ruoli IAM federati per continuare ad accedere agli account Core trasferiti?

Sì. I ruoli predefiniti AWS Identity and Access Management (IAM) creati da AMS rimangono disponibili nell'account trasferito. Tuttavia, questi ruoli e politiche sono progettati per essere utilizzati con la gestione degli accessi AMS. Per fornire l'accesso necessario agli utenti, potrebbe essere necessario distribuire le proprie risorse IAM.

D: Come posso ottenere l'accesso completo all'account MALZ di gestione, Shared Services, Networking o a un altro account MALZ non applicabile dopo l'offboarding dalla landing zone multi-account AMS?

Dopo l'offboarding, segui le istruzioni riportate in Reimpostazione di una password utente root smarrita o dimenticata per utilizzare le credenziali dell'utente principale (root) per accedere agli account Core diversi dall'account di gestione. A differenza di altri tipi di account, l'account di gestione conserva un dispositivo di autenticazione a più fattori (MFA) inaccessibile associato all'utente root per impedirne l'utilizzo. Per riottenere l'accesso root è necessario seguire la procedura di ripristino del dispositivo MFA perso.

D: Quali modifiche vengono apportate durante l'offboarding dell'account Core?

Per informazioni sulle azioni intraprese da AMS quando il servizio esclude gli account, consulta. Modifiche all'offboarding

D: Quanto tempo occorre per completare l'offboarding dell'account Core?

Il completamento del processo di offboarding dell'account Core richiede in genere fino a 30 giorni. Tuttavia, per assicurarti che tutti i passaggi richiesti siano stati completati correttamente, devi avviare la richiesta di offboarding almeno 7 giorni prima dell'inizio dell'offboarding. Per facilitare la transizione, pianifica in anticipo e invia la richiesta di offboarding in anticipo.

D: Come faccio a gestire i componenti condivisi dopo l'offboarding di AMS?

AMS Managed Active Directory e altri componenti dell'infrastruttura di servizi condivisi sono progettati per l'accesso degli operatori AMS. Potrebbe essere necessario aggiornare i gruppi di sicurezza Amazon Elastic Compute Cloud (Amazon EC2), la policy di controllo dei AWS Organizations servizi (SCP) o apportare altre modifiche per mantenere l'accesso completo a questi componenti.

D: Posso chiudere gli account Core fuori bordo?

Per impostazione predefinita, gli account delle applicazioni hanno diverse dipendenze dagli account MALZ Core, ad esempio l' AWS Organizations appartenenza, la connettività di rete del gateway di transito e la risoluzione DNS tramite AMS Managed Active Directory. Dopo aver risolto queste dipendenze, puoi disattivare e chiudere l'account Core scollegato. Per ulteriori informazioni, consulta Account Multi-Account Landing Zone.

Account principale: offboarding RACI

- R: Parte responsabile. La parte responsabile del completamento dell'attività elencata.
- A: Parte responsabile. La parte che approva l'attività completata.
- C: Parte consultata. Una parte le cui opinioni vengono richieste, in genere in qualità di esperti in materia, e con la quale esiste una comunicazione bilaterale.
- I: Parte informata. Una parte che viene informata sui progressi, spesso solo al completamento dell'attività o del risultato.

Attività	Custon	AWS Managed Services (AMS)
Prerequisiti		

Attività	Custon	AWS Managed Services (AMS)
Verifica l'accesso all'indirizzo email root per ogni ID di account AWS che verrà offboardato	R	C
Verifica l'accesso e aggiorna il numero di telefono dell'utente root per l'account di gestione	R	C
Consulta la documentazione AMS sulle azioni consigliate ai clienti e prepara gli account per l'offboarding AMS	R	C
Offboarding		
Invia una richiesta di servizio per richiedere l'offboarding della landing zone	R	I
Offboard dei componenti AMS dagli account Core	I	R
Post-imbarco		
Reimposta la password dell'account utente root e verifica l'accesso root negli account esterni	R	C
Chiudi gli account o segui le indicazioni di AMS sulle azioni consigliate ai clienti nella documentazione sull'offboarding di AMS per continuare a utilizzare gli account	R	C

Modifiche all'offboarding

La tabella seguente descrive le azioni intraprese da AMS per l'offboarding delle landing zone multi-account, i potenziali impatti e le azioni consigliate.

Componente	Account type (Tipo di account)	Azioni intraprese per l'offboard	Potenziali impatti	Azione consigliata al cliente
Gestione degli accessi	Account delle applicazioni	Dopo l'offboarding, non è più possibile inviare un accesso RFCs temporizzato allo EC2 stack di accesso tramite host AMS bastion just-in-time AMS non gestisce più i componenti relativi all'accesso su nessuno stack di EC2 risorse esistente (PBIS Open agent, script di aggiunta al dominio)	Non è possibile utilizzare AMS bastions tramite RFS per accedere alle istanze EC2 EC2 le istanze avviate da un provider non fornito da AMS non AMIs vengono aggiunte al dominio Active Directory gestito Se non vengono rimossi, gli script di avvio di AMS negli stack di risorse esistenti potrebbero produrre errori a causa della mancanza di dipendenze AMS e impedire il ricongiungimento a un dominio diverso	Utilizzate metodi alternativi per accedere all'istanza (vedi) EC2 Accedi alle alternative Rimuovi gli script di avvio di AMS dagli stack di EC2 risorse esistenti (vedi) Disabilita gli script di EC2 avvio di AMS
Gestione degli accessi (continua)	Account principali	Se hai effettuato la migrazione da PBIS Open a PBIS Enterprise (AD Bridge), AMS non rinnova	Se la licenza PBIS Enterprise ha una scadenza, le credenziali di Active Directory non sono	Se hai effettuato la migrazione a PBIS Enterprise (AD Bridge), decidi se mantenere la licenza

Componente	Account type (Tipo di account)	Azioni intraprese per l'offboard	Potenziali impatti	Azione consigliata al cliente
		più la licenza dopo l'offboarding dell'account principale	valide per gli stack di istanze esistenti basati su Linux EC2	o disattivarla (vedi) PBIS Open/Enterprise (AD Bridge)
Registrazione, monitoraggio, gestione Incident/Event	Account applicativi e principali	I componenti AMS da distribuire Avvisi dal monitoraggio di base in AMS vengono rimossi Gli CloudWatch allarmi Amazon implementati esistenti rimangono ma non creano più incidenti AMS AWS Config le autorizzazioni di aggregazione di AMS e dell'account di sicurezza MALZ Core vengono rimosse AWS Config le regole rimangono implementate e Amazon GuardDuty rimane abilitato, ma non crea più incidenti AMS	Alle risorse appena create non sono applicati il monitoraggio e gli allarmi di base di AMS Gli allarmi metrici dell'infrastruttura e gli eventi di sicurezza non generano più incidenti AMS AWS Config non è più aggregato in un account centrale	Definisci, acquisisci e analizza le metriche operative per visualizzare gli eventi del carico di lavoro e intraprendere le azioni appropriate. Implementa qualsiasi flusso di lavoro di avviso richiesto per continuare e ad applicare il monitoraggio operativo e gli allarmi richiesti sulle nuove risorse e per ricevere avvisi di sicurezza da e AWS Config Amazon. GuardDuty

Componente	Account type (Tipo di account)	Azioni intraprese per l'offboard	Potenziali impatti	Azione consigliata al cliente
Gestione della continuità (Backup e ripristino)	Account delle applicazioni	AMS non monitora più i processi di backup né esegue richieste di backup e ripristino Gli archivi di backup predefiniti di AMS, la chiave di crittografia di backup e il ruolo di backup rimangono	Gli errori delle operazioni di backup potrebbero non essere rilevati	Monitora e rivedi le configurazioni del piano di backup
Gestione delle patch	Account applicativi e core	AMS non monitora più le operazioni di patch per verificarne l'esecuzione corretta né esegue le patch manuali AMS non aggiorna più i componenti dell'infrastruttura AMS Le linee di base delle patch fornite da AMS vengono mantenute I runbook di automazione AWS Systems Manager delle patch forniti da AMS non sono condivisi e non sono più disponibili per l'uso	Gli errori delle operazioni di patching potrebbero non essere rilevati Le configurazioni di patch esistenti che dipendono dai runbook Systems Manager Automation forniti da AMS devono essere riconfigurate per continuare senza interruzioni.	Rivedi e riconfigura le configurazioni di applicazione delle patch in base alle esigenze

Componente	Account type (Tipo di account)	Azioni intraprese per l'offboard	Potenziali impatti	Azione consigliata al cliente
Gestione di rete	Account delle applicazioni	Se specificato, l'allegato del gateway di transito nell'account dell'applicazione offboarding viene rimosso	L'account dell'applicazione fuori bordo non può più utilizzare un gateway di transito per accedere a servizi condivisi, come Active Directory gestito o altri account dell'applicazione	Specificare `DeleteTransitGatewayAttachment` come `False` mantenere la connettività del gateway di transito
Gestione della sicurezza	Account delle applicazioni	L'account è separato dalla console centrale Trend Micro DSM. Inoltre, gli agenti endpoint non inoltrano più avvisi tramite il processo di gestione degli incidenti di AMS Gli agenti Trend Micro rimangono installati ma non vengono più gestiti o aggiornati da AMS Le personalizzazioni AMI fornite da AMS che implementano l'agente Trend Micro non vengono più gestite o aggiornate da AMS.	EC2 ad esempio, i rilevamenti di malware negli endpoint potrebbero non essere rilevati L'agente Trend micro non viene distribuito su EC2 istanze avviate da un fornitore non fornito da AMS AMIs	Valuta le opzioni per continuare o interrompere Trend Micro (vedi) Trend Micro Deep Security

Componente	Account type (Tipo di account)	Azioni intraprese per l'offboard	Potenziali impatti	Azione consigliata al cliente
Gestione della sicurezza (continua)	Account principali	L'infrastruttura Trend Micro DSM rimane invariata negli account Shared Services ma non è più gestita o aggiornata da AMS Trend Micro DSM non inoltra più gli avvisi tramite il processo di gestione degli incidenti di AMS	EC2 ad esempio, i rilevamenti di malware negli endpoint potrebbero passare inosservati EC2 la mancata manutenzione dell'infrastruttura (aggiornamenti delle definizioni, licenze e così via) potrebbe influire sulla protezione degli endpoint delle istanze	Decidi se continuare o interrompere Trend Micro (vedi (vedi) Trend Micro Deep Security

Componente	Account type (Tipo di account)	Azioni intraprese per l'offboard	Potenziali impatti	Azione consigliata al cliente
Gestione delle modifiche	Account Application e Core	La console e l'API AMS RFC vengono rimosse Le politiche di controllo del servizio personalizzate AMS (SCPs) che contengono restrizioni di accesso a livello di account vengono rimosse durante l'offboarding dell'account dell'Applicazione ed eliminate durante l'offboarding dell'account Core	È necessario utilizzare un' AWS API nativa per creare nuove risorse, modificare le risorse esistenti o aggiornare gli stack esistenti CloudFormation Le restrizioni di accesso non vengono più imposte a livello di account tramite AMS fornito da SCPs	Assicurati che i ruoli utente forniscano un accesso sufficiente per utilizzare i servizi AWS Crea SCPs per fornire restrizioni di autorizzazione a livello di account

Componente	Account type (Tipo di account)	Azioni intraprese per l'offboard	Potenziali impatti	Azione consigliata al cliente
Immagini e automazioni del sistema operativo AMS per la gestione dei servizi	Account applicativi e Core	AMS non fornisce più supporto sulle personalizzazioni e sugli script di avvio inclusi in AMS fornito EC2 AMIs I servizi AMS forniti EC2 AMIs restano disponibili negli account offboardati I runbook Systems Manager Automation forniti da AMS non sono condivisi e non sono più disponibili per l'uso	Dopo l'offboarding, AMS AMIs ha fornito il comando CloudFormation send cfn-signal lanciato a `FAILURE` causa della mancanza di dipendenze dai componenti AMS I processi operativi che dipendono dai runbook Systems Manager Automation forniti da AMS potrebbero fallire.	Rivedi e aggiorna tutti i processi di compilazione o operativi che dipendono dai runbook forniti da AMS AMIs o da Systems Manager Automation.
Infrastruttura di servizi condivisi	Account principali	L'accesso AMS viene rimosso e AMS non gestisce più i componenti condivisi, incluso AMS Managed Active Directory AWS Transit Gateway, e AWS Organizations	Perdita di gestione rispetto all'infrastruttura condivisa	Reimposta l'accesso amministrativo ad AMS Managed Active Directory e assumi la gestione dei componenti dei servizi condivisi

Componente	Account type (Tipo di account)	Azioni intraprese per l'offboard	Potenziali impatti	Azione consigliata al cliente
Creazione di report	Account applicativi e Core	AMS non raccoglie più i dettagli a livello di account o di risorsa per i report aggregati	Perdita di informazioni sulle metriche operative e aziendali (copertura di backup e patch, gestione delle modifiche e attività relative agli incidenti)	Sostituisci la necessaria reportistica aggregata dei dati tra gli account con una soluzione propria
Account team e service desk AMS	Account applicativi e Core	L'account team AMS (CSDM, CA) e il service desk operativo AMS non supportano più gli account offboardati	Perdita del supporto operativo con esperienza nell'architettura multi-account delle landing zone progettata da AMS e nei relativi componenti	Assicurati che ci sia personale sufficiente e che abbia dimestichezza con la struttura e le risorse degli account per supportare le operazioni nell'ambiente

Accedi alle alternative

I seguenti sono metodi alternativi per mantenere l'accesso allo EC2 stack dopo aver eliminato gli account AMS:

- Utilizza Session Manager per accedere alle EC2 istanze con autorizzazioni elevate senza richiedere bastioni o accesso alla rete in entrata. Per ulteriori informazioni, consulta AWS Systems Manager Session Manager.
- Riunisci EC2 le istanze a un dominio Active Directory diverso con nuove credenziali di dominio. Se lo utilizzi Directory Service, vedi Aggiungere un' EC2 istanza alla tua directory. AWS Managed Microsoft AD

- Usa gli account utente locali che hai creato tramite uno degli altri metodi di accesso o tramite AWS Systems Manager Run Command.

Disabilita gli script di EC2 avvio di AMS

Sistemi operativi Linux

Usa il gestore di pacchetti della tua distribuzione per disinstallare il `ams-modules` pacchetto. Ad esempio, per l'uso di Amazon Linux 2`yum remove ams-modules`.

Sistemi operativi Windows

La procedura seguente illustra come disabilitare gli script di EC2 avvio in Windows:

1. Windows Server 2008/2012/2012r2/2016/2019:

   Disabilita o rimuovi l'attività pianificata di Managed Services Startup da Task Scheduler. Per elencare le attività pianificate, esegui il `Get-ScheduledTask -TaskName '*Ec2*'` comando.

   Windows Server 2022:

   Rimuovere l'attività EC2 Launch v2. Questa attività viene eseguita `Initialize-AMSBoot` in `postReady` fasi in C:\\ AmazonProgramData\ EC2 Launch\ config\ agent-config.yml sull'istanza. Di seguito è riportato un frammento di un esempio: `agent-config.yml`

   ```
   {
    "task": "executeScript",
    "inputs": [
     {
      "frequency": "always",
      "type": "powershell",
      "runAs": "localSystem"
     }
    ]
   }
   ```

2. (Facoltativo) Rimuovi il seguente contenuto del file:

   ```
   C:\Program Files\WindowsPowerShell\Modules\AWSManagedServices.*
   C:\Windows\System32\WindowsPowerShell\v1.0\Modules
   \AWSManagedServices.Build.Utilities\*
   ```

PBIS Open/Enterprise (AD Bridge)

Per determinare se si utilizza l'edizione PBIS Open o PBIS Enterprise (AD Bridge), esegui il comando seguente in un'istanza gestita Linux EC2 :

```
yum info | grep pbis
```

Di seguito è riportato un esempio di output che mostra PBIS Enterprise (AD Bridge):

```
Name        : pbis-enterprise
From repo   : pbise
Name        : pbis-enterprise-devel
Repo        : pbise
Description : The pbis-enterprise-devel package includes the development
```

PBIS aperto

PBIS Open è un prodotto obsoleto che non supporta più. BeyondTrust Per ulteriori informazioni, consulta la documentazione di pbis-open. BeyondTrust

AD Bridge (PBIS Enterprise)

Puoi effettuare una delle seguenti operazioni:

- Rinnova le licenze e continua a utilizzare AD Bridge. Contatta BeyondTrust per discutere di licenze e supporto.
- Interrompi l'uso di AD Bridge. Esegui il seguente comando Shell per rimuovere il pacchetto PBIS-Enterprise dalle istanze gestite da Linux. Per ulteriori informazioni, consulta la BeyondTrust documentazione Abbandona un dominio e disinstalla l'agente AD Bridge.

  ```
  $ sudo /opt/pbis/bin/uninstall.sh purge
  ```

Abbandona il dominio Active Directory gestito da AMS senza rimuovere l'agente PBIS

È possibile abbandonare l'Active Directory gestito da AMS senza rimuovere l'agente PBIS. Utilizzate una delle seguenti soluzioni, a seconda del sistema operativo in uso:

Linux operating systems

Utilizza PBIS dell'AD gestito da AMS per eseguire il seguente comando di shell per annullare l'accesso a un'istanza Linux EC2 . Per ulteriori informazioni, consulta la documentazione di BeyondTrust pbis-open o BeyondTrust AD Bridge, a seconda della versione utilizzata.

```
$ sudo /opt/pbis/bin/domainjoin-cli leave
```

Potresti visualizzare un messaggio di errore simile al seguente:

```
Error: LW_ERROR_KRB5_REALM_CANT_RESOLVE [code 0x0000a3e1]
Cannot resolve network address for KDC in requested realm
```

Se si verifica questo errore, esegui i seguenti comandi per eliminare il registro del provider AD e riavviare `lwsm` i servizi:

```
$ /opt/pbis/bin/regshell dir '[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers
\ActiveDirectory\DomainJoin]'
```

Utilizza l'output dell'ID di directory ricevuto dal comando precedente (ad esempio,**`A123EXAMPLE.AMAZONAWS.COM`**) per eseguire i seguenti comandi:

```
$ /opt/pbis/bin/regshell delete_tree \
'[HKEY_THIS_MACHINE\Services\lsass\Parameters\Providers\ActiveDirectory\DomainJoin
\DIRECTORYID]'

$ /etc/pbis/redhat/lwsmd restart

$ /opt/pbis/bin/lwsm restart lwreg
```

Windows operating systems

```
# Collect hostname and domain name using:

Test-ComputerSecureChannel -verbose

# Disjoin computer from the domain:

netdom remove hostname /domain:domain name /force
```

> **Note**
>
> Assicurati di disabilitare o rimuovere l'attività pianificata di Managed Services Startup come indicato inDisabilita gli script di EC2 avvio di AMS.

Trend Micro Deep Security

Utilizza una delle seguenti opzioni per continuare o interrompere l'uso di Trend Micro Deep Security:

Continua l'utilizzo

- (In caso di offboarding dell'intero MALZ) Dopo l'offboarding dell'account Core, ricollegate gli account Application scollegati al Trend Micro Deep Security Manager (DSM) esistente e mantenete le licenze nell'account Shared Services. Per ulteriori informazioni, consulta Aggiungere account cloud e Verificare le informazioni sulla licenza. AWS

  1. Accedi all'account dei servizi condivisi e vai alla console Secrets Manager.
  2. Recupera le credenziali di amministratore della console DSM memorizzate nel percorso. `/ams/eps/`
  3. Accedere alla console DSM all'indirizzo https://dsm.sentinel.int.
  4. Scegliete Use Cross Account Role, quindi immettete**`arn:aws:iam::ACCOUNTID:role/mc_eps_cross_account_role`**. Sostituisci ACCOUNTID con l'ID dell'account dell'applicazione offboardato.
  5. Scegli Next (Successivo).
  6. Attendi alcuni minuti che DSM elabori la scoperta dell'account e dimostri che la sincronizzazione è avvenuta correttamente.
- Ricollegate gli account delle applicazioni scollegati a una nuova installazione di Trend Micro DSM. Per ulteriori informazioni, vedere Attivazione e protezione degli agenti e Attivazione dell'agente.
- Ricollega gli account delle applicazioni scollegati a Trend Micro Cloud One. Per ulteriori informazioni, consulta Migrazione da Deep Security a Workload Security e Migrazione da un DSM locale.

Interrompere l'utilizzo

- Disinstalla Trend Micro Deep Security Agents dagli account delle applicazioni scollegati. Per ulteriori informazioni, consulta Disinstalla Deep Security.

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 di incidenti e 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 con ciascuno di questi account OUs è soggetta alla specifica modalità AMS offerta da tali account di base. OUs 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 e 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 una 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.

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 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 clienteCustomerActionPending, oppure suNoActionPending, 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

Riuscito	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	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

Riuscito	Errore
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 esecuzione, si noti che se si forniscono più risorse o RFCs che hanno una lunga durata UserData, l'esecuzione richiede più tempo Eseguito: la RFC è stata eseguita Riuscito/Riuscito: la RFC è stata completata con successo	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

> **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 `InProgress`Success, 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 la modalità di esecuzione = manuale o «revisione richiesta», l'altra è la 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 ripristinare qualsiasi risorsa, utilizzate invece il tipo di modifica «review required» (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 (ct-3kinq0u4l33zf), automatizzato e senza revisione, 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 la TAC automatica (ct-3kinq0u4l33zf), che non richiede alcuna revisione 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 la revisione obbligatoria, manuale, CT.

Consigliamo di utilizzare il CT manuale obbligatorio per la revisione (ct-34sxfo53yuzah) solo quando i tipi di risorse alla deriva non sono supportati dalla correzione della deriva nessuna revisione richiesta, automatizzata, CT (ct-3kinq0u4l33zf) o quando la correzione della deriva non è richiesta, 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 che hanno 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 esaminare i tipi di modifica richiesti, è necessario richiedere un'ora di inizio che sia almeno 24 ore dopo la data prevista di invio della 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 «revisioni richieste» 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 quanto riguarda il tipo di modifica «revisione obbligatoria», 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 «review required» CTs, AMS consiglia di utilizzare l'opzione ASAP Scheduling (scegliere ASAP nella console, lasciare vuote le date di inizio e fine nell'API/CLI) poiché CTs richiedono che un operatore AMS esamini la RFC e possibilmente 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. Usa Inline Create (esegui 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_ID" --change-type-version "VERSION" --title
 "TITLE" --execution-parameters "{\"Description\": \"example\"}"
```

CREAZIONE DEL MODELLO:

> **Note**
>
> Questo esempio di creazione di un 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 le versioni di lunga durata UserData: Create e CTs Create ASG. EC2 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: la riga dell'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 data e ora ISO86 01 (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 data e ora ISO86 01 (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 data e ora ISO86 01 (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 data e ora ISO86 01 (ad esempio, «20170101 T000000Z»)	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 data e ora ISO86 01 (ad esempio, «20170101 T000000Z»)	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 data e ora ISO86 01 (ad esempio, «20170101 T000000Z»)	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 data e ora ISO86 01 (ad esempio, «20170101 T000000Z»)	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
Title	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 del tipo di modifica, 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. Questo avvertimento non

si applica all'API/CLI AMS, ma è comunque importante programmare il manuale con RFCs almeno 8 ore di anticipo.

> **Note**
>
> Quando si utilizza «review required» CTs, 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 il tipo di modifica `AutomationStatus` per uno specifico tipo di modifica utilizzando la CLI AMS, esegui questo comando:

```
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 correlato allo stack. 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. Questa avvertenza non si applica all'API/CLI AMS, ma è comunque importante programmare il manuale con RFCs almeno 8 ore di anticipo.

AMS mira a rispondere a una CT manuale entro quattro 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, è necessario 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 consigliabile rimuovere tutte le risorse aggiunte manualmente da uno stack prima di inviare una richiesta RFC relativa allo stack di eliminazione. 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, in quanto tentano 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 EC2 stack: (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, si avvia un'istanza, che è una copia dell'AMI in esecuzione come server virtuale nel cloud. AMIs sono molto utili e necessari per creare EC2 istanze o gruppi di Auto Scaling; tuttavia, è necessario rispettare alcuni requisiti:

- L'istanza specificata `Ec2InstanceId` deve essere interrotta affinché la RFC abbia esito positivo. Non utilizzate istanze del gruppo Auto Scaling (ASG) per questo parametro perché l'ASG interromperà 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

In caso di EC2 errori 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 o crea una richiesta di assistenza. Per maggiori dettagli, consulta Corrispondenza e allegato RFC (console) e Creazione di una richiesta di servizio in AMS.

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 e sulle EC2 istanze in AWS. È possibile trovarli nella AMS Advanced Application Developer's GuideMigrating workload: Linux pre-ingestion validation e Migrating workload: Windows pre-ingestion validation.

- EC2 Assicurati che l'istanza 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' EC2 istanza 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

EC2 errori di blocco dello stack di istanze

- Verifica se l'istanza è già interrotta o terminata.
- Se l' EC2 istanza è online e vedi l'`InternalError`errore, invia una richiesta di servizio affinché AMS possa esaminarla.
- 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.

EC2 lo stack di istanze crea errori

Il `InternalError` messaggio proviene da CloudFormation; un motivo dello stato CREATION_FAILED. Puoi trovare i 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.

EC2 errori di ripristino del volume dell'istanza

AMS crea una RFC interna per la risoluzione dei problemi quando il ripristino del volume dell' EC2 istanza fallisce. Ciò avviene perché il ripristino del volume delle EC2 istanze 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 contenente 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 o effettuare richieste di assistenza.

- Per richiedere informazioni o consigli, o per accedere a un servizio IT gestito da AMS o per richiedere un servizio aggiuntivo ad AMS, utilizza la console AMS e invia una richiesta di servizio. Per i dettagli, consulta Creazione di una richiesta di assistenza. Per informazioni generali sulle richieste di assistenza AMS, vedere Gestione delle richieste di assistenza.
- 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 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	Sì. Breaks for CloudFormation,CloudTrail, EFS OpenSearch, CloudWatch Logs, SQS, SSM, Tagging api, poiché questi servizi non supportan	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
quelli sopra elencati devono avere prefissi simili a «o in case». `AMS* MC*` upper/lower/mix	o 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 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.		

Standard	Si rompe	Rischi	Raccomandazioni
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 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-	Sì. Lo scopo delle azioni self-service consente di eseguire azioni aggirando il sistema RFC AMS.	Il modello di accesso sicuro è un aspetto tecnico fondamentale di AMS e un utente 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'utente IAM deve disporre di un periodo di tempo limitato e concedere le autorizzazioni in base al privilegio minimo e. need-to-know

Standard	Si rompe	Rischi	Raccomandazioni
Service Provisioned (SSPS) sono esentati a condizione che le azioni vengano eseguite entro i limiti del ruolo assegnato.		L'accesso è registrato CloudTrail solo.	

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 endpoint tra account che appartengono allo stesso cliente.	Sì. Non possibile tramite la policy IAM.	Il traffico in uscita dal tuo account AMS non viene monitorato una volta che esce dal confine dell'account.	Ti consigliamo di effettuare il peering solo con account AMS 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

Standard	Si rompe	Rischi	Raccomandazioni
			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 organizzazione non può essere ottenuta mediante la politica IAM.	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 condividerli all'esterno dell'organizzazione. Possiamo verificarlo in diversi modi, verificalo con il tuo gestore di fornitura dei servizi cloud (CSDM).
20. Qualsiasi registro può essere inoltrato 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			

Standard	Si rompe	Rischi	Raccomandazioni
il dominio e-mail al nome dell'azienda del cliente e all'account collegato a PAYER) utilizzando strumenti interni.			

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 Modifica diretta | Abilita il tipo di modifica (ct-3rd4781c2nnhp), consulta la sezione «Informazioni aggiuntive» per il tipo di modifica pertinente nella sezione AMS Advanced Change Type Reference Change Type Reference Change Type by Classification.

Servizio	Azione
AWS Key Management Service (AWS KMS)	Aggiornamento
AWS Certificate Manager	Create
AWS Identity and Access Management (IAM)	Qualsiasi
Site-to-Site VPN	Qualsiasi
Pianificatore di risorse AMS	
AWS Backup	Crea un piano di backup
Inserimento del carico di lavoro AMS () WIGs	Qualsiasi
Filtro di uscita AMS (Palo Alto gestito)	
Modifiche all'account AMS Advanced MALZ	
Amazon GuardDuty	

Servizio	Azione
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 il nome host
Amazon Machine Images (AMI)	Elimina, condividi
Gruppo EC2 di sicurezza Amazon	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	Create

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

- 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

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 in[Prerequisiti per la modalità AMS Developer](#).
2. Invia una richiesta di modifica (RFC) utilizzando la gestione del tipo di modifica (CT) | Account gestito | Modalità sviluppatore | Abilita (è richiesta la revisione). Per un esempio di come utilizzare questo CT, consulta [Developer Mode | Enable (Review Required)](#).

   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 the`AWSManagedServicesDevelopmentRole`, `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 consentit e tranne. `SetWebACL`

Servizio	Note
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.

Servizio	Note
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: • `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 da`AMS`, `mcManagementHostASG` , and/or `sentinel`.

Servizio	Note
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.
AWS Identity and Access Management (IAM)	Non è possibile eliminare i limiti di autorizza zione 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 (`AWSManagedServicesDevelopme ntRole` per MALZ, `customer_developer _role` per SALZ)). Non è possibile modificare le risorse IAM con il prefisso:`ams`,,,`mc`. `customer_deny_poli cy` and/or `sentinel` Quando si crea una nuova risorsa IAM (ruolo, utente o gruppo), è necessario allegare il limite di autorizzazione (MALZ:`AWSManage dServicesDevelopmentRolePer missionsBoundary` , SALZ:`ams-app-i nfra-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`

Servizio	Note
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-`
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 (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 necessita di 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 (revisione richiesta) (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 di Amazon AppStream 2.0 nel tuo account AMS

Usa la modalità AMS Self-Service Provisioning (SSP) per accedere alle funzionalità di Amazon AppStream 2.0 (AppStream 2.0) direttamente nel tuo account gestito AMS. AppStream 2.0 ti consente di spostare le tue applicazioni desktop in AWS, senza riscriverle. È possibile installare le applicazioni nella AppStream versione 2.0, impostare configurazioni di avvio e rendere le applicazioni disponibili agli utenti. AppStream 2.0 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. AppStream La versione 2.0 consente di avviare applicazioni nella propria rete, il che significa che le applicazioni possono interagire con le AWS risorse esistenti.

Amazon AppStream 2.0 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 AppStream 2.0.

AppStream 2.0 nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso alla AppStream versione 2.0 nel mio account AMS?

Richiedi l'accesso alla AppStream versione 2.0 inviando una RFC al 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 della AppStream versione 2.0 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 flotte AppStream 2.0 e generatori di immagini ai domini Microsoft Active Directory.
  - Creazione di report di AppStream utilizzo personalizzati 2.0.
  - Il branding personalizzato non è attualmente supportato.

D: Quali sono i prerequisiti o le dipendenze per utilizzare la AppStream versione 2.0 nel mio account AMS?

Durante l'invio della RFC a onboard AppStream 2.0, includi il nome del bucket Amazon S3 da utilizzare per il report sull'utilizzo 2.0. AppStream Il nome del bucket viene aggiunto a quello creato durante l'onboarding della `customer-appstream-usagereports-policy` versione 2.0. AppStream

D: Quali funzionalità AppStream 2.0 richiedono una funzionalità separata? RFCs

- Per scegliere un endpoint VPC di interfaccia per AppStream 2.0, 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 la AppStream versione 2.0, consulta Creazione e streaming dagli endpoint VPC dell'interfaccia nella guida per AppStream l'utente 2.0.

- 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 AppStream 2.0 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 2.0. AppStream
- Per creare e scegliere un ruolo IAM che sarà disponibile su tutte le istanze di streaming del parco istanze, invia un tipo di modifica Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entità o policy (revisione richiesta) RFC (ct-3dpd8mdd9jn1r) richiedendo il ruolo IAM con la policy richiesta. Il nome del ruolo IAM deve sempre iniziare con il prefisso: «customer_appstream».
- Le flotte e gli image builder di Amazon AppStream 2.0 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 AppStream 2.0 in Concessione delle autorizzazioni per la creazione e la gestione di oggetti informatici Active Directory.
- Per creare report di utilizzo AppStream 2.0 personalizzati, invia un tipo RFC di gestione | Altro | Altro | Crea modifica richiedendo quanto segue:
  - "AppStreamUsageReports" Creazione di uno 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 di utilizzo dell'ARN del bucket Amazon S3 AppStream per la versione 2.0.

  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 di utilizzo AppStream 2.0,

consulta Creare report personalizzati e analizzare i dati di utilizzo della AppStream versione 2.0, nella AppStream documentazione 2.0.

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 creare 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 (revisione richiesta) (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 Management | AWS service | Self-provisioned service | Aggiungi (review required) (ct-3qe6io8t6jtny) (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 (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 in 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 (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 Management | AWS service | Self-provisioned service | Aggiungi (review required) (ct-3qe6io8t6jtny) tipo di modifica. 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 necessarie 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 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 (revisione richiesta) (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 AWS servizio completamente gestito che semplifica l'automazione della creazione, gestione e distribuzione di

immagini server personalizzate, sicure e up-to-date «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 usi 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 ulteriori informazioni, consulta EC2 Image Builder.

EC2 Domande frequenti su 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 (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 Image EC2 Builder?

- EC2 Ruolo collegato al servizio di 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}/*` Ad 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 Image Builder. EC2

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 . In questo modo non è più necessario effettuare il provisioning, configurare o ridimensionare i cluster di macchine virtuali per eseguire i contenitori.

AWS Fargate 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 di federazione.

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 (revisione richiesta) (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 Kubernetes con 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 usare 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 (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 EC2 gruppi di nodi gestiti o autogestiti non è supportata in AMS. Se hai l'esigenza di utilizzare i EC2 nodi di lavoro, 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:
  - [Obbligatorio] 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, consulta
    - 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):

- [Obbligatorio] 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 (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 EC2 cluster 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
  - EC2 Profilo dell'istanza: customer_emr_cluster_instance_profile
  - Ruolo Auto Scaling: customer_emr_cluster_autoscaling_role
- EC2 Gruppi di sicurezza:
  - 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 conto dell'utente. 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 (revisione richiesta) tipo di modifica (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 (IAM) | Create entità o policy (revisione richiesta) (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 servizio Management | | Self-provisioned Servizio AWS | Aggiungi (è richiesta la revisione) il tipo di modifica prima di utilizzare Amazon EventBridge per effettuare 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 SSP`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 adatta automaticamente al volume e alla velocità effettiva dei dati in entrata. Con Amazon Managed Service for Apache Flink, paghi solo per le risorse utilizzate dalle tue applicazioni di streaming. Non sono previsti costi minimi o di configurazione. 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 Management | AWS service | Self-provisioned service | Aggiungi (review required) (ct-3qe6io8t6jtny) (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 (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 Management | AWS service | Self-provisioned service | Aggiungi (review required) (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 politica aprendo una RFC con il tipo di modifica KMS Key | Create (Review Required):

  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 QuickSight nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle QuickSight funzionalità direttamente nel tuo account gestito da AMS. QuickSight 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, QuickSight consente di creare e pubblicare facilmente

dashboard interattivi che includono approfondimenti sull'apprendimento automatico (ML). Per ulteriori informazioni, consulta Amazon QuickSight.

QuickSight nelle domande frequenti su AWS Managed Services

Domande e risposte comuni:

D: Come posso richiedere l'accesso QuickSight 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_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 QuickSight nel mio account AMS?

- AWS le impostazioni delle risorse su QuickSight non ti saranno accessibili a causa della dipendenza dalla policy 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.
- QuickSight il servizio 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 l'integrazione QuickSight con Active Directory (AD). QuickSight on AMS non supporta l'integrazione con AD a causa di incompatibilità tra la struttura degli account AMS e i QuickSight requisiti di fiducia.

D: Quali sono i prerequisiti o le dipendenze da utilizzare QuickSight nel mio account AMS?

- Quando AMS riceve questa RFC da aggiungere QuickSight, ti viene inviata una richiesta di assistenza per ulteriori informazioni; fornisci loro quanto segue:
  - QuickSight nome dell'account (ad esempio, *`CustomerName`*`-quicksight`
  - QuickSight Edizione (Standard o Enterprise)
  - La AWS regione in cui abilitare il QuickSight servizio (l'impostazione predefinita è la regione AMS AWS).

- Un indirizzo e-mail di notifica per QuickSight l'account.
- (Facoltativo) Il bucket S3 in cui si trovano i file di dati da analizzare.
- Il VPC e la sottorete a IDs cui si connettono QuickSight supportano una funzionalità per aggiungere una connessione VPC, che consente la connettività privata tra QuickSight 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 del modello 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 (revisione richiesta) (ct-3qe6io8t6jtny) il tipo di modifica. 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 sorgente 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 fornito automaticamente dall' 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 Management | Advanced stack components | Identity and Access Management (IAM) | Aggiorna il tipo di modifica dell'entità o della policy (revisione richiesta) (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 (revisione richiesta) (ct-3qe6io8t6jtny) il tipo di modifica. 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 nei loro stack tecnologici 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 (revisione richiesta) (ct-3qe6io8t6jtny) il tipo di modifica. 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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 practice 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 tuoi 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 per 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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 EC2 Amazon/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`, che è 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, questa operazione viene eseguita 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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 un'opzione di accettazione del rischio, 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 | Aggiungi (revisione richiesta) (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 richiesta di modifica (RFC) ad AMS per eliminare o modificare i certificati esistenti, poiché tali azioni richiedono l'accesso amministrativo completo (utilizzare il tipo di modifica Gestione | Altro | Altro | Aggiornamento (ct-0xdawir96cy7k). 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 EC2 istanze, contenitori, dispositivi IoT e 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 tu stesso 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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 rimangano 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' CodeCommitonboarding, CodeBuild CodeDeploy, e CodePipeline con un'unica RFC, invia Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) modifica il tipo 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'onboarding CodeCommit, CodeBuild CodeDeploy, e CodePipeline con un'unica RFC, invia il tipo di modifica Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (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 e EC2 i AWS Fargate server AWS Lambda 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.

> **Note**
>
> Per effettuare l'onboard e CodePipeline con una singola RFC CodeCommit CodeBuild CodeDeploy, invia Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) modifica il tipo 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?

Attualmente supportiamo Compute Platform solo come: Amazon/On-premises. EC2 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 entrare a far parte di CodeCommit CodeBuild, CodeDeploy, e CodePipeline con un'unica RFC, invia Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) modifica il tipo 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 di elaborazione (EC2 Amazon ASGs e) può comportare costi di infrastruttura non necessari, mentre un approvvigionamento insufficiente di elaborazione può portare a prestazioni delle applicazioni scadenti. Compute Optimizer ti aiuta a scegliere i tipi di istanze EC2 Amazon ottimali, comprese quelle che fanno parte di un gruppo Amazon Auto EC2 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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 EC2 calcolo Amazon 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 nel 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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 AWS DataSync Amazon EC2 AMI, il tipo di istanza, la sottorete, il gruppo di sicurezza e fai riferimento a una EC2 coppia di chiavi Amazon 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 AWS DataSync . EC2

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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 AWS Elastic Disaster Recovery nel tuo account AMS

Utilizza la modalità AMS Self-Service Provisioning (SSP) per accedere alle AWS Elastic Disaster Recovery funzionalità direttamente nel tuo account gestito AMS. AWS Elastic Disaster Recovery 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 AWS Elastic Disaster Recovery 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 AWS Elastic Disaster Recovery.

AWS Elastic Disaster Recovery nelle domande frequenti su AWS Managed Services

D: Come posso richiedere l'accesso AWS Elastic Disaster Recovery al mio account AMS?

Richiedi l'accesso inviando un Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 AWS Elastic Disaster Recovery nel mio account AMS?

Non ci sono restrizioni d'uso AWS Elastic Disaster Recovery nel tuo account AMS.

D: Quali sono i prerequisiti o le dipendenze da utilizzare AWS Elastic Disaster Recovery 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 (review required) 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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. 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 RFC Management | Other | Other (ct-1e1xtak34nx76) per distribuire il. `customer_lakeformation_workflow_role` Nella RFC, è necessario fornire il nome del bucket S3 se il bucket è una fonte quando vengono creati i 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 Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo di modifica. Questa RFC fornisce i seguenti `customer_lambda_admin_role` ruoli IAM al tuo account: e. `customer_lambda_basic_execution_role` Dopo averli inseriti 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 le `AWSXrayWriteOnlyAccess` autorizzazioni `AWSLambdaBasicExecutionRole` e; per informazioni, consulta 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 | Aggiungi (review required) (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 (revisione richiesta) tipo di modifica (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. Fai clic su Next (Successivo).
5. Inserisci il nome e la descrizione segreti, il nome inizia sempre con customer-shared/. Ad esempio customer-shared/mykey2022. Fai clic su Next (Successivo).
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 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 in AWS Managed Services

D: Come posso richiedere l'accesso AWS Security Hub CSPM al mio account AMS?

Richiedi l'accesso a Security Hub 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 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 tramite Management | AWS service | Self-provisioned service | Aggiungi (revisione richiesta) (ct-3qe6io8t6jtny) tipo 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 automazio ne 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
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 ResourceP roperty —	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.

Ricerca dei dati necessari (SKMS), AMS

Per trovare i dati di cui hai bisogno quando usi i tuoi account AWS Managed Services (AMS) è necessario utilizzare il sistema AMS Service Knowledge Management, o SKMS. AMS.

SKMS è l'acronimo di Service Knowledge Management System e si riferisce a tutte le informazioni relative al servizio AWS Managed Services (AMS) per un cliente. AMS dispone di un'API SKMS per la ricerca di dati.

Argomenti

Che cos'è la gestione della conoscenza del servizio?

La gestione della conoscenza del servizio è l'archivio di tutte le informazioni sul tuo account AMS. Le informazioni su quanto segue sono ottenute dal sistema di gestione della conoscenza dei servizi AMS (SKMS), tramite l'API AMS SKMS o tramite la console AMS:

- VPCs
- Sottoreti gestite
- Stack e componenti dello stack, incluse EC2 istanze Amazon e altre risorse
- Immagini di macchine Amazon (AMIs)

Puoi utilizzare le informazioni dell'SKMS per comprendere l'infrastruttura in gestione e come input per la gestione delle modifiche e le richieste di assistenza per creare, modificare o rimuovere l'infrastruttura.

> **Note**
>
> Tutte le chiamate API AMS SKMS vengono registrate in. AWS CloudTrail

Accedi a SKMS tramite l'API AMS SKMS, che fornisce operazioni per la scoperta di informazioni su un ambiente (VPCs e sulle sottoreti) e sulle risorse applicative (stack, istanze Amazon e immagini di EC2 istanze AMIs) che possono essere distribuite lì.

VPCs e le immagini delle istanze vengono configurate in un account, con le autorizzazioni di accesso necessarie, durante l'onboarding. Una volta stabilite, è possibile utilizzare il sistema di gestione delle modifiche per riempirle con stack funzionanti. VPCs

Trovare un VPC IDs in AMS

Un cloud privato virtuale (VPC) ha una o più sottoreti. In AMS il tuo VPC si trova in un Regione AWS e hai sottoreti private e pubbliche.

Consulta anche Trovare una sottorete IDs in AMS.

Alcuni richiedono CTs il. VpcId Per trovare un ID VPC, puoi utilizzare la console AMS o l'API/CLI.

Console AMS:

Nel pannello di navigazione, seleziona VPCse il VPC pertinente. Si apre la pagina dei dettagli del VPC per il VPC selezionato con informazioni tra cui l'ID VPC.

API ListVpcSummaries o CLI AMS SKMS:

> **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.

1. Negli esempi seguenti, il primo comando richiede un elenco di riepiloghi per tutti gli VPCs elementi dell'account. Il secondo comando richiede l'elenco di VPCs, con un filtro di query per elencare solo quelli VPCs creati nel 2016 e restituisce i valori CreatedTime VpcId, e Name.

   > **Note**
   >
   > È possibile ottenere l'AMS SKMS CLI tramite la pagina Risorse per sviluppatori nella console AMS.

   ```
   aws amsskms list-vpc-summaries --output table
   ```

   ```
   ----------------------------------------------------
   |                ListVPCSummaries                  |
   +--------------------------------------------------+
   |                 VPCSummaries                     |
   |+-----------------+--------------------------------|
   |   CreatedTime     |   2016-01-15T18:50:11Z       |
   |   VpcId           |   vpc-01234567890abcdef      |
   |   LastModifiedTime|   2016-01-15T18:50:11Z       |
   |   Name            |   952444781316-initial-vpc   |
   |+-----------------+--------------------------------|
   |                  Visibility                      |
   ```

```
|+------------------+-------------------------------|
|   Id             |  PrivateAndPublic             |
|   Name           |  PrivateAndPublic             |
|+------------------+-------------------------------|
```

2. Questa volta con una domanda:

```
aws amsskms list-VPC-summaries --query "VPCSummaries[?
starts_with(@.CreatedTime,to_string(`2016`))].[CreatedTime, VpcId, Name]" --output
 table
```

```
-------------------------------------------------------------------------
|                              ListVPCSummaries                         |
+---------------------+-----------------------+--------------------------+
|2016-01-15T18:50:11Z | vpc-01234567890abcdef | 952444781316-initial-VPC |
+---------------------+-----------------------+--------------------------+
```

Trovare una sottorete IDs in AMS

Diverse risorse richiedono che tu specifichi una sottorete, o un elenco di sottoreti, al momento della configurazione. Per trovare le sottoreti, è possibile utilizzare la console AMS oppure AMS SKMS API/CLI. Note that the AMS SKMS API/CLI è privato e deve essere installato prima di poterlo utilizzare.

Console AMS:

1. Nel riquadro di navigazione, seleziona VPCse il VPC pertinente. La pagina dei dettagli del VPC per il VPC selezionato si apre con una tabella di sottoreti, fai clic su un ID di sottorete per aprire la pagina dei dettagli e trovare l'ID.

API ListSubnetSummaries o CLI AMS SKMS:

> **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 trovare le sottoreti per il tuo VPC, puoi cercare con il `list-subnet-summaries` comando come mostrato.

> **Note**
>
> Se stai cercando sottoreti che non si trovano in un account AMS, puoi provare. `aws ec2 describe-subnets --region us-west-2`

1. L'operazione SKMS: API/CLI ListSubnetSummaries

   Un elenco semplice:

   ```
   aws amsskms list-subnet-summaries
   ```

   Uscita su una tabella:

   ```
   aws amsskms list-subnet-summaries --output table
   ```

2. L' ListSubnetSummaries operazione dell'API SKMS dispone di parametri per restringere i risultati in base alla visibilità. Inoltre, puoi filtrare i risultati in base al nome. Se utilizzi la CLI, puoi anche utilizzare l'`--query`opzione per restringere l'output o cercare una parte di un valore. Ad esempio, per trovare tutte le sottoreti di un particolare VPC, puoi usare questo comando:

```
aws amsskms list-subnet-summaries --query
 "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

Il che restituisce qualcosa del genere:

```
-------------------------------------------------------------------
|                   ListSubnetSummaries                           |
+---------+------------         -------+---------------------------+
|  Private|  subnet-01234567890abcdef  |  Demo Deployment Zone #1  |
|  Private|  subnet-01234567890abcdef  |  Demo Deployment Zone #1  |
|  Public |  subnet-01234567890abcdef  |  Demo DMZ #1              |
|  Public |  subnet-01234567890abcdef  |  Demo DMZ #1              |
+---------+----------         ---------+---------------------------+
```

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

3. Se ne hai più VPCs, includi un filtro VPC nel comando, quindi esegui il comando per ogni VPC. Ad esempio:

```
list-subnet-summaries --filter Attribute=VpcId,Value=vpc-xxxxxxxx --query
 "SubnetSummaries.sort_by(@,&Visibility.Name)[].[Visibility.Name,SubnetId,Name]" --
output table
```

4. In AWS, usa describe-subnet.

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

Nomi di sottorete

Le sottoreti AMS vengono create automaticamente dopo che l'input è stato raccolto dall'utente e aggiunto al sistema. AMS utilizza una formula per creare i nomi delle sottoreti: A *`ACCOUNT_ID`* - -. *`SUBNET-TYPE AZ-IDENTIFIER`* Il tipo di sottorete potrebbe essere `dmz`shared-services, o. `customer-application` Se si dispone di più di una sottorete relativa all'applicazione cliente, è possibile aggiungere un identificatore opzionale al nome della sottorete, dopo l'ID dell'account, per indicare che la sottorete è una sottorete «aggiuntiva» o «riservata».

Trova AMI IDs, AMS

Un'Amazon Machine Image, o AMI, è un modello per EC2 istanze Amazon, creato da un' EC2 istanza Amazon. AWS fornisce aggiornamenti AMIs (con patch, ad esempio) ogni mese; tuttavia, AWS Managed Services (AMS) richiede AMIs che siano stati modificati per l'uso con AMS. AMS ne rilascia di nuovi AMIs che puoi utilizzare subito dopo Patch Tuesday ogni mese.

Amazon Machine Images (AMIs) sono modelli di configurazione delle istanze utilizzati per creare EC2 istanze in AWS. AMS richiede che lo specifico AMIs venga utilizzato per le risorse gestite da AMS. I tipi di modifica per la creazione di EC2 istanze e i gruppi di EC2 Auto Scaling richiedono la specificazione di un AMI per AMS da utilizzare come base per le istanze create dal tipo di modifica. AMS consiglia di selezionare sempre l'AMI più recente disponibile.

Per ulteriori informazioni AWS AMIs, consulta AWS AMI Design.

Quando crei uno EC2 stack Amazon o un gruppo Amazon EC2 Auto Scaling per il tuo account AMS, devi specificare un AMI tramite. AmiId Sei limitato a AMIs iniziare con «cliente-» e ti consigliamo di scegliere sempre l'AMI più recente.

Per trovare l'AMI più recente per il tuo account, puoi cercare con un comando CLI AMS SKMS o utilizzare la pagina dei dettagli della console AMS per il VPC pertinente:

- Usa la console AMS: AMIs le opzioni disponibili sono elencate nella pagina AMI della console AMS. Seleziona tra AMIs i nomi che iniziano con «customer-».
- Usa l' API/CLI ListAmis operazione AMS SKMS.

> **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`

Ecco un esempio di CLI con un'`query`opzione che limita i risultati al cliente: AMIs

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?
starts_with(Name,'customer')].[Name,AmiId]" --output table
```

Questo esempio utilizza l'`filter`opzione con l'`query`opzione per trovare Windows AMIs che inizia con «cliente»:

```
aws amsskms list-amis --vpc-id VPC_ID --query "Amis.sort_by(@,&Name)[?
starts_with(Name,'customer')].[Name,AmiId]" --filter Attribute=Platform,Value=windows
 --output table
```

- 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

Trova gruppo di sicurezza (SG) IDs, AMS

Amazon EC2 crea e OpenSearch crea un dominio CTs richiede un ID del gruppo di sicurezza. Questo sarà nel modulo`sg-02ce123456e7893c7`. Il tuo account ha almeno due gruppi di sicurezza predefiniti; vediGruppi di sicurezza. Inoltre, è possibile che esistano gruppi di sicurezza creati per scopi specifici. Per scoprire i tuoi gruppi di sicurezza:

- Console AWS: utilizza la console EC2 o VPC per visualizzare tutti i gruppi di sicurezza per il VPC selezionato.
- API/CLI (quando accedi al tuo account AMS):

  Elenca i tuoi gruppi di sicurezza:

```
aws ec2 describe-security-groups
```

Trova entità IAM in AMS

Il tuo account ha i ruoli e le politiche IAM predefiniti; vedi Ruolo utente IAM in AMS e i profili di istanza IAM predefiniti; vedi EC2 Profilo dell'istanza IAM con le policy predefinite. Per scoprire i tuoi ruoli e le tue policy IAM:

- Console: utilizza la console IAM per visualizzare tutte le policy e i ruoli IAM per il tuo account.
- API/CLI (quando accedi al tuo account 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`

Elenca i tuoi ruoli:

```
aws --profile saml iam list-roles
```

Elenca le tue politiche:

```
aws --profile saml iam list-role-policies --role-name ROLE_NAME
```

Trova lo stack IDs in AMS

Per trovare uno Stack ID, puoi utilizzare la EC2 console Amazon, la console AMS o l'API/CLI AMS SKMS.

Console AMS:

- Nel riquadro di navigazione RFCs, seleziona e fai clic sulla RFC che ha creato lo stack. Utilizzate l'opzione di filtro in alto per ridurre l'elenco. Si apre la pagina dei dettagli RFC che include l'output di esecuzione con l'ID dello stack.
- In alternativa, puoi selezionare Stacks nel pannello di navigazione per aprire la pagina con l'elenco degli stack, quindi sfogliare l'elenco degli stack fino allo stack che ti interessa. Questo metodo è più utile se conosci l'oggetto dello stack che stai cercando.

EC2 Console Amazon:

Nel riquadro di navigazione, seleziona Istanze o Load Balancer o Auto Scaling Groups.

API ListStackSummaries o CLI AMS SKMS:

> **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 visualizzare un elenco di pile nell'account corrente, esegui l' ListStackSummaries operazione dell'API SKMS (CLI:). `list-stack-summaries` Per ottenere informazioni complete su una particolare istanza dello stack, by, run. StackId GetStack

- Negli esempi seguenti, il primo comando richiede un elenco di riepiloghi per tutte le istanze dello stack dell'account. Il secondo comando richiede l'elenco delle istanze dello stack, con un filtro di query per elencare solo quelle di un modello di stack specifico e restituisce i valori, Name e. VpcId StackId

```
aws amsskms list-stack-summaries --output table
```

```
-------------------------------------------------------------------
|                          ListStackSummaries                     |
```

```
|                                  StackSummaries                |
+------------+----------------------+--------------------+--------+
|   VpcId    |         StackId      |  StackTemplateId   |  Name  |
+------------+----------------------+--------------------+--------+
|vpc-0123abcd|stack-1fb7fe2212345678|stm-sdhopvbb123456789|Test ELB|
|vpc-0123abcd|stack-8323cc0e12345678|stm-s2b72beb123456789|S3 store|
|vpc-0123abcd|stack-2309fa0712345678|stm-sdhopvbb123456789|ELB     |
|vpc-0123abcd|stack-5e61a70512345678|stm-sdpabqbb123456789|PatchSim|
|vpc-0123abcd|stack-bd0e080d12345678|stm-s2b72beb123456789|CLI demo|
+------------+----------------------+--------------------+--------+
```

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

> **Note**
>
> Per informazioni sull'utilizzo dell'istanza IDs per l'accesso, vedi anche. Accesso alle istanze tramite bastioni

Trova istanze IDs o indirizzi IP in AMS

- 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"
    }
```

```
}
```

Trova Amazon Resource Names (ARNs) in AMS

Un Amazon Resource Name (ARN) è una stringa che identifica in modo univoco una AWS risorsa, come EC2 istanze, bucket S3, account, funzioni Lambda e così via. AWS richiede un ARN quando si desidera specificare una risorsa in modo inequivocabile per tutti AWS, ad esempio nelle policy IAM, nei tag Amazon Relational Database Service (Amazon RDS) e nelle chiamate API. ARNs sono costituiti da identificatori che specificano il servizio, la regione, l'account e altre informazioni. Esistono tre formati ARN:

```
arn:aws:service:region:account-id:resource-id
arn:aws:service:region:account-id:resource-type/resource-id
arn:aws:service:region:account-id:resource-type:resource-id
```

> **Note**
>
> Il formato esatto di un ARN dipende dal servizio e dal tipo di risorsa. Per ulteriori informazioni ARNs, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces and ARN Formats.
> Per esempi di formato ARN suddivisi per risorsa, vedere la tabella dei tipi di risorse del AWS Service Authorization Reference.

Trovare l'ARN di un oggetto AWS può essere difficile. Ecco tre modi per provare:

- Console di servizio AWS: accedi alla console di servizio AWS pertinente, individua la risorsa e trova l'ARN nei dettagli della risorsa.
- AWS API/CLI (devi prima installare l'AWS CLI): cerca il servizio pertinente nell'AWS CLI Command Reference, quindi, a seconda del servizio AWS, cerca l'operazione pertinente, ad esempio `describe`get, or e così via. Ad esempio, per tutti i ruoli, le policy e gli utenti IAM, puoi ottenere l'ARN nell'output della CLI con:

  ```
  aws iam get-role --role-name EMR_DefaultRole
  ```

- Costruisci l'ARN in base al formato pertinente: trova il formato ARN per la risorsa, esaminando la pagina Azioni, risorse e chiavi di condizione per i servizi AWS, trova il servizio pertinente, quindi

l'azione pertinente e approfondisci il formato ARN della risorsa. Una volta ottenuto il formato, sostituisci le variabili con le impostazioni pertinenti.

Puoi creare tu stesso l'ARN seguendo il formato appropriato (i formati cambiano in base al servizio e al tipo di risorsa) e inserendo le informazioni. Ecco alcuni esempi di ARN:

- Un Account AWS ARN ha la seguente sintassi:

```
arn:aws:iam::ACCOUNT-ID:root
```

- Un ARN S3 ha una gerarchia piatta di bucket e oggetti associati:

```
arn:aws:s3:::ams-bucket
```

- Un EC2 ARN ha sotto-tipi di risorse come immagini, gruppi di sicurezza, istanze e così via. Questo esempio include l'ID dell'istanza alla fine:

```
arn:aws:ec2:us-east-1:123456789012:instance/i-012abcd34efghi56
```

- Un ARN Lambda ha il nome della funzione per la parte resource-id e potrebbe essere necessario includere il numero di versione alla fine, come mostrato in questo esempio:

```
arn:aws:lambda:us-east-1:123456789012:function:api-function:1
```

Il AWS Key Management Service servizio fornisce queste informazioni: Individuazione dell'ID della chiave e dell'ARN della chiave.

Per trovare l'ARN di una tabella DynamoDB, usa la CLI di descrizione della tabella di descrizione di DynamoDB.

Per una scoperta da non addetti ai lavori AWS ARNs, consulta AWS ARN Explained: Amazon Resource Name Guide.

Trova risorse tramite ARN in AMS

Amazon Resource Names (ARNs) identifica in modo univoco AWS le risorse. Per informazioni sui ARNs formati ARN, consulta Amazon Resource Names (ARNs) e AWS Service Namespaces e ARN Formats.

> **Note**
>
> Per ottenere dettagli su una risorsa dal relativo ARN, è necessario avere accesso all'account che ha creato la risorsa.

Non esiste un percorso diretto AWS per cercare tutti i dettagli delle risorse dall'ARN della risorsa, poiché i servizi hanno più tipi di risorse con varie informazioni correlate. Se disponi dell'ARN per una risorsa, puoi determinare:

- Il AWS servizio correlato (il terzo segmento ARN) indica quale console AWS guardare per trovare la risorsa
- L'ID della risorsa (il sesto o settimo segmento ARN) conferma che hai trovato la risorsa giusta

Oppure puoi cercare i comandi AWS CLI disponibili per quel servizio nel AWS CLI Command Reference per informazioni su come ottenere dettagli sulla risorsa.

Ad esempio, dal seguente ARN, è possibile determinare se il servizio è`lambda`, l'account è`123456789012`, il tipo di risorsa è `function` e il nome della funzione è. `TestFunction`

```
arn:aws:lambda:us-east-1:123456789012:function:TestFunction
```

Da qui, puoi consultare la documentazione AWS CLI per il servizio Lambda per scoprire come recuperare maggiori dettagli con vari comandi, come e. `get-function` `get-function-configuration`

Ad esempio, puoi usare i seguenti comandi per ottenere maggiori informazioni su una funzione Lambda se ne hai il nome o l'ARN:

```
aws lambda get-function-configuration --function-name TestFunction
```

```
aws lambda get-function-configuration --function-name arn:aws:lambda:us-
east-1:123456789012:function:TestFunction
```

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.

Gestione degli accessi in AMS

Scopri come accedere alle risorse usando SSH, o Remote Desktop Protocol (RDP), e come usare i bastioni.

Il sistema di gestione degli accessi AWS Managed Services (AMS) viene configurato durante l'onboarding. Solo gli utenti con il ruolo utente AMS IAM, federati tramite AMS, possono accedere alle risorse AMS nell'account.

Oltre alla fiducia federata, descritta di seguito, i gruppi di sicurezza AMS sono un elemento importante nell'accesso alle applicazioni pubbliche e private. Per informazioni sui gruppi di sicurezza AMS e su come modificarli, consultaGruppi di sicurezza.

Argomenti

Cos'è la gestione degli accessi?

La gestione degli accessi è il modo in cui AMS protegge le risorse consentendo solo l'accesso autorizzato e autenticato. AMS utilizza un ruolo utente e un profilo di istanza IAM predefiniti, oltre all'autenticazione a più fattori, ai gruppi di sicurezza, ai nomi dei bastioni compatibili con DNS e altro ancora per proteggere le tue risorse.

AMS si concentra su tre tipi di accesso che richiedono una gestione:

- Accesso alla console: sfruttando la federazione, gli utenti di Active Directory dell'account possono accedere alla console tramite Single Sign-On (SSO). Se hai configurato l'autenticazione a più fattori per questi account, puoi continuare a richiedere l'autenticazione a più fattori per accedere alla console.
- Accesso all'istanza con RDP o SSH: sfruttando un trust di Active Directory, gli utenti dell'Active Directory esistente dell'account possono richiedere l'accesso a un'istanza e quindi autenticarsi correttamente su un bastione e sull'istanza utilizzando le credenziali aziendali esistenti. Se

hai configurato l'autenticazione a più fattori per tali account, puoi continuare a richiedere l'autenticazione a più fattori per richiedere l'accesso a un'istanza. AMS utilizza una propria soluzione MFA per limitare l'accesso dei tecnici AMS alle istanze.

- Accesso alle applicazioni: varia in base al caso d'uso.

Argomenti

Perché e quando AMS accede al tuo account

AWS Managed Services (AMS) gestisce l'infrastruttura AWS e talvolta, per motivi specifici, gli operatori e gli amministratori AMS accedono al tuo account. Questi eventi di accesso sono documentati nei tuoi AWS CloudTrail (CloudTrail) log.

Nei seguenti argomenti vengono spiegati perché, quando e come AMS accede al tuo account.

Trigger di accesso all'account cliente AMS

L'attività di accesso all'account cliente AMS è determinata dai trigger. I fattori scatenanti oggi sono i AWS ticket creati nel nostro sistema di gestione dei problemi in risposta agli allarmi e agli eventi di Amazon CloudWatch (CloudWatch) e le segnalazioni di incidenti o le richieste di assistenza che invii. Per ogni accesso potrebbero essere eseguite più chiamate di servizio e attività a livello di host.

La giustificazione dell'accesso, i trigger e l'iniziatore del trigger sono elencati nella tabella seguente.

Trigger di accesso

Accesso	Iniziatore	Trigger
Applicazione di patch	AMBITI	Problema con la patch
Implementazioni dell'infrastruttura	AMS	Problema di distribuzione
Indagine interna sui problemi	ARMS	Problema (un problema che è stato identificato come sistemico)

Accesso	Iniziatore	Trigger
Indagine e risoluzione degli avvisi	AMS	Elementi di lavoro operativi (SSM OpsItems) di AWS Systems Manager
Esecuzione RFC manuale	Utente corrente	Problema relativo alla richiesta di modifica (RFC). (La modalità non automatizzata RFCs potrebbe richiedere l'accesso di AMS alle tue risorse)
Indagine e risoluzione degli incidenti	Utente corrente	Caso di assistenza in entrata (un incidente o una richiesta di assistenza inviata dall'utente)
Adempimento della richiesta di assistenza in entrata	Utente corrente	

Ruoli IAM di accesso all'account cliente AMS

Quando attivato, AMS accede agli account dei clienti utilizzando i ruoli AWS Identity and Access Management (IAM). Come tutte le attività del tuo account, i ruoli e il loro utilizzo vengono registrati. CloudTrail

> **Important**
>
> Non modificare o eliminare questi ruoli.

Ruoli IAM per l'accesso di AMS agli account dei clienti

Nome ruolo	Tipo di account (SALZ, MALZ Management, MALZ Application, ecc.)	Descrizione
ams-service-admin	SALZ, MALZ	Accesso automatizzato ai servizi AMS e implementazioni automatizzate dell'infrastruttura, ad esempio Patch, Backup, Riparazione automatica.
ams-application-infra-read-solo	SALZ, applicazione MALZ, applicazione MALZ Tools-Applicazione	Accesso in sola lettura da parte dell'operatore
ams-application-infra-operations		Accesso dell'operatore per incidents/service le richieste
ams-application-infra-admin		Accesso ad Admin
ams-primary-read-only	Gestione MALZ	Accesso in sola lettura da parte dell'operatore
ams-primary-operations		Accesso dell'operatore per incidents/service le richieste
ams-primary-admin		Accesso ad Admin
ams-logging-read-only	Registrazione MALZ	Accesso in sola lettura da parte dell'operatore
ams-logging-operations		Accesso dell'operatore per incidents/service le richieste
ams-logging-admin		Accesso ad Admin
ams-networking-read-only	Rete MALZ	Accesso in sola lettura da parte dell'operatore
ams-networking-operations		Accesso dell'operatore per incidents/service le richieste

Nome ruolo	Tipo di account (SALZ, MALZ Management, MALZ Applicati on, ecc.)	Descrizione
ams-networking-admin		Accesso ad Admin
ams-shared-services-read-solo	Servizi condivisi MALZ	Accesso in sola lettura da parte dell'operatore
ams-shared-services-operations		Accesso dell'operatore per incidents/service le richieste
ams-shared-services-admin		Accesso ad Admin
ams-security-read-only	Sicurezza MALZ	Accesso in sola lettura da parte dell'operatore
ams-security-operations		Accesso dell'operatore per incidents/service le richieste
ams-security-admin		Accesso ad Admin
ams-access-security-analyst	SALZ, applicazi one MALZ, applicazione MALZ Tools, MALZ Core	Accesso di sicurezza AMS
ams-access-security-analyst-sola lettura		AMS Security, accesso in sola lettura
Sentinel_ _Ruolo_ 0 MBhe AdminUser PXHaz RQadu PVc CDc	SALZ	[BreakGlassRole] Utilizzato per inserire BreakGlass negli account dei clienti
PowerUserSentinel_ _Ruolo_ S0 0 wZuPu ROOl lazDb RI9	SALE, MALZ	Accesso Poweruser agli account dei clienti per l'esecuzione di RFC

Nome ruolo	Tipo di account (SALZ, MALZ Management, MALZ Application, ecc.)	Descrizione
Sentinel_ _Role_PD4L6RW9RD0LNLKD5 ReadOnlyUser JOo		ReadOnly accesso agli account dei clienti per l'esecuzione di RFC
ams_admin_role		Accesso amministrativo agli account dei clienti per l'esecuzione di RFC
AWSManagedServices_Provisioning_CustomerStacksRole		Utilizzato per avviare e aggiornare gli stack CFN per conto dei clienti tramite Ingest CloudFormation
customer_ssm_automation_role		Ruolo passato dalle esecuzioni CT a SSM Automation per l'esecuzione dei runbook
ams_ssm_automation_role	SALZ, applicazione MALZ, codice MALZ	Ruolo passato dai servizi AMS a SSM Automation per l'esecuzione dei runbook
ams_ssm_iam_deployment_role	Applicazione MALZ	Ruolo utilizzato dal catalogo IAM
ams_ssm_shared_svcs_intermediary_role	Servizi condivisi MALZ	Ruolo utilizzato dall'applicazione ams_ssm_automation_role per eseguire documenti SSM specifici nell'account Shared Services
AmsOpsCenterRole	SALZ, MALZ	Utilizzato per creare e aggiornare gli account dei OpsItems clienti
AMSOpsItemAutoExecutionRole		Utilizzato per ottenere documenti SSM, descrivere i tag delle risorse OpsItems, aggiornare e avviare l'automazione

Nome ruolo	Tipo di account (SALZ, MALZ Management, MALZ Application, ecc.)	Descrizione
customer-mc-ecProfilo a 2 istanze		Profilo predefinito dell' EC2 istanza del cliente (ruolo)

Richiesta dell'accesso all'istanza

Per accedere a una risorsa, devi prima inviare una richiesta di modifica (RFC) per tale accesso. È possibile richiedere due tipi di accesso: amministratore (autorizzazioni di lettura/scrittura) e sola lettura (accesso utente standard). Per impostazione predefinita, l'accesso dura otto ore. Queste informazioni sono obbligatorie:

- Stack ID, o set di stack IDs, per l'istanza o le istanze a cui desideri accedere.
- Il nome di dominio completo del tuo dominio affidabile AMS.
- Il nome utente di Active Directory della persona che desidera accedere.
- L'ID del VPC in cui si trovano gli stack a cui desideri accedere.

Una volta ottenuto l'accesso, puoi aggiornare la richiesta in base alle tue esigenze.

Per esempi di come richiedere l'accesso, vedi Stack Admin Access | Grant o Stack Read-only Access | Grant.

Come e quando usare l'account utente root in AMS

L'utente root è il superutente del tuo AWS account. AMS monitora l'utilizzo dei root. Ti consigliamo di utilizzare root solo per le poche attività che lo richiedono, ad esempio: modifica delle impostazioni dell'account, attivazione dell'accesso AWS Identity and Access Management (IAM) alla fatturazione e alla gestione dei costi, modifica della password root e abilitazione dell'autenticazione a più fattori (MFA). Vedi Attività che richiedono credenziali utente root nella Guida per l'utente.AWS Identity and Access Management

> **Note**
>
> L'MFA è abilitata durante l'onboarding di AMS Advanced per impedire specificamente l'accesso degli utenti root. L'accesso root negli account gestiti da AMS è diverso dagli altri AWS account ed è fondamentale per la sicurezza dell'intero ambiente gestito da AMS. La MFA configurata è una MFA virtuale e viene eseguita utilizzando un dispositivo di proprietà di AMS. Dopo aver configurato la MFA virtuale con l'assistenza di AMS, il token virtuale viene immediatamente eliminato. Ciò garantisce che né tu né AMS conserviate la possibilità di accedere all'account come utente root. L'accesso root può essere riattivato solo su richieste speciali (spiegate di seguito) e AMS prevede che tali accessi vengano utilizzati solo quando assolutamente necessario. Per informazioni sulla MFA, consulta Secure New Account with Multi-Factor Authentication.

L'accesso root attiva sempre una risposta del team AMS Security and Operations. AMS monitora le chiamate API per l'accesso root e gli allarmi vengono attivati se viene rilevato tale accesso.

La richiesta dell'accesso root è leggermente diversa tra i tipi di account AMS.

Accesso root con landing zone con account singolo AMS Advanced:

Se disponi di una landing zone con un solo account, contatta il tuo cloud service delivery manager (CSDM) e gli architetti cloud (CAs) per consigliarli sulle operazioni di accesso root necessarie. È meglio dare un preavviso di ventiquattro ore prima dell'attività proposta.

Accesso root con landing zone multi-account AMS Advanced:

Per gli account di applicazione, Shared Services, Security o Networking zone con più account, usa il tipo di modifica Gestione | Altro | Altro (ct-1e1xtak34nx76). Includi la data, l'ora e lo scopo dell'utilizzo delle credenziali dell'utente root e pianifica la RFC per assicurarti di dare un preavviso di ventiquattro ore prima dell'attività proposta. Usa il tuo account di gestione delle landing zone multi-account per inviare la RFC.

Inoltre, contattate il vostro CSDM con CAs ventiquattro ore di anticipo per informarlo sulle operazioni di accesso root necessarie.

Operazioni AMS e risposta di sicurezza all'utilizzo del root:

AMS riceve un allarme quando viene utilizzato l'account utente root. Se l'utilizzo delle credenziali root non è pianificato, contatta il team di sicurezza AMS e il team dell'account per verificare se si tratta di

un'attività prevista. Se non si tratta di un'attività prevista, AMS collabora con il team di sicurezza per esaminare il problema.

Console AMS Advanced e EC2 accesso Amazon

Accesso alla console AMS Advanced.

Accesso alle tue EC2 istanze Amazon.

Invia una richiesta di accesso:

Accesso alle tue EC2 istanze AMS Amazon:

Accesso alla console AWS di gestione e alla console AMS

Durante l'onboarding, ti viene fornito un accesso alla console di AWS gestione (con privilegi limitati: puoi scrivere sulla console AMS e su alcuni campi nella pagina delle informazioni sui clienti). È possibile accedere alla console AMS selezionando il collegamento Managed Services nella console di AWS gestione. L'accesso federato o le credenziali condivise (nome utente/password) vengono preparate come concordato con il team di amministrazione IT. Per un'ulteriore creazione di account o gruppi, invia una richiesta di servizio ad AMS.

Per informazioni su come accedere alla console di AWS gestione, consulta Utilizzo della console di AWS gestione.

Per alcuni suggerimenti sull'uso della console AMS, consulta Uso della console AMS.

Accesso temporaneo alla console AMS

Se non hai ancora configurato un provider di identità (ad esempio SAML) per l'autenticazione su AMS, puoi ottenere l'accesso temporaneo alla console AMS. Contattate il vostro CSDM per richiedere una richiesta di modifica dell'entità o della politica (ct-3dpd8mdd9jn1r) per vostro conto con questi valori:

- UserName: Un nome per l'entità utente IAM che stai creando

- AccessType: «Accesso alla console»
- UserPermissions: «Accesso temporaneo alla console AMS per *USERNAME* (la persona a cui desideri avere accesso temporaneo)»
- Notifiche e-mail: il tuo indirizzo e-mail, in modo da poter approvare la richiesta quando AMS te lo richiede

> **Note**
>
> Questa RFC per l'accesso temporaneo alla console AMS richiede una revisione e un'accettazione di sicurezza da parte del team di sicurezza interno e di AMS Global Security.

Dopo aver completato questa richiesta e aver potuto accedere, devi approvare la RFC che è stata creata, per tenere traccia dell'approvazione e consentire al team AMS di concludere il lavoro. Per approvare la RFC, trovala nella pagina dell'elenco della RFC (accanto ad essa sarà presente un contrassegno di approvazione in sospeso), selezionala per aprire la pagina dei dettagli RFC relativa a quella RFC, quindi scegli Approva. Tieni presente che non potrai utilizzare AMS finché la RFC non sarà approvata.

Quando la RFC viene completata con successo, AMS operations ti fornisce il nuovo utente IAM e una password. Quindi segui questi passaggi:

1. Vai alla console di AWS gestione e accedi con le credenziali fornite. Ti verrà chiesto di creare una nuova password. Al momento dell'accesso è inoltre necessario impostare l'autenticazione a più fattori (MFA); per ulteriori informazioni, consulta Using Multi-Factor Authentication (MFA) in. AWS
2. Nella console di AWS gestione, passa al ruolo IAM fornito (). `customer_CustomerCode_readonly_user_role`
3. Apri la console AMS Managed Services.

> **Note**
>
> L'accesso temporaneo è predefinito a sessanta giorni; tuttavia, puoi richiedere un'estensione di trenta giorni contattando il tuo CSDM.

Accesso alle istanze tramite bastioni

Tutti gli accessi alle risorse all'interno degli account gestiti da AMS, sia per i clienti che per gli operatori AMS, sono limitati dall'uso di host bastion. Gestiamo i bastioni RDP Linux e Windows per l'accesso agli account AMS Advanced sia per Multi-account landing zone (MALZ) che per Single Account Landing Zone (SALZ).

I tuoi bastioni sono accessibili solo tramite la tua connessione privata (VPN o) DX. Direct Connect Oltre ai firewall per prevenire il traffico in entrata, i bastioni vengono riforniti regolarmente (con le credenziali esistenti) secondo una pianificazione prestabilita.

> **Note**
>
> Per informazioni sullo spostamento di file su un' EC2 istanza, consulta Trasferimento di file: PC Windows o MAC locale su Amazon Linux EC2.

MALZ

Puoi accedere alle istanze del tuo account accedendo a un'istanza bastion con le tue credenziali Active Directory (AD). Amazon utilizza bastioni situati nella rete perimetrale VPC (account di rete) e tu usi i bastioni dei tuoi clienti, situati nella sottorete Customer Bastions nell'account di servizi condivisi.

Quando il tuo ambiente AMS è inizialmente integrato, hai due bastioni SSH e due bastioni RDP a seconda della tua scelta.

SALZ

Puoi accedere alle istanze del tuo account accedendo a un'istanza bastion con le tue credenziali di Active Directory (AD). AMS utilizza bastioni situati nelle sottoreti della rete perimetrale e tu usi bastioni situati nelle tue sottoreti private.

Quando il tuo account è inizialmente registrato, hai due bastioni RDP e due SSH, per impostazione predefinita.

> **Note**
>
> Come parte della landing zone con account singolo, AMS fornisce bastioni RDP (Windows) e SSH (Linux) per accedere ai tuoi stack; tuttavia, puoi scegliere se desideri

solo bastioni RDP o solo bastioni SSH. Per richiedere che vengano mantenuti solo i bastioni RDP o solo i bastioni SSH, invia una richiesta di servizio.

Per accedere a un'istanza, è necessario:

- Accesso concesso allo stack. Per ottenere l'accesso a uno stack, vedi Stack Admin Access | Grant o Stack Read-Only Access | Grant.
- L'ID dello stack a cui desideri accedere per ottenere l'accesso all'istanza. Per trovare un ID dello stack, consulta. Trova lo stack IDs in AMS
- L'IP dell'istanza a cui desideri accedere. Per trovare l'IP di un'istanza, consultaTrova istanze IDs o indirizzi IP in AMS.
- Il nome del bastione adatto al DNS o l'IP del bastione. Di seguito vengono descritti come utilizzare nomi di bastione compatibili con DNS e come trovare un IP bastione.

Nomi bastioni compatibili con DNS

AWS Managed Services (AMS) utilizza nomi di 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)`*`.A`*`AccountNumber`*`.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)`*`.A`*`ACCOUNT_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`

Riduzione dei costi sui bastioni della single-account landing zone (SALZ)

AMS fornisce due bastioni SSH e due bastioni RDP nella configurazione predefinita per consentirti di connetterti alle tue EC2 istanze Amazon e implementa anche due bastioni DMZ nella configurazione predefinita per le operazioni di servizio. Per impostazione predefinita, i bastioni utilizzano EC2 istanze Amazon di dimensioni m4. Hai la possibilità di modificare le EC2 istanze Amazon utilizzate per bastions in t3.small e risparmiare sui costi.

Se utilizzi istanze on demand, istanze spot o un piano di risparmio, dovresti prendere in considerazione questa funzionalità e risparmiare sui costi. Se utilizzi istanze riservate, valuta se l'utilizzo di istanze t3.small potrebbe ridurre i costi. Per cambiare il tipo di istanza, invia una RFC con Management | Advanced stack components | EC2 instance stack | Resize (ct-15mazjj88xc69) CT dal tuo account AMS.

Contatta il tuo cloud service delivery manager (CSDM) per ulteriori domande o per verificare se puoi trarre vantaggio da questa funzionalità.

Utilizzo degli indirizzi IP 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.

Esempi di accesso alle istanze in AMS

Questi esempi mostrano come accedere a un'istanza nel tuo account AMS utilizzando un bastion dopo aver ottenuto l'accesso tramite un RFC. Per informazioni su come ottenere l'accesso concesso, consulta. Richiesta dell'accesso all'istanza

> **Note**
>
> Per informazioni sullo spostamento di file su un' EC2 istanza, consulta Trasferimento di file: PC Windows o MAC locale su Amazon Linux EC2.

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. Utilizzo degli indirizzi IP bastion

  > **Note**
  >
  > Un' EC2 istanza Amazon creata tramite un gruppo Amazon EC2 Auto Scaling avrà un indirizzo IP che si accende e si chiude ciclicamente e dovrai usare la tua EC2 console Amazon per trovare quell'indirizzo IP.

- Nome utente (ad esempio*DOMAIN_FQDN**USERNAME*) e password: credenziali per l'account. *USERNAME*Deve essere il tuo nome utente di Active Directory.

  Tieni presente che è possibile utilizzare un nome utente nel formato username@customerdomain.com, ma può causare problemi con la configurazione del PBIS.

- Indirizzo IP dello stack: puoi trovarlo esaminando l'output di esecuzione per la RFC che hai inviato per avviare lo stack o cerca l'indirizzo IP dell' EC2 istanza Amazon nella console Amazon. EC2 Per una singola EC2 istanza Amazon, puoi anche utilizzare il comando AMS SKMS ListStackSummaries per trovare l'ID dello stack e quindi GetStack trovare l'indirizzo IP dello stack. Per il riferimento all'API AMS SKMS, consulta la scheda Report nella console AWS Artifact.

Accedi all'indirizzo IP del bastione, SSH o RDP, a seconda dei casi, e accedi utilizzando una delle seguenti procedure.

> **Note**
>
> I bastioni RDP consentono solo due connessioni simultanee. Quindi, nel migliore dei casi, solo 4 amministratori sono in grado di connettersi agli stack di Windows contemporaneamente. Se hai bisogno di più connessioni per RDP, consulta AMS Bastion Options durante le migrazioni e l'onboarding delle applicazioni nella guida all'onboarding di AMS.

Da computer Linux a istanza Linux

Usa SSH per connetterti al bastione SSH e quindi 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 su 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
```

Controllo degli accessi basato sul team o sul ruolo in un account AMS

Scenario: due team applicativi A e B utilizzano un unico account AMS per le rispettive app «AA» e «BB», rispettivamente. Il team A desidera accedere solo alle risorse per l'app «AA» e il team B desidera accedere solo alle risorse per l'app «BB». Come posso configurarlo?

Usa gli strumenti del loro ITSM per implementare i controlli di accesso basati sul team (TBAC). Ad esempio, puoi utilizzare l'app AMS ServiceNow Connector per l'integrazione con AMS. APIs Contattate il vostro CSDM per una guida di alto livello su questa implementazione.

Configurazione automatica delle istanze in AMS Advanced

Il servizio di configurazione automatizzata delle istanze AMS Advanced viene eseguito quotidianamente e analizza e aggiorna automaticamente l'SSM, gli CloudWatch agenti e i file di configurazione sulle istanze gestite EC2 . Gli aggiornamenti si applicano, se necessario, a:

- SSM e agenti CloudWatch
- CloudWatch file di configurazione

Questi aggiornamenti consentono ad AMS di accedere alle EC2 istanze gestite da AMS e di configurarle in modo che emettano log e metriche appropriati.

Argomenti

Prerequisiti per la configurazione automatica delle istanze

Per i clienti AMS Advanced che distribuiscono istanze con Change Management, devono essere soddisfatti i seguenti prerequisiti:

- L'agente SSM è installato e in uno stato gestito.
- L'istanza è contrassegnata come istanza gestita. (Il `aws:cloudformation:stack-name` tag ha un valore che inizia con `stack- osc-`.)

Se l'agente SSM non è già installato sulla tua istanza, puoi installarlo utilizzando la funzione di installazione automatica dell'agente SSM di AMS. Per ulteriori informazioni, consulta Installazione automatica di SSM Agent.

In alternativa, puoi installare l'agente SSM manualmente. Per ulteriori informazioni, consulta gli argomenti seguenti:

- Linux: installa manualmente l'agente SSM su EC2 istanze per Linux - AWS Systems Manager

- Windows: installa manualmente l'agente SSM su EC2 istanze per Windows Server - AWS Systems Manager

Per ulteriori informazioni sull'agente SSM, consulta la documentazione AWS Working with SSM Agent.

Installazione automatica di SSM Agent

Per fare in modo che AMS gestisca le tue istanze Amazon Elastic Compute Cloud (Amazon EC2), devi installare AWS Systems Manager SSM Agent su ciascuna istanza. Se sulle istanze non è installato SSM Agent, puoi utilizzare la funzionalità di installazione automatica di AMS SSM Agent.

> **Note**
>
> - Questa funzionalità è disponibile solo per EC2 le istanze che non fanno parte di un gruppo Auto Scaling e che eseguono sistemi operativi Linux supportati da AMS.
> - La funzionalità di installazione automatica dell'agente AMS SSM è disattivata per impostazione predefinita. Per abilitarla, contatta la tua CA o il CSDM.

Prerequisiti per l'utilizzo di SSM Agent

- Assicurati che il profilo di istanza associato alle istanze di destinazione abbia una delle seguenti politiche (o autorizzazioni equivalenti a quelle consentite in esse):
  - Amazon SSMManaged EC2 InstanceDefaultPolicy
  - Amazon SSMManaged InstanceCore
- Assicurati che non esista una Service Control Policy al AWS Organizations livello che neghi esplicitamente le autorizzazioni elencate nelle politiche precedenti.

  Per ulteriori informazioni, consulta la pagina Configurazione delle autorizzazioni dell'istanza richieste per Systems Manager.
- Per bloccare il traffico in uscita, assicurati che i seguenti endpoint di interfaccia siano abilitati sul VPC in cui risiedono le istanze di destinazione (sostituisci «regione» nell'URL in modo appropriato):
  - ssm.<regione>.amazonaws.com
  - ssmmessages.<regione>.amazonaws.com

- messaggi ec2. <region>.amazonaws.com

Per ulteriori informazioni, consulta Migliorare la sicurezza delle EC2 istanze utilizzando gli endpoint VPC per Systems Manager.

Per suggerimenti generali sull'attivazione o la risoluzione dei problemi relativi alla disponibilità dei nodi gestiti, consulta Soluzione 2: verifica che sia stato specificato un profilo di istanza IAM per l'istanza (solo istanze) EC2 .

> **Note**
>
> AMS arresta e avvia ogni istanza come parte del processo di installazione automatica. Quando un'istanza viene interrotta, i dati archiviati nei volumi di archiviazione delle istanze e i dati archiviati nella RAM vengono persi. Per ulteriori informazioni, consulta Cosa succede quando si interrompe un'istanza.

Richiedi l'installazione automatica di SSM Agent sulle tue istanze

Se i tuoi account sono registrati su AMS Accelerate Patch Add-On, configura una finestra di manutenzione delle patch (MW) per le istanze. È necessario un agente SSM funzionante per completare il processo di patch. Se l'agente SSM non è presente su un'istanza, AMS tenta di installarlo automaticamente durante la finestra di manutenzione della patch.

> **Note**
>
> AMS arresta e avvia ogni istanza come parte del processo di installazione automatica. Quando un'istanza viene interrotta, i dati archiviati nei volumi di archiviazione delle istanze e i dati archiviati nella RAM vengono persi. Per ulteriori informazioni, consulta Cosa succede quando si interrompe un'istanza.

Come funziona l'installazione automatica di SSM Agent

AMS utilizza i dati EC2 degli utenti per eseguire lo script di installazione sulle istanze. Per aggiungere lo script dei dati utente ed eseguirlo sulle istanze, AMS deve arrestare e avviare ogni istanza.

Se l'istanza ha già uno script di dati utente esistente, AMS completa i seguenti passaggi durante il processo di installazione automatica:

1. Crea un backup dello script di dati utente esistente.
2. Sostituisce lo script dei dati utente esistente con lo script di installazione di SSM Agent.
3. Riavvia l'istanza per installare SSM Agent.
4. Arresta l'istanza e ripristina lo script originale.
5. Riavvia l'istanza con lo script originale.

Modifiche automatiche

Il servizio di configurazione automatizzata delle istanze AMS Advanced apporta le modifiche necessarie alle EC2 istanze.

Cosa cambia:

- Aggiorna automaticamente il codice sulle istanze Linux
- Aggiorna automaticamente PBIS su istanze Linux
- Aggiorna automaticamente la versione minima di SSM e agenti CloudWatch
- CloudWatch file di configurazione, dettagli di aggiornamento
- Log configurati automaticamente

Aggiorna automaticamente il codice sulle istanze Linux

AMS aggiorna automaticamente il codice dell'istanza sulle istanze Linux. Questo aiuta a migliorare complessivamente la stabilità operativa e la sicurezza dei componenti e dell'ambiente AMS.

Domande frequenti:

Cosa è incluso nell'On Instance Code (OIC) su Linux?

> OIC include il pacchetto ams-toolkit insieme ad alcuni file di configurazione e cron job. AMS richiede questi file e pacchetti per l'integrazione (Active Directory e altre dipendenze). CloudFormation Preconfiguriamo questi file in formato AMS AMIs o li installiamo sull'istanza durante l'ingestione del carico di lavoro.

Quando AMS aggiornerà l'OIC?

AMS aggiorna OIC quando rilascia una nuova versione con correzioni di bug o altri miglioramenti. Il flusso di lavoro per verificare la versione e l'aggiornamento dell'OIC viene eseguito quotidianamente.

Aggiorna automaticamente PBIS su istanze Linux

AMS utilizza il modulo Power Broker Identity Service (PBIS) per unire le istanze Linux in Active Directory gestita da AMS.

AMS aggiorna automaticamente PBIS sulle istanze Linux.

Domande frequenti:

Quando AMS aggiornerà il PBIS?

AMS attiva l'aggiornamento PBIS al riavvio. Se è disponibile una nuova versione di PBIS, AMS tenta di installare la nuova versione al successivo riavvio dell'istanza.

L'aggiornamento PBIS può essere disattivato?

Puoi disattivare l'aggiornamento PBIS a livello di istanza o account:

- Livello di account: crea un parametro nell'archivio dei parametri SSM: Nome:`/ams/skip-pbis-update`, Valore: `true` (in ogni caso).

> **Note**
>
> Il profilo dell'istanza deve disporre delle autorizzazioni per leggere i parametri SSM. Se manca il flag, il comportamento predefinito consiste nell'eseguire l'aggiornamento.

- Livello di istanza:
  - Basato su tag: aggiungi il seguente tag all'istanza: Key:`skip_pbis_update`, Value: `true` (in ogni caso).
  - File di configurazione: aggiungi il seguente flag al `/opt/aws/ams/etc/ams.conf.d/state.ini` file: `skip_pbis_update = true.`

> **Note**
>
> Il tag ha una priorità più alta rispetto al parametro SSM. Puoi disattivare l'aggiornamento PBIS a livello di account tramite il parametro, ma attivarlo per una o più istanze aggiungendo un tag`Key:skip_pbis_update`,. `Value: false`

Per configurare una qualsiasi delle opzioni descritte, segui la procedura standard di gestione delle modifiche nel tuo ambiente AMS.

Aggiorna automaticamente la versione minima di SSM e agenti CloudWatch

La versione minima di AMS Advanced (dell'SSM o CloudWatch degli agenti) è la versione testata dal team di assistenza AMS e preapprovata per il sistema operativo in uso. Cerchiamo di rimanere proattivi e di utilizzare l'ultima versione stabile e compatibile, in modo che il numero di versione cambi nel tempo. Puoi trovare la versione minima attuale inviando una richiesta di servizio ad AMS.

- Gestione degli agenti SSM

  L'agente Amazon SSM è responsabile dell'esecuzione di comandi remoti sull'istanza. L'automazione della configurazione dell'istanza garantisce che l'agente SSM esegua la versione minima.
- Gestione degli agenti Cloudwatch

  L' CloudWatch agente Amazon è responsabile dell'emissione dei log e dei parametri del sistema operativo. La configurazione automatizzata dell'istanza esegue le seguenti operazioni:
  - Se necessario, disabilita il precedente CloudWatch Log Agent e migra la configurazione al nuovo agente unificato CloudWatch
  - Se sull'istanza è in esecuzione il precedente CloudWatch Log Agent, la configurazione automatizzata dell'istanza disabilita il servizio precedente di CloudWatch Log Agent e ne migra la configurazione all'agente unificato. CloudWatch
  - Personalizza la CloudWatch configurazione per emettere log e metriche appropriati.

  File e directory interessati:
  - Windows
    - %ProgramData%\ Amazon\AmazonCloudWatchAgent\
    - %ProgramData%\ Amazon\AmazonCloudWatchAgent\ Configs\

- Linux
  - /opt/aws/amazon-cloudwatch-agent/etc/
  - /-cloudwatch-agent.d/ opt/aws/amazon-cloudwatch-agent/etc/amazon
  - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json

CloudWatch file di configurazione, dettagli di aggiornamento

Leggiamo CloudWatch le configurazioni personalizzate (solo JSON) dalle seguenti CloudWatch directory (vedi directory consigliate) e le uniamo alla configurazione AMS standard: CloudWatch

- CloudWatch File
  - Nell'istanza:
    - Windows
      - %ProgramData%\ Amazon\AmazonCloudWatchAgent\ Configs\
      - %ProgramFiles%\\ ModulesWindowsPowerShell\ AWSManaged Services.Logging.Utilities\ Files\ Config.json
    - Linux
      - /opt/aws/ams/opt/aws/amazon-cloudwatch-agent/etc/amazon-cloudwatch-agent.json
  - Su Amazon S3:
    - Windows:
      - https://ams-configuration-artifacts- *REGION_NAME* .s3. *REGION_NAME*.amazonaws. com/ configurations/cloudwatch/latest/windows-cloudwatch-config.json
    - Linux:
      - https://- .s3. ams-configuration-artifacts *REGION_NAME* *REGION_NAME*.amazonaws. com/ configurations/cloudwatch/latest/linux-cloudwatch-config.json

Log configurati automaticamente

Configuriamo la tua istanza per scrivere i seguenti log.

- Windows:
  - SSMAgentRegistro Amazon
  - AmazonCloudWatchAgentLog

  - SSMErrorRegistro Amazon
  - AmazonCloudFormationLog
  - ApplicationEventLog
  - EC2ConfigServiceEventLog
  - MicrosoftWindowsAppLockerEXEAndDLLEventRegistro
  - MicrosoftWindowsAppLockerMSIAndScriptEventLog
  - MicrosoftWindowsGroupPolicyOperationalEventLog
  - SecurityEventLog
  - SystemEventLog
- Linux:
  - /var/log/amazon/ssm/amazon-ssm-agent.log
  - /var/log/amazon/ssm/errors.log
  - /.log var/log/audit/audit
  - /-init-output.log var/log/cloud
  - /var/log/cloud-init.log
  - /var/log/cron
  - /var/log/dpkg.log
  - /var/log/maillog
  - /var/log/messages
  - /var/log/secure
  - /var/log/spooler
  - /var/log/syslog
  - /.log var/log/yum
  - /.log var/log/zypper

Monitoraggio e gestione degli eventi in AMS

Argomenti

Il sistema di monitoraggio AWS Managed Services (AMS) monitora le risorse AMS per individuare guasti, peggioramento delle prestazioni e problemi di sicurezza. Il sistema di monitoraggio AMS si basa su servizi AWS come Amazon CloudWatch (CloudWatch), Amazon GuardDuty, Amazon Macie e. AWS Health Oltre al sistema di monitoraggio, AMS TrendMicro DeepSecurity implementa anche la protezione dal malware sulle istanze Amazon Elastic Compute Cloud (Amazon EC2), per informazioni sulle impostazioni predefinite di sicurezza degli endpoint (EPS), consulta. Sicurezza degli endpoint (EPS)

Il monitoraggio AMS offre i seguenti vantaggi:

- Una base di monitoraggio in modo da avere un livello di protezione predefinito anche se non configuri nessun altro monitoraggio per i tuoi account gestiti. Per informazioni, consulta Avvisi dal monitoraggio di base in AMS.
- Avvisi di indagine per determinare l'azione appropriata. Ad esempio, se GuardDuty rileva un'attività che indica tentativi di brute force su un' EC2 istanza Amazon, AMS analizza i log di flusso VPC per comprendere l'origine e il contesto dell'attività.

- Correzione degli avvisi, quando possibile, per prevenire o ridurre l'impatto sulle applicazioni. Ad esempio, se utilizzi un' EC2 istanza Amazon autonoma che non supera il controllo dello stato del sistema, AMS tenta di ripristinare l'istanza interrompendola e riavviandola. Per ulteriori informazioni, consulta Correzione automatica degli avvisi con AMS.
- Trasparenza sugli avvisi attivi e precedentemente risolti utilizzando. OpsCenter Ad esempio, se hai un utilizzo imprevisto elevato della CPU su un' EC2 istanza Amazon, puoi richiedere l'accesso alla console AWS Systems Manager (include l'accesso alla OpsCenter console) e visualizzarla OpsItem direttamente nella OpsCenter console.

Che cos'è il monitoraggio?

Il sistema di monitoraggio AMS monitora le AWS risorse per individuare guasti, peggioramento delle prestazioni e problemi di sicurezza. In qualità di account gestito, AMS configura e distribuisce allarmi per le AWS risorse applicabili, le monitora ed esegue le correzioni ove applicabile.

Il sistema di monitoraggio AMS genera avvisi in base alla configurazione di monitoraggio dell'account. La configurazione di monitoraggio di un account si riferisce a tutti i parametri delle risorse dell'account che creano un avviso; per informazioni sui parametri delle risorse, vedereAvvisi dal monitoraggio di base in AMS. La configurazione di monitoraggio di un account include le definizioni degli CloudWatch allarmi e le regole CloudWatch degli eventi che generano l'avviso (allarme o evento).

La configurazione di monitoraggio di base è l'insieme di definizioni di allarme (Avvisi dal monitoraggio di base in AMS) curato da AMS per il monitoraggio delle risorse nell'account gestito. La configurazione di monitoraggio di un account può differire dalla configurazione di base, a seguito delle modifiche richieste dall'utente.

Una notifica di guasti imminenti, in corso, ricorrenti o potenziali, peggioramento delle prestazioni o problemi di sicurezza generati dal monitoraggio di base configurato in un account viene chiamata avviso. Esempi di avvisi sono Amazon CloudWatch Alarm, Amazon CloudWatch Event, Event o Finding di un servizio AWS come Amazon GuardDuty e un evento o un avviso di Trend Micro Deep Security.

Gli avvisi provenienti da servizi AWS relativi alla sicurezza come Amazon, GuardDuty Amazon Macie o Trend Micro Deep Security sono chiamati avvisi di sicurezza per differenziarli da altri tipi di avvisi.

Il monitoraggio AMS offre i seguenti vantaggi:

- La possibilità di personalizzare gli allarmi relativi alle risorse di base per soddisfare le vostre esigenze.

- Correzione automatica degli avvisi, quando possibile, per prevenire o ridurre l'impatto sulle applicazioni. Ad esempio, se utilizzi un' EC2 istanza Amazon autonoma che non supera il controllo dello stato del sistema, AMS tenta di ripristinare l'istanza interrompendola e riavviandola. Per ulteriori informazioni, consulta Correzione automatica degli avvisi con AMS.
- Trasparenza sugli avvisi attivi e precedentemente risolti utilizzando. OpsCenter Ad esempio, se hai un utilizzo imprevisto elevato della CPU su un' EC2 istanza Amazon, puoi richiedere l'accesso alla AWS Systems Manager console (che include l'accesso alla OpsCenter console) e visualizzarla OpsItem direttamente nella OpsCenter console.
- Analisi degli avvisi per determinare le azioni appropriate.
- Avvisi generati in base alla configurazione dell'account e ai servizi supportati. AWS La configurazione di monitoraggio di un account si riferisce a tutti i parametri delle risorse dell'account che creano un avviso. La configurazione di monitoraggio di un account include le definizioni di CloudWatch allarme e EventBridge (precedentemente noti come CloudWatch Eventi) che generano l'avviso (allarme o evento). Per ulteriori informazioni sui parametri delle risorse, vedere. Avvisi dal monitoraggio di base in AMS
- Notifica di guasti imminenti, in corso, ricorrenti o potenziali, peggioramento delle prestazioni o problemi di sicurezza generati dal monitoraggio di base configurato in un account (noto come avviso). Esempi di avvisi includono un CloudWatch allarme, un evento o un risultato da un servizio AWS, come GuardDuty o AWS Health.

Cosa monitora il sistema di monitoraggio AMS?

In linea con il modello di responsabilità dei servizi condivisi di AWS Managed Services (AMS), il sistema di monitoraggio AMS monitora l'infrastruttura AWS. Per dettagli sul monitoraggio di base in AMS, incluse le risorse AWS monitorate e il tipo di avvisi per ciascuna risorsa, consulta. Avvisi dal monitoraggio di base in AMS Per EC2 le istanze Amazon, AMS monitora il sistema operativo e fornisce un monitoraggio di base basato su parametri del sistema operativo come l'utilizzo della CPU e l'utilizzo del volume root.

Ti consigliamo di integrare il monitoraggio AMS con un monitoraggio aggiuntivo utilizzando servizi AWS personalizzati per la tua applicazione. Per indicazioni sul monitoraggio della disponibilità, consulta la sezione «Monitoraggio e allarmi» in questo white paper Reliability Pillar. È possibile configurare il monitoraggio in base alle proprie esigenze operative; come eseguire questa operazione è illustrato in and. Creazione di CloudWatch allarmi aggiuntivi in AMS Creazione di CloudWatch metriche e allarmi personalizzati in AMS

Monitoraggio proattivo della Single-Account Landing Zone di Active Directory Trust in AMS

AMS single-account landing zone (SALZ) monitora lo stato dei trust unidirezionali tra Managed Active Directory (AD) nel tuo account gestito AMS e il dominio della tua azienda. La fiducia unidirezionale con Managed AD è fondamentale per le richieste di accesso e le richieste di accesso alle istanze. Con questo nuovo monitoraggio, AMS ora risponde in modo proattivo ai problemi relativi alla fiducia e riduce il tempo medio necessario per rilevare gli incidenti relativi all'accesso.

Questa funzionalità viene abilitata automaticamente nei tuoi account AWS Managed Services (AMS).

C'è un piccolo impatto sui costi. La funzionalità utilizza quattro CloudWatch parametri AWS e due CloudWatch allarmi AWS per un trust.

Come funziona il monitoraggio

Guarda la seguente grafica sull'architettura di monitoraggio in AWS Managed Services (AMS).

Il diagramma seguente fornisce una panoramica di alto livello del flusso di lavoro di monitoraggio della landing zone con più account AMS e del flusso di lavoro di monitoraggio della landing zone con account singolo AMS.

- Generazione: al momento dell'onboarding dell'account, AMS configura il monitoraggio di base (una combinazione di allarmi CloudWatch (CW) e regole degli eventi CW) per tutte le risorse create in un account gestito. La configurazione di monitoraggio di base genera un avviso quando viene attivato un allarme CW o viene generato un evento CW.
- Aggregazione:
  - Multi-Account Landing Zone: gli avvisi vengono generati dalle vostre risorse all'interno degli account Application e Core Organizational Unit e inviati al sistema di monitoraggio AMS indirizzandoli tramite l'account Security.
  - Zona di destinazione per account singolo: tutti gli avvisi generati dalle tue risorse vengono inviati al sistema di monitoraggio AMS indirizzandoli a un argomento SNS dell'account.
  - Puoi anche configurare il modo in cui AMS raggruppa gli avvisi. EC2 AMS raggruppa tutti gli avvisi relativi alla stessa EC2 istanza in un unico incidente o crea un incidente per avviso, a seconda delle preferenze. Puoi modificare questa configurazione in qualsiasi momento

collaborando con il tuo Cloud Service Delivery Manager o Cloud Architect. Funziona allo stesso modo indipendentemente dal fatto che utilizzi Multi-Account Landing Zone o Single-Account Landing Zone.

- Elaborazione: AMS analizza gli avvisi e li elabora in base al loro potenziale impatto. Gli avvisi vengono elaborati come descritto di seguito.
  - Avvisi con un impatto noto sui clienti: portano alla creazione di un nuovo rapporto sugli incidenti e AMS segue il processo di gestione degli incidenti; per informazioni sulla gestione degli incidenti, vedere. Risposta agli incidenti AMS

    Esempio di avviso: un' EC2 istanza Amazon non supera un controllo dello stato del sistema, AMS tenta di ripristinare l'istanza interrompendola e riavviandola.
  - Avvisi con un impatto incerto sui clienti: per questi tipi di avvisi, AMS invia un rapporto sugli incidenti, in molti casi chiedendo di verificare l'impatto prima che AMS intervenga. Tuttavia, se i controlli relativi all'infrastruttura vengono superati, AMS non ti invia una segnalazione sull'incidente.

    Ad esempio: un avviso per un utilizzo della CPU superiore all'85% per più di 10 minuti su un' EC2istanza Amazon non può essere immediatamente classificato come incidente poiché questo comportamento potrebbe essere previsto in base all'utilizzo. In questo esempio, AMS Automation esegue controlli relativi all'infrastruttura sulla risorsa. Se tali controlli vengono superati, AMS non invia una notifica di avviso, anche se l'utilizzo della CPU supera il 99%. Se Automation rileva che i controlli relativi all'infrastruttura non riescono sulla risorsa, AMS invia una notifica di avviso e verifica se è necessaria una mitigazione. Le notifiche di avviso sono illustrate in dettaglio in questa sezione. AMS offre opzioni di mitigazione nella notifica. Quando rispondi alla notifica confermando che l'avviso è un incidente, AMS crea un nuovo rapporto sull'incidente e inizia il processo di gestione degli incidenti AMS. Le notifiche di servizio che ricevono una risposta di «nessun impatto sul cliente» o nessuna risposta per tre giorni, vengono contrassegnate come risolte e l'avviso corrispondente viene contrassegnato come risolto.
  - Avvisi senza impatto sul cliente: se, dopo la valutazione, AMS determina che l'avviso non ha alcun impatto sul cliente, l'avviso viene chiuso.

    Ad esempio, AWS Health notifica la presenza di un' EC2 istanza che richiede la sostituzione, ma da allora tale istanza è stata interrotta.

EC2 notifiche raggruppate di istanze

È possibile configurare il monitoraggio AMS per raggruppare gli avvisi della stessa EC2 istanza in un unico incidente. Il tuo Cloud Service Delivery Manager o Cloud Architect può configurarlo per te. È possibile configurare quattro parametri per ogni account gestito da AMS.

1. Ambito: scegli a livello di account o basato su tag.
   - Per specificare una configurazione applicabile a ogni EC2 istanza di quell'account, scegli scope = a livello di account.
   - Per specificare una configurazione che si applica solo alle EC2 istanze di quell'account con un tag specifico, scegli scope = tag-based.
2. Regola di raggruppamento: scegli classica o istanza.
   - Per configurare il raggruppamento a livello di istanza per ogni risorsa del tuo account, scegli ambito = a livello di account e regola di raggruppamento = istanza.
   - Per configurare risorse specifiche nel tuo account per utilizzare il raggruppamento a livello di istanza, tagga tali istanze e quindi scegli scope = basato su tag e regola di raggruppamento = livello di istanza.
   - Per non utilizzare il raggruppamento di istanze per gli avvisi nel tuo account, scegli la regola di raggruppamento = classica.
3. Opzione di coinvolgimento: scegli nessuna opzione, solo report o predefinita.
   - Affinché AMS non crei incidenti o non esegua automazioni per gli allarmi utilizzando tali risorse mentre la configurazione è attiva, scegli nessuna.
   - Affinché AMS non crei incidenti o esegua automazioni per gli allarmi da tali risorse mentre la configurazione è attiva e non esegua documenti di correzione automatica di Systems Manager, ma per includere i record di questi eventi nei report, scegli solo report. Ciò può essere utile se desiderate ridurre il volume dei casi di assistenza in caso di incidenti con cui interagite e se alcuni incidenti causati da alcune risorse non richiedono un'attenzione immediata, ad esempio quelli relativi a un account non di produzione.
   - Affinché AMS elabori gli avvisi, esegua automazioni e crei casi di incidenti quando necessario, scegli Default.
4. Risolvi dopo: scegli tra 24 ore, 48 ore o 72 ore. Infine, configura quando i casi di incidente vengono chiusi automaticamente. Se l'ora dell'ultima corrispondenza tra i casi raggiunge il valore Resolve after configurato, l'incidente viene chiuso.

Notifica di avviso

Come parte dell'elaborazione degli avvisi, basata sull'analisi dell'impatto, AWS Managed Services (AMS) crea un incidente e avvia il processo di gestione degli incidenti per la correzione, quando è possibile determinare l'impatto. Se non è possibile determinare l'impatto, AMS invia una notifica di avviso all'indirizzo e-mail associato al tuo account tramite una notifica di servizio. In alcuni scenari, questa notifica di avviso non viene inviata. Ad esempio, se i controlli relativi all'infrastruttura vengono superati per un avviso di utilizzo elevato della CPU, all'utente non viene inviata una notifica di avviso. Per ulteriori informazioni, consulta il diagramma sull'architettura di monitoraggio AMS per il processo di gestione degli avvisi in. Come funziona il monitoraggio

Notifica di avviso basata su tag

Utilizza i tag per inviare notifiche di avviso relative alle tue risorse a diversi indirizzi e-mail. È consigliabile utilizzare notifiche di avviso basate su tag, poiché le notifiche inviate a un singolo indirizzo e-mail potrebbero creare confusione quando più team di sviluppatori utilizzano lo stesso account. Le notifiche di avviso basate su tag non sono influenzate dalle EC2 notifiche raggruppate di istanze impostazioni scelte.

Con le notifiche di avviso basate su tag puoi:

- Inviare avvisi a un indirizzo e-mail specifico: contrassegna le risorse che dispongono di avvisi che devono essere inviati a un indirizzo e-mail specifico con,. `key = OwnerTeamEmail` `value = EMAIL_ADDRESS`
- Invia avvisi a più indirizzi e-mail: per utilizzare più indirizzi e-mail, specifica un elenco di valori separati da virgole. Ad esempio, `key = OwnerTeamEmail`, `value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`. Il numero totale di caratteri per il campo del valore non può superare 260.
- Usa una chiave di tag personalizzata: per utilizzare una chiave di tag personalizzata, fornisci il nome della chiave tag personalizzata al tuo CSDM in un'e-mail che dia esplicitamente il consenso all'attivazione di notifiche automatiche per la comunicazione basata su tag. È consigliabile utilizzare la stessa strategia di tagging per i tag di contatto in tutte le istanze e le risorse.

> **Note**
>
> Il valore chiave *`OwnerTeamEmail`* non deve necessariamente essere nel caso di camel. Tuttavia, i tag fanno distinzione tra maiuscole e minuscole ed è consigliabile utilizzare il formato consigliato.
> L'indirizzo e-mail deve essere specificato per intero, con il segno «at» (@) per separare la parte locale dal dominio. Esempi di indirizzi e-mail non validi: *`Team.AppATabc.xyz`* o*`john.doe`*. Per indicazioni generali sulla tua strategia di tagging, consulta AWS Tagging resources. Non aggiungere informazioni di identificazione personale (PII) nei tag. Usa liste di distribuzione o alias laddove possibile.
> La notifica di avviso basata su tag è supportata per le risorse dei seguenti Amazon Services: Elastic Block Store (EBS) EC2, Elastic Load Balancing (ELB), Application Load Balancer (ALB), Network Load Balancer, Relational Database Service (RDS), Elastic File System (EFS) e VPN. OpenSearch FSx Site-to-Site

Visualizzazione della configurazione di monitoraggio per un account AMS

È possibile visualizzare due parti fondamentali della configurazione di monitoraggio di un account:

- CloudWatch Allarmi: puoi visualizzare tutti gli allarmi CW presenti nell'account accedendo alla CloudWatch console e selezionando diversi servizi di interesse.
- CloudWatch Eventi:
  - Zona di destinazione multiaccount: CloudWatch gli eventi monitorati nell'account possono essere trovati filtrando tutte le regole degli eventi CW con la stringa. `"ams-"`
  - Zona di destinazione per account singolo: CloudWatch gli eventi monitorati nell'account possono essere trovati filtrando tutte le regole degli eventi CW con la stringa. `"mc-"`

Modifica della configurazione di monitoraggio per un account AMS

Puoi modificare la configurazione di monitoraggio di base per EC2 le risorse Amazon. Per gli avvisi che possono essere configurati, consulta. Avvisi dal monitoraggio di base in AMS È possibile modificare la definizione degli allarmi, la destinazione degli allarmi o disattivare la notifica di allarme per i monitor di base in modo che gli avvisi soddisfino i requisiti operativi dell'applicazione. È possibile

richiedere alcune o tutte le modifiche menzionate in precedenza inviando un CT di gestione | Altro | Altro | Aggiornamento (ct-0xdawir96cy7k) con i seguenti dettagli.

- Istanza IDs [opzionale, se non menzionata, tutte le istanze dell'account rientrano nell'ambito]
- CloudWatch nome metrico, ad esempio, utilizzo della CPU/swap free/ IOwait
- Target: ID e-mail/numero di telefono per l'argomento SMS/SNS

Per ulteriori informazioni sul tipo di modifiche che puoi richiedere nella configurazione di monitoraggio di base, consulta la CloudWatch documentazione di Amazon.

Notifiche di incidenti con riconoscimento delle applicazioni in AMS

Utilizza le notifiche automatiche di incidenti basate sulle applicazioni per personalizzare la tua esperienza di comunicazione per i casi di supporto creati da AMS per tuo conto. Quando utilizzi questa funzione, AMS recupera le preferenze personalizzate relative ai carichi di lavoro AWS Service Catalog AppRegistryper arricchire le comunicazioni relative agli incidenti AMS con metadati sulle tue applicazioni e personalizzare la gravità dei casi di supporto creati da AMS per tuo conto. Per utilizzare questa funzionalità, devi prima effettuare il provisioning AWS Service Catalog AppRegistry nel tuo account AMS.

Per ulteriori informazioni sui valori predefiniti di monitoraggio di AMS, consulta. Monitoraggio e gestione degli eventi in AMS

Effettua il provisioning AppRegistry nel tuo account AMS e crea applicazioni

Il AppRegistry servizio è disponibile in modalità Self-service Provisioning (SSP) per il tuo account AMS. Per istruzioni su come richiedere l'accesso, consulta Usare AMS SSP per il provisioning AWS Service Catalog AppRegistry nel tuo account AMS.

Dopo il provisioning AppRegistry, utilizza uno dei seguenti metodi per creare applicazioni:

1. AWS console: per ulteriori informazioni sulla creazione di un'applicazione AppRegistry tramite la console AWS, consulta Creating Applications nella AWS Service Catalog AppRegistry Administrator Guide.
2. CloudFormation: Puoi definire la tua AppRegistry applicazione proprio come definisci qualsiasi altra risorsa. Per ulteriori informazioni, consulta Riferimento al tipo di risorsa AWS Service Catalog AppRegistry nella Guida dell'utente di CloudFormation .

Crea tag per abilitare l'arricchimento dei casi

È necessario etichettare le applicazioni prima che AMS possa accedere ai metadati delle applicazioni. La tabella seguente elenca il tag richiesto.

Chiave tag	Valore tag
è gestito da ams	true

Personalizza la gravità dei casi di supporto AMS per le tue applicazioni

Puoi personalizzare la gravità dei casi di supporto creati da AMS specificando l'importanza dell'applicazione per l'organizzazione. Questa impostazione è controllata da un gruppo di attributi associato all'applicazione in AppRegistry. Il nome del nome del gruppo di attributi deve corrispondere al seguente schema:

```
AMS.<ApplicationName>.CommunicationOptions
```

Nello schema precedente, `ApplicationName` deve corrispondere al nome utilizzato al AppRegistry momento della creazione dell'applicazione.

Contenuto di esempio:

```
{
"SchemaVersion": "1.0",
"Criticality": "low"
}
```

SchemaVersion

Ciò determina la versione dello schema che stai utilizzando e il sottoinsieme di funzionalità disponibili per l'uso.

Versione dello schema	Funzionalità
1.0	Severità personalizzata dei casi di supporto in base al valore di criticità

Criticità

La criticità di questa applicazione determina la gravità dei casi di supporto creati dai sistemi automatizzati AMS.

Valori validi:

```
low|normal|high|urgent|critical
```

Per ulteriori informazioni sui livelli di gravità, consulta SeverityLevelnell'Supporto AWS API Reference.

Campo obbligatorio: sì

Rivedi le autorizzazioni richieste

Per utilizzare questa funzionalità, AMS richiede l'accesso alle seguenti autorizzazioni: AWS Identity and Access Management

- Io sono: ListRoleTags
- Io sono: ListUserTags
- sourcegrouptaggingapi: GetResources
- service catalog-app: GetApplication
- servicecatalog-app: ListAssociatedAttributeGroups
- servicecatalog-app: GetAttributeGroup

> **Important**
>
> Assicurati che non esista una policy IAM o una policy di controllo del servizio (SCP) che neghi le azioni precedenti.

Le chiamate API vengono effettuate dal ruolo. `ams-access-admin` Di seguito è riportato un esempio di ciò che potresti vedere:

```
arn:aws:sts::111122223333:assumed-role/ams-access-admin/AMS-AMSAppMetadataLookup-*
```

Utilizzo OpsCenter in AMS

Il team operativo di AWS Managed Services (AMS) lo utilizza AWS Systems Manager OpsCenterper diagnosticare e correggere molti avvisi relativi alle tue risorse.

L'utilizzo OpsCenter riduce il tempo medio di risoluzione (MTTR), fornendo al contempo una visione trasparente delle code operative dei team operativi AMS.

Con OpsCenter, AMS offre una visione trasparente degli elementi di lavoro operativi, noti anche come OpsItems, su cui i team AMS stanno lavorando attivamente, oltre alle soluzioni automatizzate.

Per ulteriori informazioni su OpsCenter e OpsItems, consulta AWS Systems Manager OpsCenter. Per informazioni su come accedere alla Console di AWS gestione, consulta Working with the AWS Management Console. Dalla Console di gestione AWS puoi accedere alla console AWS Systems Manager e OpsCenter, per ulteriori informazioni, consulta AWS Systems Manager Session Manager. OpsCenter fornisce anche un'API che puoi usare; per informazioni, consulta Ulteriori informazioni su OpsCenter.

OpsCenter è una funzionalità dal prezzo di circa 1000 dollari OpsItems che costa meno di $10. Per informazioni, consulta Prezzi di AWS Systems Manager.

Notifiche di avviso da AMS

Come parte dell'elaborazione degli avvisi, basata sull'analisi dell'impatto, AWS Managed Services (AMS) crea un incidente e avvia il processo di gestione degli incidenti per la correzione, quando è possibile determinare l'impatto. Nel caso in cui non sia possibile determinare l'impatto, AMS invia una notifica di avviso all'indirizzo e-mail associato all'account tramite una notifica di servizio; consulta il diagramma sull'architettura di monitoraggio AMS per il processo di gestione degli avvisi in. Come funziona il monitoraggio

Ricezione di avvisi generati da AMS

AWS Managed Services (AMS) ti consente di ricevere notifiche di avviso direttamente per le EC2 risorse Amazon per ridurre i ritardi nelle comunicazioni. Per ricevere direttamente EC2 gli avvisi Amazon, iscrivi la tua destinazione (indirizzo e-mail preferito) all'argomento Direct-Customer-Alerts di Amazon SNS utilizzando il tipo di modifica Gestione | Monitoraggio e notifica | SNS | Subscribe (ct-3rcl9u1k017wu).

> **Note**
>
> Per impostazione predefinita, non tutti gli avvisi di base vengono inviati all'argomento Direct-Customer-Alerts. Per visualizzare tutti gli avvisi generati dal sistema di monitoraggio AMS, iscriviti all'argomento Amazon SNS relativo al sistema di monitoraggio AMS. Nella richiesta, richiedi «AMS Monitoring Topic», specifica un canale di abbonamento per ricevere gli avvisi (Lambda, Amazon SQS, HTTP/S, e-mail o SMS) e specifica gli endpoint (ad esempio, indirizzi e-mail, se scegli il protocollo e-mail) che riceveranno gli avvisi.
> L'argomento di monitoraggio AMS riceve gli avvisi utilizzati dai servizi condivisi AMS, quindi può essere rumoroso.

Per ulteriori informazioni, consulta la sezione Iscriviti nel riferimento all'API di iscrizione ad Amazon Simple Notification Service.

Per un elenco degli avvisi di base forniti da AMS, consulta. Avvisi dal monitoraggio di base in AMS

Notifiche di avviso basate su tag in AMS

Utilizza i tag per inviare notifiche di avviso relative alle tue risorse a diversi indirizzi e-mail. È consigliabile utilizzare notifiche di avviso basate su tag, poiché le notifiche inviate a un singolo indirizzo e-mail potrebbero creare confusione quando più team di sviluppatori utilizzano lo stesso account.

> **Important**
>
> Le notifiche di avviso basate su tag funzionano solo per le notifiche relative ad Amazon EC2, Amazon EBS, Elastic Load Balancing, Network Load Balancer, Application Load Balancer, Amazon RDS, Amazon Redshift e. OpenSearch
> Non aggiungere informazioni di identificazione personale (PII) nei tag.

Invia avvisi a un indirizzo email specifico

Contrassegna le risorse con avvisi che devono essere inviati a un indirizzo email specifico con,. `key = OwnerTeamEmail` `value = EMAIL_ADDRESS`

Invia avvisi a più indirizzi e-mail

Per utilizzare più indirizzi e-mail, specifica un elenco di valori separati da virgole. Ad esempio, `key = OwnerTeamEmail`, `value = EMAIL_ADDRESS_1, EMAIL_ADDRESS_2, EMAIL_ADDRESS_3, ...`. Il numero totale di caratteri per il campo del valore non può superare 260.

Usa una chiave tag personalizzata

Per utilizzare una chiave tag personalizzata, fornisci il nome della chiave tag personalizzata al tuo CSDM in un'e-mail in cui acconsenti all'attivazione della notifica automatica per la comunicazione basata su tag. È consigliabile utilizzare la stessa strategia di etichettatura per i tag di contatto in tutte le istanze e le risorse.

L'indirizzo e-mail deve essere specificato per intero, con il segno «at» (@) per separare la parte locale dal dominio. Esempi di indirizzi e-mail non validi: `Team.AppATabc.xyz` o`john.doe`. Per indicazioni generali sulla strategia di tagging, consulta Utilizzo dei tag. Per etichettare una risorsa esistente, invia una RFC con il tipo di modifica Deployment | Advanced stack components | Tag | Create (auto) (ct-3cx7we852p3af).

> **Note**
>
> Il valore chiave non deve necessariamente essere in caso di cammello. `OwnerTeamEmail` Tuttavia, i tag fanno distinzione tra maiuscole e minuscole ed è consigliabile utilizzare il formato consigliato.

Correzione automatica degli avvisi con AMS

Dopo la verifica, AWS Managed Services (AMS) corregge automaticamente determinati avvisi in base a condizioni e processi specifici descritti in questa sezione.

Nome dell'avviso	Descrizione	Soglie	Azione
Canale sicuro non funzionante	L'allarme Broken Secure Channel viene attivato sulle EC2 istanze Windows quando l'istanza perde la connessione con	La soglia supera il valore definito 10 volte negli ultimi 15 minuti.	La correzione automatica di AMS verifica che l'istanza sia online in SSM, che il nome host non sia duplicato e che

Nome dell'avviso	Descrizione	Soglie	Azione
	il controller di dominio AD.		l'oggetto AD Computer sia allineato allo stack. CloudFormation La riparazione ripara la connessione sicura del canale per ripristinare l'accesso all'istanza.
Verifica dello stato non riuscita	Possibili guasti hardware o uno stato di errore dell'istanza.	Il sistema ha rilevato uno stato di errore almeno una volta negli ultimi 15 minuti.	La riparazione automatica AMS verifica innanzitutto se l'istanza è accessibile. Se l'istanza è inaccessi bile, viene interrotta e riavviata. L'arresto e l'avvio consentono all'istanza di migrare verso il nuovo hardware sottostante. Per ulteriori informazioni, consulta la sezione seguente "EC2 Status Check Failure Remediation Automatio n».
AMSLinuxD iskUsage	Si attiva quando l'utilizz o su disco di 1 punto di montaggio (spazio designato su un volume) sull' EC2 istanza si sta esaurendo.	La soglia supera il valore definito 6 volte negli ultimi 30 minuti.	La riparazione automatic a AMS elimina innanzitu tto i file temporanei. Se ciò non libera abbastanza spazio su disco, estende il volume per evitare tempi di inattività se il volume si riempie.

Nome dell'avviso	Descrizione	Soglie	Azione
AMSWindowsDiskUsage	Quando l'utilizzo del disco di 1 punto di montaggio (spazio designato su un volume) sull' EC2 istanza è esaurito.	La soglia supera il valore definito 6 volte negli ultimi 30 minuti.	La riparazione automatica AMS elimina innanzitutto i file temporanei. Se ciò non libera abbastanza spazio su disco, estende il volume per evitare tempi di inattività se il volume si riempie.

Nome dell'avviso	Descrizione	Soglie	Azione
RDS-EVENT-0089	L'istanza database ha utilizzato oltre il 90% dello storage allocato.	Lo spazio di archiviazione è allocato per oltre il 90%.	La correzione automatica AMS verifica innanzitutto che il DB sia in uno stato modificabile e disponibile o che lo spazio di archiviazione sia pieno. Tenta quindi di aumentare lo storage allocato, gli IOPS e il throughput di storage tramite un changeset. CloudFormation Se è già stata rilevata una deriva dello stack, ricorre all'API RDS per evitare tempi di inattività. Questa funzionalità può essere disattivata aggiungendo il seguente tag all'istanza DB RDS: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Nome dell'avviso	Descrizione	Soglie	Azione
RDS-EVENT-0007	Lo storage allocato per l'istanza DB è esaurito. Per risolvere, alloca spazio di archiviazione aggiuntivo.	Lo storage è allocato al 100%.	La correzione automatica AMS verifica innanzitutto che il DB sia in uno stato modificabile e disponibile o che lo spazio di archiviazione sia pieno. Tenta quindi di aumentare lo storage allocato, gli IOPS e il throughput di storage tramite un changeset. CloudFormation Se è già stata rilevata una deriva dello stack, ricorre all'API RDS per evitare tempi di inattività. Questa funzionalità può essere disattivata aggiungendo il seguente tag all'istanza DB RDS: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Nome dell'avviso	Descrizione	Soglie	Azione
RDS-EVENT-0224	Lo storage allocato richiesto raggiunge o supera la soglia di archiviazione massima configurata.	La soglia massima di archiviazione per l'istanza DB è stata esaurita o è maggiore o uguale allo storage allocato richiesto.	La riparazione automatica AMS verifica innanzitutto che la quantità richiesta di storage RDS superi la soglia massima di archiviazione. Se confermata, AMS tenta di aumentare la soglia massima di archiviazione del 30% con un CloudFormation changeset o un'API RDS diretta se il provisioning delle risorse non viene effettuato tramite. CloudFormation Questa funzionalità può essere disattivata aggiungendo il seguente tag all'istanza DB RDS: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Nome dell'avviso	Descrizione	Soglie	Azione
Capacità di archiviazione RDS	Rimane meno di 1 GB nello storage allocato per l'istanza DB.	Lo storage è allocato al 99%.	La correzione automatica AMS verifica innanzitutto che il DB sia in uno stato modificabile e disponibile o che lo spazio di archiviazione sia pieno. Tenta quindi di aumentare lo storage allocato, gli IOPS e il throughput di storage tramite un changeset. CloudFormation Se è già stata rilevata una deriva dello stack, ricorre all'API RDS per evitare tempi di inattività. Questa funzionalità può essere disattivata aggiungendo il seguente tag all'istanza DB RDS: `"Key: ams:rt:ams-rds-max-allocated-storage-policy, Value: ams-opt-out".`

Amazon EC2 Broken Secure Channel: nota sull'automazione della riparazione

Prima che la riparazione automatica di AWS Managed Services (AMS) esegua la correzione dei problemi relativi al Broken Secure Channel di Amazon EC2 Windows, l'automazione esegue i seguenti controlli preliminari e crea un rapporto sugli incidenti per ulteriori indagini:

- Verifica che lo stato SSM dell' EC2 istanza Amazon sia «Online».

- Verifica se l' EC2 istanza Amazon fa parte di un gruppo Auto Scaling e se tutte le istanze del gruppo Auto Scaling hanno lo stesso nome host.
- Verifica se l' EC2 istanza Amazon fa parte dello CloudFormation stack utilizzato per il provisioning. Se l'istanza è stata rimossa dallo CloudFormation stack, l'automazione verifica se l'unità organizzativa (OU) di Active Directory associata fa ancora riferimento allo stack.

Una volta superate le convalide di cui sopra, l'automazione procede alla correzione del canale Broken Secure.

Fasi di riparazione:

- La riparazione automatica tenta di ripristinare il canale sicuro tra l' EC2 istanza e il dominio AD, ripristinando l'accesso all'istanza.
- Dopo la riparazione, l'automazione verifica che sia stato stabilito il canale sicuro. In caso di esito negativo, AMS crea un incidente e incarica le operazioni di AMS di indagare.

EC2 errore nel controllo dello stato: note sull'automazione della riparazione

Come funziona la riparazione automatica AMS in caso di problemi relativi al controllo EC2 dello stato:

- Se la tua EC2 istanza Amazon è diventata irraggiungibile, l'istanza deve essere interrotta e riavviata in modo da poter essere migrata su un nuovo hardware e ripristinata.
- Se la radice del problema è all'interno del sistema operativo (dispositivi mancanti in fstab, danneggiamento del kernel e così via), l'automazione non è in grado di ripristinare l'istanza.
- Se l'istanza appartiene a un gruppo Auto Scaling, l'automazione non interviene: l'azione di AutoScalingGroup ridimensionamento sostituisce l'istanza.
- Se l'istanza ha EC2 Auto Recovery abilitato, la riparazione non interviene.

EC2 automazione della correzione dell'utilizzo dei volumi

Come funziona la riparazione automatica di AWS Managed Services (AMS) in caso di problemi di utilizzo dei EC2 volumi:

- L'automazione verifica innanzitutto se l'espansione del volume è necessaria e se può essere eseguita. Se l'espansione è ritenuta appropriata, l'automazione può aumentare la capacità del volume. Questo processo automatizzato bilancia l'esigenza di crescita con un'espansione controllata e limitata.

- Prima di estendere un volume, l'automazione esegue attività di pulizia (Windows: Disk Cleaner, Linux: Logrotate + rimozione del registro dell'agente di Simple Service Manager) sull'istanza per cercare di liberare spazio.

  > **Note**
  >
  > Le attività di pulizia non vengono eseguite sulle istanze della famiglia EC2 «T» perché si affidano ai crediti della CPU per la continuità delle funzionalità.

- Su Linux, l'automazione supporta solo l'estensione dei file system di tipo EXT2 C e XFS. EXT3 EXT4
- Su Windows, l'automazione supporta solo New Technology File System (NTFS) e Resilient File System (ReFS).
- L'automazione non estende i volumi che fanno parte di Logical Volume Manager (LVM) o di un array RAID.
- L'automazione non estende i volumi dell'Instance Store.
- L'automazione non interviene se il volume interessato è già superiore a 2 TiB.
- L'espansione attraverso l'automazione è limitata a un massimo di tre volte alla settimana e cinque volte in totale nell'arco della vita del sistema.
- L'automazione non aumenta il volume se l'espansione precedente è avvenuta nelle ultime sei ore.

Quando queste regole impediscono all'automazione di intervenire, AMS contatta l'utente tramite una richiesta di servizio in uscita per determinare le azioni successive da intraprendere.

Automazione della correzione degli eventi a basso livello di storage di Amazon RDS

Come funziona la riparazione automatica di AWS Managed Services (AMS) con i problemi relativi agli eventi di storage insufficiente di Amazon RDS:

- Prima di provare a estendere lo storage dell'istanza Amazon RDS, l'automazione esegue diversi controlli per garantire che l'istanza Amazon RDS sia in uno stato modificabile e disponibile o pieno di spazio di archiviazione.
- Se viene rilevata una deriva CloudFormation dello stack, la correzione avviene tramite l'API Amazon RDS.
- L'azione di riparazione non viene eseguita nei seguenti scenari:

  - Lo stato dell'istanza Amazon RDS non è «disponibile» o «pieno di spazio di archiviazione».
  - Lo storage delle istanze Amazon RDS non è attualmente modificabile (ad esempio quando lo storage è stato modificato nelle ultime sei ore).
  - L'istanza Amazon RDS ha lo storage con scalabilità automatica abilitato.
  - L'istanza Amazon RDS non è una risorsa all'interno di uno CloudFormation stack.
- La riparazione è limitata a un'espansione ogni sei ore e a non più di tre espansioni nell'arco di quattordici giorni consecutivi.
- Quando si verificano questi scenari, AMS ti contatta per segnalarti un incidente in uscita per determinare le azioni successive.

Creazione di CloudWatch allarmi aggiuntivi in AMS

Puoi creare nuovi CloudWatch allarmi utilizzando il tipo di modifica AWS Managed Services (AMS) Deployment | Monitoring and notification CloudWatch | | Create alarms.

> **Important**
>
> AMS non monitora gli CloudWatch allarmi creati da te.

Utilizzo di CloudWatch parametri e allarmi personalizzati per le EC2 istanze Amazon (funziona solo per le distribuzioni mutabili che non si basano sull'aggiornamento distribuito ai AMIs gruppi di Auto Scaling):

1. Produci uno script di monitoraggio delle applicazioni e una metrica personalizzata. Per ulteriori informazioni e accesso a script di esempio, consulta Monitoring Memory and Disk Metrics EC2 for Amazon Linux Instances. Gli script di CloudWatch monitoraggio di Amazon per EC2 le istanze Amazon Linux dimostrano come produrre e utilizzare metriche CloudWatch personalizzate di Amazon. Questi script Perl di esempio contengono un esempio completamente funzionale che crea report sui parametri di memoria, swap e uso dello spazio su disco relativi a un'istanza Linux.
2. Carica il tuo script di monitoraggio. Per caricare lo script di monitoraggio nella configurazione del gruppo Auto Scaling o dell' EC2 istanza Amazon, puoi UserData utilizzarlo durante la configurazione del gruppo Auto Scaling o dell'istanza EC2 Amazon oppure, se l'applicazione è stata distribuita CodeDeploy con, puoi modificare la configurazione con Deployment | Applications | application | Deploy CT (CodeDeploy ct-2edc3sd1sqmrb).

3. Pubblica la metrica personalizzata su CloudWatch (la prima volta che pubblichi un punto dati per una nuova metrica personalizzata, questa viene creata), vedi Pubblicazione di metriche personalizzate.
4. Crea l' CloudWatch allarme, vedi Creare un CloudWatch avviso per un'istanza.

> **Important**
>
> I dati di monitoraggio devono essere inviati a questo percorso [`infra/INSTANCE_ID/YOUR_CUSTOM_METRIC`]

Per modificare o eliminare un CloudWatch allarme, invia una RFC con Management | Other | Other | Create change type (ct-1e1xtak34nx76) con i parametri necessari per completare l'azione come descritto nel riferimento all'API Amazon. CloudWatch PutMetricAlarm

Puoi utilizzare il flusso di eventi. CloudWatch AMS è integrato con CloudWatch e puoi richiedere che qualsiasi chiamata API AWS attivi un CloudWatch evento.

A tale scopo, invia un messaggio Management | Other | Other | Update CT (ct-0xdawir96cy7k) con le chiamate API che ti interessano. Un operatore AMS ti contatterà per raccogliere i requisiti. Per ulteriori informazioni, consulta la CloudWatch documentazione di Amazon.

Per accedere allo stream degli CloudWatch eventi, invia un messaggio Management | Other | Other | Update CT (ct-0xdawir96cy7k) per aggiungere un party all'argomento relativo alle notifiche SNS. Un operatore AMS ti contatterà per raccogliere i requisiti.

Creazione di CloudWatch metriche e allarmi personalizzati in AMS

Puoi archiviare i parametri aziendali e applicativi in Amazon CloudWatch. Puoi visualizzare grafici e impostare allarmi in base a questi parametri, proprio come puoi fare per i parametri CloudWatch già archiviati per le tue risorse AWS Managed Services (AMS). Per ulteriori informazioni CloudWatch, consulta Amazon CloudWatch Concepts.

Amazon SNS consente alle applicazioni di inviare messaggi urgenti a più abbonati tramite un meccanismo «push» verso l'AMS Managed Monitoring System o MMS, l'argomento Amazon SNS (SNS) su cui vengono pubblicati gli allarmi, in questo caso, MMS e le code SQS. Puoi utilizzarlo CloudWatch per creare metriche personalizzate e, tramite un argomento SNS, farti avvisare da AMS in modo appropriato. Per fare ciò, segui questi passaggi.

> **Note**
>
> Questo processo non funziona per le distribuzioni immutabili che si basano sull'aggiornamento AMIs distribuito nei gruppi di Auto Scaling, ma è adatto per le distribuzioni di applicazioni mutabili (non ASG).
> La configurazione di una metrica personalizzata entro i limiti di AMS Advanced è un'attività complessa. Per un esempio tratto da CloudWatch, vedi Esempio: contare le occorrenze di un termine.

1. Produci lo script di monitoraggio dell'applicazione e la metrica personalizzata (come l'esempio del conteggio delle occorrenze). Per ulteriori informazioni e accesso a script di esempio, consulta Monitoring Memory and Disk Metrics EC2 for Amazon Linux Instances.
2. Carica il tuo script di monitoraggio. Per caricare lo script di monitoraggio nella configurazione del gruppo Auto Scaling o dell' EC2 istanza Amazon, puoi UserDatautilizzarlo durante la configurazione del gruppo Auto Scaling o dell'istanza EC2 Amazon oppure, se l'applicazione è stata distribuita CodeDeploy con, puoi modificare la configurazione con Deployment | Applications | application | Deploy CT (CodeDeploy ct-2edc3sd1sqmrb).
3. Pubblica la metrica personalizzata su CloudWatch (la prima volta che pubblichi un punto dati per una nuova metrica personalizzata, questa viene creata), vedi Pubblicare metriche personalizzate.
4. Per integrare la metrica relativa ai clienti nel sistema di monitoraggio delle applicazioni, richiedi ad AMS di creare un argomento SNS per la metrica inviando una RFC con Deployment | Monitoring and notification | SNS | Create change type (ct-3dfnglm4ombbs).
5. Crea l' CloudWatch allarme, consulta Creazione di CloudWatch allarmi Amazon.

> **Important**
>
> I dati di monitoraggio devono essere inviati a questo percorso [infra/*INSTANCE_ID*/*YOUR_CUSTOM_METRIC*].

Utilizzo di CloudWatch Application Insights per.Net e SQL server in AMS

Puoi utilizzare Amazon CloudWatch Application Insights per configurare i monitor per le risorse delle tue applicazioni AWS Managed Services (AMS) per analizzare continuamente i dati alla ricerca di segni di problemi con le tue applicazioni e ridurre il tempo medio di riparazione (MTTR) nella risoluzione dei problemi delle applicazioni. Per i dettagli su CloudWatch Application Insights, consulta CloudWatch Application Insights for .NET e SQL Server.

> **Important**
>
> AMS non monitora i problemi di CloudWatch Application Insights perché riguardano il codice dell'applicazione controllato dall'utente.

Per utilizzare CloudWatch Application Insights, invia una RFC con il tipo di modifica Deployment | Advanced stack components | Identity and Access Management (IAM) | Create entità o policy (revisione richiesta) (ct-3dpd8mdd9jn1r) con una richiesta per creare un ruolo IAM che ti fornisca l'autorizzazione a configurare Application Insights. CloudWatch Esistono due opzioni per ricevere i problemi identificati: tramite un argomento SNS o con un obiettivo nelle regole degli eventi. CloudWatch Nella RFC, specifica quale vuoi. Se prevedi di utilizzare le regole CloudWatch degli eventi, specifica anche la definizione della regola nella RFC. Dopo aver configurato CloudWatch Application Insights, riceverai una notifica di potenziali problemi, inclusi approfondimenti che indicano una possibile causa principale.

Per scoprire come assumere il ruolo, consulta la AMS Onboarding Guide Federate your Active Directory with the AMS IAM Roles.

Utilizzo di Amazon EventBridge Managed Rules in AMS

AMS Advanced utilizza Amazon EventBridge Managed Rules. Una Managed Rule è un tipo di regola unico direttamente collegato ad AMS. Queste regole corrispondono agli eventi in arrivo e li inviano alle destinazioni per l'elaborazione. Le Managed Rules sono predefinite da AMS e includono i modelli di eventi richiesti dal servizio per gestire gli account dei clienti e, se non diversamente definito, solo il servizio proprietario può utilizzare queste Managed Rules.

Le AMS Managed Rules sono collegate al `events.managedservices.amazonaws.com` servizio principale. Queste Managed Rules sono gestite tramite il ruolo

AWSServiceRoleForManagedServices_Eventscollegato al servizio. Per eliminare queste regole è necessaria una conferma speciale da parte del cliente. Per ulteriori informazioni, consulta Eliminazione delle regole gestite per AMS.

Per ulteriori informazioni sulle regole, consulta Rules nella Amazon EventBridge User Guide.

Amazon EventBridge Managed Rules implementato da AMS

Regole EventBridge gestite da Amazon

Nome regola	Descrizione	Definizione
AMSAdvancedCoreRule	Questa regola inoltra Amazon CloudWatch Alarms a AMS Monitoring. Gli CloudWatch eventi di Amazon monitorano gli CloudWatch allarmi.	`{ { "source": ["aws.cloudwatch"], "detail-type": ["CloudWatch Alarm State Change"], } }`

Creazione di regole gestite per AMS

Non è necessario creare manualmente Amazon EventBridge Managed Rules. Quando effettui l'onboarding su AMS tramite la console di AWS gestione AWS CLI, l'API o l' AWS API, AMS le crea per te.

Modifica delle regole gestite per AMS

AMS non consente di modificare le Managed Rules. Il nome e lo schema di eventi per ogni Managed Rule sono predefiniti da AMS.

Eliminazione delle regole gestite per AMS

Non è necessario eliminare manualmente le Managed Rules. Quando esci da AMS tramite la Console di AWS gestione, l'API o l' AWS API AWS CLI, AMS ripulisce le risorse ed elimina tutte le Managed Rules di proprietà di AMS per te.

Nel caso in cui AMS non riesca a rimuovere le Managed Rules durante l'offboarding, puoi anche utilizzare la EventBridge console Amazon, AWS CLI o l' AWS API per eliminare manualmente le Managed Rules. Per fare ciò, devi prima abbandonare AMS e procedere all'eliminazione forzata delle Managed Rules.

Trusted Remediator in AMS

Trusted Remediator è una soluzione AWS Managed Services che automatizza la riparazione e le raccomandazioni. AWS Trusted AdvisorAWS Compute Optimizer Trusted Remediator crea consigli quando Trusted Advisor e Compute Optimizer indica opportunità per ridurre i costi, migliorare la disponibilità del sistema, ottimizzare le prestazioni o colmare le lacune di sicurezza per te. Account AWS Con Trusted Remediator, puoi rispondere a questi consigli su sicurezza, prestazioni, ottimizzazione dei costi, tolleranza agli errori e limiti di servizio in modo sicuro e standardizzato che utilizza le migliori pratiche consolidate. Trusted Remediator consente di configurare una soluzione di riparazione e viene eseguito automaticamente in base a una pianificazione creata dall'utente, semplificando il processo di riparazione. Questo approccio semplificato risolve i problemi in modo coerente, efficiente e senza interventi manuali.

Vantaggi principali di Trusted Remediator

Di seguito sono riportati i principali vantaggi di Trusted Remediator:

- Maggiore sicurezza, prestazioni e ottimizzazione dei costi: Trusted Remediator consente di migliorare il livello di sicurezza generale degli account, ottimizzare l'utilizzo delle risorse e ridurre i costi operativi.
- Configurazione e configurazione self-service: è possibile configurare Trusted Remediator in base ai propri requisiti e preferenze.
- Correzione automatizzata Trusted Advisor dei controlli e AWS Compute Optimizer delle raccomandazioni: dopo la configurazione, Trusted Remediator esegue automaticamente le azioni di riparazione per i controlli selezionati. Questa automazione elimina la necessità di interventi manuali.

- Implementazione delle migliori pratiche: le azioni correttive si basano su best practice consolidate, quindi i problemi vengono risolti in modo standardizzato ed efficace.
- Esecuzione pianificata: è possibile scegliere il programma di riparazione che si allinea ai flussi di lavoro operativi. day-to-day

Trusted Remediator ti consente di affrontare in modo proattivo i problemi identificati nei tuoi AWS ambienti, aiutandoti a rispettare le migliori pratiche e a mantenere un'infrastruttura cloud sicura, ad alte prestazioni ed economica.

Come funziona Trusted Remediator

Di seguito è riportato un esempio del flusso di lavoro Trusted Remediator:

Trusted Remediator valuta Trusted Advisor e consiglia Compute Optimizer per te e crea. Account AWS AWS Systems Manager OpsItems OpsCenter Quindi, è possibile utilizzare i documenti di automazione Trusted Remediator per rimediare automaticamente o manualmente. OpsItems Di seguito sono riportati i dettagli per ogni tipo di riparazione:

- Riparazione automatica: Trusted Remediator esegue il documento di automazione e monitora l'esecuzione. Una volta completato il documento di automazione, Trusted Remediator risolve l'Opsitem.
- Riparazione manuale: Trusted Remediator crea OpsItem il file da esaminare. Dopo la revisione, puoi creare un RFC automatizzato, Trusted Remediator | Finding | Remediate, modifica il tipo per correggere la risorsa. Per informazioni sulle fasi di riparazione manuale, vedere. Esegui riparazioni manuali in Trusted Remediator

I log di riparazione sono archiviati in un bucket Amazon S3. Puoi utilizzare i dati nel bucket S3 per creare dashboard personalizzati per la reportistica. QuickSight AMS fornisce anche report su richiesta per Trusted Remediator. Per ricevere questi report, contattate il vostro CSDM.

Termini chiave per Trusted Remediator

Di seguito sono riportati i termini che è utile conoscere quando si utilizza Trusted Remediator in AMS:

- AWS Trusted Advisor e AWS Compute Optimizer: servizi di ottimizzazione del cloud forniti da AWS. Trusted Advisor e Compute Optimizer ispezionano AWS l'ambiente e forniscono consigli basati sulle migliori pratiche nelle seguenti sei categorie:

  - Ottimizzazione dei costi
  - Prestazioni
  - Sicurezza
  - Tolleranza ai guasti
  - Eccellenza operativa
  - Limiti del servizio

  Per ulteriori informazioni, consultare AWS Trusted Advisor e AWS Compute Optimizer.

- Trusted Remediator: una soluzione di correzione AMS per controlli e raccomandazioni. Trusted AdvisorAWS Compute Optimizer Trusted Remediator ti aiuta a correggere in sicurezza i Trusted Advisor controlli e le raccomandazioni di Compute Optimizer con le migliori pratiche note per migliorare la sicurezza, le prestazioni e ridurre i costi. Trusted Remediator è facile da configurare e configurare. La configurazione viene effettuata una sola volta e Trusted Remediator esegue le riparazioni secondo la pianificazione preferita (giornaliera o settimanale).
- AWS Systems Manager Documento SSM: un file JSON o YAML che definisce le azioni eseguite sulle risorse. AWS Systems Manager AWS Il documento SSM funge da specifica dichiarativa per automatizzare le attività operative su più risorse e istanze. AWS
- AWS Systems Manager OpsCenter OpsItem: Una risorsa per la gestione dei problemi operativi nel cloud che ti aiuta a tracciare e risolvere i problemi operativi nel tuo ambiente. AWS OpsItems forniscono un sistema di visualizzazione e gestione centralizzato dei dati e dei problemi operativi su tutte Servizi AWS le risorse. Ciascuno di essi OpsItem rappresenta un problema operativo, ad esempio un potenziale rischio per la sicurezza, un problema di prestazioni o un incidente operativo.
- Configurazione: una configurazione è un insieme di attributi memorizzati in AWS AppConfig, una funzionalità di AWS Systems Manager. L'applicazione Trusted Remediator AWS AppConfig aiuta a configurare le riparazioni a livello di account.
- Modalità di esecuzione: la modalità di esecuzione è un attributo di configurazione che determina come eseguire la correzione per ogni Trusted Advisor risultato del controllo. Sono supportate quattro modalità di esecuzione: automatizzata, manuale, condizionale, inattiva.
- Sostituzione delle risorse: questa funzionalità utilizza i tag delle risorse per sovrascrivere una configurazione per risorse specifiche.
- Registro degli elementi di riparazione: un file di registro nel bucket di registro S3 di Trusted Remediator remediation. Il registro degli elementi di riparazione viene creato al momento della creazione della riparazione. OpsItems Questo file di registro contiene la correzione manuale

dell'esecuzione OpsItems e la correzione automatica dell'esecuzione. OpsItems Utilizzate questo file di registro per tenere traccia di tutti gli elementi di riparazione.

- Registro di esecuzione automatizzata della riparazione: un file di registro nel bucket di registro S3 di Trusted Remediator remediation. Il registro di esecuzione automatica della riparazione viene creato al termine dell'esecuzione automatizzata di un documento SSM. Questo registro contiene i dettagli di esecuzione SSM per la correzione automatica dell'esecuzione. OpsItems Utilizza questo file di registro per tenere traccia delle riparazioni automatiche.

Inizia a usare Trusted Remediator in AMS

Trusted Remediator è disponibile in AMS senza costi aggiuntivi. Trusted Remediator supporta configurazioni con account singolo e multiaccount.

Accedere a Trusted Remediator

Per effettuare l'onboarding dei tuoi account AMS su Trusted Remediator, invia un'e-mail ai tuoi Cloud Architect o ai Cloud Service Delivery Manager (). CSDMs Nell'e-mail, includi le seguenti informazioni:

- Account AWS: Il numero identificativo dell'account a dodici cifre. Tutti gli account che desideri aggiungere a Trusted Remediator devono appartenere allo stesso cliente AMS Advanced.
  - Account amministratore delegato: l'account utilizzato per Trusted Advisor controllare la configurazione di Compute Optimizer per uno o più account.
  - Account membro: questi sono gli account collegati all'account amministratore delegato. Questi account ereditano le configurazioni dall'account amministratore delegato. È possibile avere uno o più account membro.

    > **Note**
    >
    > Gli account membro ereditano le configurazioni dall'account amministratore delegato. Se hai bisogno di configurazioni diverse per account specifici, esegui l'onboarding di più account amministratore delegato con le tue configurazioni preferite. Pianifica la struttura dell'account e le configurazioni con i tuoi Cloud Architects prima di iniziare.

- Regione AWS: Il Regione AWS luogo in cui si trovano le tue risorse. Per un elenco di Regioni AWS, vedi Servizi AWS per regione.
- Pianificazione e orario di riparazione: il tuo programma di riparazione preferito (giornaliero o settimanale). Trusted Remediator raccoglie Trusted Advisor i controlli e avvia la riparazione all'ora

pianificata. Ad esempio, è possibile impostare il programma di riparazione per l'1:00 di domenica di ogni settimana, ora solare dell'Australia orientale.

- E-mail di notifica: Trusted Remediator utilizza l'e-mail di notifica per avvisarti quotidianamente in caso di correzioni. L'oggetto dell'e-mail di notifica è «Riepilogo delle riparazioni di Trusted Remediator» e il contenuto fornisce informazioni sulle riparazioni di Trusted Remediator eseguite nelle ultime 24 ore.

> **Note**
>
> Esaminate le applicazioni e le risorse dopo ogni riparazione pianificata. Per ulteriore assistenza, contatta AMS.

Dopo aver inviato la richiesta di onboard con i dettagli richiesti alla CA o al CSDM, AMS effettua l'onboarding dei tuoi account su Trusted Remediator. Trusted Remediator utilizza AWS AppConfig, una funzionalità di AWS Systems Manager, per definire la configurazione per i controlli. Trusted Advisor Queste configurazioni sono un insieme di attributi che vengono memorizzati in. AWS AppConfig Per evitare addebiti non autorizzati alle risorse, tutti i Trusted Advisor controlli supportati sono impostati su Inattivo quando gli account vengono registrati su Trusted Remediator. Queste configurazioni consentono di correggere automaticamente Trusted Advisor controlli specifici o di valutare e correggere manualmente i controlli rimanenti. Le configurazioni sono altamente personalizzabili e consentono di applicare configurazioni per ogni controllo. Trusted Advisor Per ulteriori informazioni, consulta Configurare Trusted Advisor la correzione degli assegni in Trusted Remediator.

Configura Trusted Remediator nel tuo Account AWS

Una volta completata l'onboarding, la CA o il CDSM invia una notifica all'utente e le configurazioni predefinite vengono create nell'amministratore delegato. Account AWS La configurazione viene archiviata nell'applicazione Trusted Remediator. AWS AppConfig È possibile utilizzare RFC Management | Trusted Remediator | Remediation configuration | Update per richiedere aggiornamenti della configurazione. Per ulteriori informazioni, consulta Configurare Trusted Advisor la correzione degli assegni in Trusted Remediator.

Per visualizzare le configurazioni predefinite di Trusted Remediator, completa i seguenti passaggi:

1. Apri la AWS Systems Manager console all'indirizzo. https://console.aws.amazon.com/systems-manager/

> **Note**
>
> Assicurati di utilizzare l'account amministratore delegato.

2. Scegli Gestione delle applicazioni, AppConfig.
3. Seleziona Trusted Remediator dall'elenco delle applicazioni.

Di seguito è riportato un esempio di AWS AppConfig console che mostra le configurazioni di Trusted Remediator:

Scegli i controlli e i consigli per rimediare

Per impostazione predefinita, la modalità di esecuzione della riparazione è inattiva per tutti i Trusted Advisor controlli e le raccomandazioni di Compute Optimizer nella configurazione. In questo modo si evitano riparazioni non autorizzate e si proteggono le risorse. AMS fornisce documenti di automazione SSM selezionati per la correzione degli assegni. Trusted Advisor

Per selezionare i controlli a cui desideri correggere con Trusted Remediator, completa i seguenti passaggi:

1. Consulta l'elenco dei consigli supportati Trusted Advisor e di Compute Optimizer o il nome dei documenti di automazione SSM associati per decidere quali controlli e consigli desideri correggere con Trusted Remediator.
2. Invia una richiesta di gestione | Trusted Remediator | Remediation | Update per aggiornare la configurazione per i controlli selezionati. Trusted Advisor Per istruzioni su come selezionare i controlli, vedere. Configurare Trusted Advisor la correzione degli assegni in Trusted Remediator

Tieni traccia delle tue riparazioni in Trusted Remediator

Dopo aver aggiornato la configurazione a livello di account, Trusted Remediator crea per ogni correzione. OpsItems Trusted Remediator esegue il documento SSM per la riparazione automatica in base al programma di riparazione. OpsItems Per istruzioni su come visualizzare tutte le riparazioni OpsItems dalla OpsCenter console Systems Manager, vedereTieni traccia delle riparazioni in Trusted Remediator.

Esegui riparazioni manuali in Trusted Remediator

È possibile correggere manualmente i Trusted Advisor controlli utilizzando un RFC automatizzato. Quando si sceglie la riparazione manuale, Trusted Remediator crea un'esecuzione manuale. OpsItem Per ulteriori informazioni, consulta Esegui riparazioni manuali in Trusted Remediator.

Raccomandazioni di Compute Optimizer supportate da Trusted Remediator

La tabella seguente elenca i consigli supportati da Compute Optimizer, i documenti di automazione SSM, i parametri preconfigurati e il risultato previsto dei documenti di automazione. Esamina il risultato previsto per aiutarti a comprendere i possibili rischi in base ai requisiti aziendali prima di abilitare un documento di automazione SSM per la correzione degli assegni.

Assicurati che la regola di configurazione corrispondente per ogni controllo di Compute Optimizer sia presente per i controlli supportati per i quali desideri abilitare la correzione. Per ulteriori informazioni, consulta Optare per i controlli. AWS Compute Optimizer Trusted Advisor

Opzione di ottimizzazione	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Corretto dimensionamento		
Consigli sulle EC2 istanze Amazon	AWSManagedServices-TrustedRemediatorResizeInstanceByComputeOptimizerRecommendation Tipo di EC2 istanza Amazon aggiornato in base ai consigli di Compute Optimizer. Le opzioni più ottimali vengono scelte mantenendo gli stessi parametri della piattaforma (architettura, hypervisor, interfaccia di rete, tipo di virtualizzazione e così via), se l'opzione esiste.	• MinimumDaysSinceLastChange: Il parametro per specificare il numero minimo di giorni dall'ultima modifica del tipo di istanza. L'impostazione di default è 7 giorni. Nessun vincolo • Crea AMIBefore ridimensionamento: per creare l'AMI dell'istanza come backup prima del ridimensionamento, imposta su «True». Per non creare un backup, imposta su «False». L'impostazione predefinita è «True». Nessun vincolo

Opzione di ottimizzazione	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Raccomand azioni sui volumi di Amazon EBS	AWSManagedServices-ModifyEB SVolume Il volume Amazon EBS viene modificato in base alle raccomand azioni di Compute Optimizer. La modifica può includere il tipo di volume, la dimensione, gli IOPS, la generazione del volume (gp2, gp3 ecc.).	• CreateSnapshot: per creare un'istantanea prima di modificare il volume, imposta su 'True. ' Per non creare un'istantanea, imposta su «False». L'impostazione predefinita è «True». Nessun vincolo • VolumeType: Il tipo di volume desiderato. Se non viene specifica to alcun tipo, viene mantenuto il tipo esistente. Nessun vincolo • VolumeSize: la dimensione desiderata del volume, in GiB. La dimensione del volume di destinazi one deve essere maggiore o uguale alla dimensione esistente del volume. Se non viene specifica ta alcuna dimensione, viene mantenuta la dimensione esistente . Nessun vincolo • Iops: il numero richiesto di I/O operazioni al secondo (IOPS). Questo parametro è valido solo per i volumi io1, io2 e gp3. Nessun vincolo • Throughput: la velocità effettiva necessaria per il provisioning di un volume, con un massimo di 1000

Opzione di ottimizzazione	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		MiB/s. Questo parametro è valido solo per i volumi gp3. Nessun vincolo • RemediateStackDrift: Per avviare la correzione della deriva, se una deriva è causata dalla modifica del volume, imposta su 'True. ' Per non tentare di correggere la deriva, imposta su «False». L'imposta zione predefinita è «True». Nessun vincolo
Raccomand azioni sulla funzione Lambda	AWSManagedServices-TrustedR emediatorOptimizeLambdaMemory AWS Lambda memoria delle funzioni ottimizzata secondo le raccomand azioni di Compute Optimizer.	RecommendedMemorySize : dimensione della memoria personali zzata, se diversa dalle opzioni consigliate. Nessun vincolo
Risorse inattive		

Opzione di ottimizzazione	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Volume Amazon EBS inattivo	AWSManagedServices-DeleteUnusedEBSVolume Il volume Amazon EBS non collegato verrà eliminato.	• CreateSnapshot: per creare un'istantanea prima di eliminare il volume, imposta su «True». Per non creare un'istantanea, imposta su «False». L'impostazione predefinita è «True». Nessun vincolo • MinimumUnattachedDays: minimo giorni non collegati del volume Amazon EBS da eliminare, fino a 62 giorni. L'impostazione predefinita è 7. Nessun vincolo
Istanza Amazon EC2 inattiva	AWSManagedServices-StopECIstanza 2 L' EC2 istanza Amazon inattiva verrà interrotta.	ForceStopWithInstanceStore: per forzare l'interruzione delle istanze che utilizzano instance store, imposta su «True». Per non forzare l'arresto, imposta su «False». Il valore predefinito 'False' impedisce l'arresto dell'istanza. Nessun vincolo

Opzione di ottimizzazione	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Istanza Amazon RDS inattiva	AWSManagedServices-StopIdle RDSInstance Interrompi un'istanza Amazon RDS inattiva. I motori supportati sono: MariadB, Microsoft SQL Server, MySQL, Oracle, PostgreSQL. Questo documento non si applica ad Aurora MySQL e Aurora PostgreSQL. L'istanza verrà interrotta per un massimo di 7 giorni e riavviata automaticamente.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Trusted Advisor controlli supportati da Trusted Remediator

La tabella seguente elenca i Trusted Advisor controlli supportati, i documenti di automazione SSM, i parametri preconfigurati e il risultato previsto dei documenti di automazione. Esamina il risultato previsto per aiutarti a comprendere i possibili rischi in base ai requisiti aziendali prima di abilitare un documento di automazione SSM per la correzione degli assegni.

Assicurati che la regola di configurazione corrispondente per ogni Trusted Advisor controllo sia presente per i controlli supportati per i quali desideri abilitare la correzione. Per ulteriori informazioni, consulta View AWS Trusted Advisor checks powered by. AWS Config Se un controllo ha AWS Security Hub CSPM i controlli corrispondenti, assicurati che il controllo Security Hub sia abilitato. Per ulteriori informazioni, vedere Abilitazione dei controlli in Security Hub. Per informazioni sulla gestione dei parametri preconfigurati, vedere Configurare la correzione dei controlli di Trusted Advisor in Trusted Remediator.

Trusted Advisor controlli di ottimizzazione dei costi supportati da Trusted Remediator

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Z4 AUBRNSmz Indirizzi IP elastici non associati	AWSManagedServices-TrustedRemediatorReleaseElasticIP Rilascia un indirizzo IP elastico che non è associato a nessuna risorsa.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c18d2gz150 - Istanze Amazon interrotte EC2	AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime - EC2 Le istanze Amazon interrotte per un certo numero di giorni vengono terminate.	• Crea AMIBefore terminazione: per creare l'AMI dell'istanza come backup prima di terminare l' EC2 istanza Amazon, scegli. `true` Per non creare un backup prima della chiusura, scegli. `false` Il valore predefinito è `true`. • AllowedDays: il numero di giorni in cui l'istanza si trova nello stato di arresto prima che venga terminata. Il valore predefinito è 30. Nessun vincolo
c18d2gz128 Repository di Amazon ECR senza policy del ciclo di vita configurata	AWSManagedServices-TrustedRemediatorPutECRLifecyclePolicy Crea una politica del ciclo di vita per il repository specificato se non esiste già una politica del ciclo di vita.	ImageAgeLimit: il limite di età massimo in giorni (1-365) per «qualsiasi» immagine nell'archivio Amazon ECR. Nessun vincolo
DAvU99Dc4C Volumi Amazon EBS sottoutilizzati	AWSManagedServices-DeleteUnusedEBSVolume Elimina i volumi Amazon EBS sottoutilizzati se i volumi non sono	• CreateSnapshot: se impostato `sutrue`, l'automazione crea uno snapshot del volume Amazon EBS prima che venga eliminato

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
	collegati negli ultimi 7 giorni. Per impostazione predefinita, viene creata una snapshot di Amazon EBS.	. L'impostazione predefinita è `true`. I valori validi sono `true` e `false` (distinzione tra maiuscole e minuscole). • MinimumUnattachedDays: minimo giorni non allegati del volume EBS da eliminare, fino a 62 giorni. Se impostato su`0`, il documento SSM non verifica il periodo non allegato ed elimina il volume se il volume non è attualmente allegato. Il valore predefinito è. 7 Nessun vincolo
ciao M8 LMh88u Bilanciatori del carico inattivi	AWSManagedServices-DeleteId leClassicLoadBalancer Elimina un Classic Load Balancer inattivo se è inutilizzato e non è registrata alcuna istanza.	IdleLoadBalancerDays: Il numero di giorni in cui il Classic Load Balancer ha 0 connessioni richieste prima di considerarlo inattivo. L'impostazione predefinita è sette giorni. Se l'esecuzione automatica è abilitata , l'automazione elimina i Classic Load Balancer inattivi se non ci sono istanze di back-end attive. Per tutti i Classic Load Balancer inattivi che dispongono di istanze di back-end attive, ma non dispongono di istanze di back-end sane, la riparazione automatica non viene utilizzata e viene creata la riparazione manuale. OpsItems

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
TI39 Half U8 Istanze database Amazon RDS inattive	AWSManagedServices-StopIdleRDSInstance L'istanza database di Amazon RDS che è rimasta inattiva negli ultimi sette giorni viene interrotta.	Non sono consentiti parametri preconfigurati. Nessun vincolo
COr6dfpM05 AWS Lambda funzioni sovradimensionate per le dimensioni della memoria	AWSManagedServices-ResizeLambdaMemory AWS Lambda la dimensione della memoria della funzione viene ridimensionata alla dimensione di memoria consigliata fornita da. Trusted Advisor	RecommendedMemorySize: l'allocazione di memoria consigliata per la funzione Lambda. L'intervallo di valori è compreso tra 128 e 10240. Se la dimensione della funzione Lambda è stata modificata prima dell'esecuzione dell'automazione, le impostazioni potrebbero essere sovrascritte da questa automazione con il valore consigliato da. Trusted Advisor
QCh7DWoux1 Istanze Amazon EC2 a basso utilizzo	AWSManagedServices-StopEC2Instance (documento SSM predefinito per la modalità di esecuzione automatica e manuale). EC2 Le istanze Amazon con basso utilizzo vengono interrotte.	ForceStopWithInstanceStore: impostato su per `true` forzare l'arresto delle istanze utilizzando instance store. In caso contrario, imposta il valore su `false`. Il valore predefinito di `false` impedisce l'arresto dell'istanza. I valori validi sono true o false (distinzione tra maiuscole e minuscole). Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
QCH7DWoux1 Istanze Amazon EC2 a basso utilizzo	AWSManagedServices-ResizeInstanceByOneLevel L' EC2 istanza Amazon viene ridimensionata di un tipo di istanza nello stesso tipo di famiglia di istanze. L'istanza viene interrotta e avviata durante l'operazione di ridimensionamento e riportata allo stato iniziale al termine dell'esecuzione del documento SSM. Questa automazione non supporta il ridimensionamento delle istanze che si trovano in un gruppo di Auto Scaling.	• MinimumDaysSinceLastChange: numero minimo di giorni dall'ultima modifica del tipo di istanza. Se il tipo di istanza è stato modificato entro un periodo di tempo specificato, il tipo di istanza non viene modificato. `0`Utilizzatelo per saltare questa convalida. Il valore predefinito è 7. • Crea AMIBefore ridimensionamento: per creare l'AMI dell'istanza come backup prima del ridimensionamento, scegli. `true` Per non creare un backup, scegli. `false` Il valore predefinito è `false`. I valori validi sono `true` e `false` (distinzione tra maiuscole e minuscole). • ResizeIfStopped: Per procedere con la modifica delle dimensioni dell'istanza, anche se l'istanza è in uno stato interrotto, scegliete . `true` Per non ridimensionare automaticamente l'istanza se si trova in uno stato interrotto, sceglietefalse. I valori validi sono `true` e `false` (distinzione tra maiuscole e minuscole). Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
QCH7DWoux1 Istanze Amazon EC2 a basso utilizzo	AWSManagedServices-TerminateInstance Le EC2 istanze Amazon a basso utilizzo vengono terminate se non fanno parte di un gruppo di Auto Scaling e la protezione dalla terminazione non è abilitata. Per impostazione predefinita, viene creata un'AMI.	Crea AMIBefore terminazione: imposta questa opzione su `true` o per `false` creare un'AMI di istanza come backup prima di terminare l' EC2 istanza. Il valore predefinito è `true`. I valori validi sono `true` e `false` (distinzione tra maiuscole e minuscole). Nessun vincolo
G31sq1e9u Cluster Amazon Redshift sottoutilizzati	AWSManagedServices-PauseRedshiftCluster Il cluster Amazon Redshift è in pausa.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1cj39rr6v Configurazione di interruzione del caricamento multiparte incompleta di Amazon S3	AWSManagedServices-TrustedRemediatorEnableS3AbortIncompleteMultipartUpload Il bucket Amazon S3 è configurato con una regola del ciclo di vita per interrompere i caricamenti in più parti che rimangono incompleti dopo determinati giorni.	DaysAfterInitiation: il numero di giorni dopo i quali Amazon S3 interrompe un caricamento incompleto in più parti. L'impostazione predefinita è 7 giorni. Nessun vincolo
c1z7kmr00n Consigli di Amazon per l'ottimizzazione dei EC2 costi per le istanze	Utilizza i consigli sulle EC2 istanze Amazon e l' EC2 istanza Amazon inattiva diRaccomandazioni di Compute Optimizer supportate da Trusted Remediator.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c1z7kmr02n Raccomandazioni per l'ottimizzazione dei costi di Amazon EBS per i volumi	Utilizza i consigli sui volumi Amazon EBS e il volume Amazon EBS inattivo di. Raccomandazioni di Compute Optimizer supportate da Trusted Remediator	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1z7kmr03n Consigli per l'ottimizzazione dei costi di Amazon RDS per le istanze DB	Usa l'istanza Amazon RDS inattiva di. Raccomandazioni di Compute Optimizer supportate da Trusted Remediator	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1z7kmr05n AWS Lambda raccomandazioni per l'ottimizzazione dei costi per le funzioni	Utilizza i consigli sulla funzione Lambda di. Raccomandazioni di Compute Optimizer supportate da Trusted Remediator	Non sono consentiti parametri preconfigurati. Nessun vincolo

Trusted Advisor controlli di sicurezza supportati da Trusted Remediator

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
12Fnkpl8Y5 Exposed Access Keys	AWSManagedServices-TrustedRemediatorDeactivateIAMAccessKey La chiave di accesso IAM esposta è disattivata.	Non sono consentiti parametri preconfigurati.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		Le applicazioni configurate con una chiave di accesso IAM esposta non possono autenticarsi.
Hs4Ma3G127 - API Gateway REST WebSocket e la registrazione dell'esecuzione dell'API devono essere abilitati Controllo corrispondente AWS Security Hub CSPM APIGateway: 1.	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging La registrazione dell'esecuzione è abilitata nella fase API.	LogLevel: Livello di registrazione per abilitare la registrazione dell'esecuzione, `ERROR` - La registrazione è abilitata solo per gli errori. `INFO` - La registrazione è abilitata per tutti gli eventi. Devi concedere ad API Gateway l'autorizzazione a leggere e scrivere i log del tuo account CloudWatch per abilitare il log di esecuzione. Per maggiori dettagli, consulta CloudWatch Configurare la registrazione per REST APIs in API Gateway.
Hs4Ma3G129 - Le fasi API REST API Gateway dovrebbero avere la traccia abilitata AWS X-Ray Controllo corrispondente AWS Security Hub CSPM APIGateway: 3.	AWSManagedServices-EnableApiGateWayXRayTracing Il tracciamento X-Ray è abilitato nella fase API.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G202 - I dati della cache dell'API REST API Gateway devono essere crittografati a riposo Controllo APIGatewaycorrispondente AWS Security Hub CSPM: 5.	AWSManagedServices-EnableAPIGatewayCacheEncryption Abilita la crittografia a riposo per i dati della cache dell'API REST di API Gateway se la fase API REST di API Gateway ha la cache abilitata.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G177 - AWS Security Hub CSPM Controllo corrispondente: i gruppi di scalabilità automatica associati a un sistema di bilanciamento del carico devono utilizzare i controlli dello stato del bilanciamento del carico .1 AutoScaling	AWSManagedServices-TrustedRemediatorEnableAutoScalingGroupELBHealthCheck I controlli dello stato di Elastic Load Balancing sono abilitati per il gruppo Auto Scaling.	HealthCheckGracePeriod: la quantità di tempo, in secondi, che Auto Scaling attende prima di verificare lo stato di integrità di un'istanza Amazon Elastic Compute Cloud entrata in servizio. L'attivazione dei controlli di integrità di Elastic Load Balancing potrebbe comportare la sostituzione di un'istanza in esecuzione se uno dei sistemi di bilanciamento del carico Elastic Load Balancing collegati al gruppo Auto Scaling la segnala come non integra. Per ulteriori informazioni, consulta Collegare un sistema di bilanciamento del carico Elastic Load Balancing al gruppo Auto Scaling

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G245: gli CloudFormation stack devono essere integrati con Amazon Simple Notification Service Controllo corrispondente AWS Security Hub CSPM : 1. CloudFormation	AWSManagedServices-EnableCFNStackNotification Associa uno CloudFormation stack a un argomento di Amazon SNS per la notifica.	NotificaARNs: gli argomenti ARNs di Amazon SNS da associare a stack selezionati CloudFormation . Per abilitare la riparazione automatica, è necessario fornire il parametro `NotificationARNs` preconfigurato.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G210: le distribuzioni devono avere la registrazione abilitata CloudFront Controllo corrispondente AWS Security Hub CSPM : CloudFront2.	AWSManagedServices-EnableCloudFrontDistributionLogging La registrazione è abilitata per le CloudFront distribuzioni Amazon.	• BucketName: il nome del bucket Amazon S3 in cui desideri archiviare i log di accesso. • S3KeyPrefix: il prefisso per la posizione nel bucket S3 per i log di distribuzione di Amazon. CloudFront • IncludeCookies: Indica se includere i cookie nei log di accesso. Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati: • BucketName • S3KeyPrefix • IncludeCookies Per informazioni su questi vincoli di correzione, vedi Come posso attivare la registrazione per la mia distribuzione? CloudFront

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G109: la convalida del file di registro deve essere abilitata CloudTrail Controllo corrispondente AWS Security Hub CSPM : CloudTrail.4	AWSManagedServices-TrustedRemediatorEnableCloudTrailLogValidation Abilita la convalida del registro delle CloudTrail tracce.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G108: i CloudTrail trail devono essere integrati con Amazon Logs CloudWatch Controllo corrispondente AWS Security Hub CSPM CloudTrail: 5.	AWSManagedServices-IntegrateCloudTrailWithCloudWatch AWS CloudTrail è integrato con CloudWatch Logs.	• CloudWatchLogsLogGroupName: nome del gruppo di CloudWatch log Logs a cui vengono CloudTrail consegnati i log. Devi utilizzare un gruppo di log esistente nel tuo account. • CloudWatchLogsRoleName: nome del ruolo IAM che l'endpoint CloudWatch Logs deve assumere per scrivere nel gruppo di log di un utente. Devi utilizzare un ruolo esistente nel tuo account. Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati: • CloudWatchLogsLogGroupName • CloudWatchLogsRoleName

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G217: gli ambienti di progetto devono avere una configurazione di registrazione CodeBuild AWS Controllo corrispondente AWS Security Hub CSPM CodeBuild: 4.	AWSManagedServices-TrustedRemediatorEnableCodeBuildLoggingConfig Abilita la registrazione del progetto. CodeBuild	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G306 - I cluster Neptune DB devono avere la protezione da eliminazione abilitata AWS Security Hub CSPM Controllo corrispondente: DocumentDB.3	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnDocumentDBSnapshot Rimuove l'accesso pubblico dallo snapshot manuale del cluster di Amazon DocumentDB.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G308 - I cluster Amazon DocumentDB devono avere la protezione da eliminazione abilitata AWS Security Hub CSPM Controllo corrispondente: DocumentDB.5	AWSManagedServices-TrustedRemediatorEnableDocumentDBClusterDeletionProtection Abilita la protezione da eliminazione per il cluster Amazon DocumentDB.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G323 - Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata AWS Security Hub CSPM Controllo corrispondente: DynamoDB.6	AWSManagedServices-TrustedRemediatorEnableDynamoDBTableDeletionProtection Abilita la protezione dall'eliminazione per le tabelle DynamoDB non AMS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
EPS02jt06w - Istantanee pubbliche di Amazon EBS	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnEBSSnapshot L'accesso pubblico per lo snapshot di Amazon EBS è disabilitato.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G118 - I gruppi di sicurezza predefiniti VPC non devono consentire il traffico in entrata o in uscita Controllo corrispondente AWS Security Hub CSPM : 2. EC2	AWSManagedServices-TrustedRemediatorRemoveAllRulesFromDefaultSG Tutte le regole di ingresso e uscita nel gruppo di sicurezza predefinito vengono rimosse.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G117 - I volumi EBS collegati devono essere crittografati a riposo Controllo corrispondente AWS Security Hub CSPM EC2: .3	AWSManagedServices-EncryptInstanceVolume Il volume Amazon EBS collegato all'istanza è crittografato.	• KMSKeyId: ID AWS KMS chiave o ARN per crittografare il volume. • DeleteStaleNonEncryptedSnapshotBackups: Un flag che decide se eliminare il backup istantaneo dei vecchi volumi non crittografati. L'istanza viene riavviata come parte della riparazione e il rollback è possibile se `DeleteStaleNonEncryptedSnapshotBackups` è impostato su, il che facilita il ripristino. `false`

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G120 - Le istanze interrotte EC2 devono essere rimosse dopo un periodo di tempo specificato Controllo corrispondente AWS Security Hub CSPM EC2: 4.	AWSManagedServices-TerminateInstance(documento SSM predefinito per la modalità di esecuzione automatica e manuale) EC2 Le istanze Amazon interrotte per 30 giorni vengono terminate.	Crea AMIBefore terminazione:. Per creare l'AMI dell'istanza come backup prima di terminare l' EC2 istanza, scegli`true`. Per non creare un backup prima della chiusura, scegli. `false` Il valore predefinito è `true`. Nessun vincolo
Hs4Ma3G120 - Le EC2 istanze arrestate devono essere rimosse dopo un periodo di tempo specificato Controllo corrispondente AWS Security Hub CSPM EC2: 4.	AWSManagedServices-TerminateEC2 InstanceStoppedForPeriodOfTime - EC2 Le istanze Amazon interrotte per il numero di giorni definito in Security Hub (il valore predefinito è 30) vengono terminate.	Crea AMIBefore terminazione: per creare l'AMI dell'istanza come backup prima di terminare l' EC2 istanza, scegli. `true` Per non creare un backup prima della chiusura, scegli. `false` Il valore predefinito è `true`. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G121 - La crittografia predefinita di EBS deve essere abilitata Controllo corrispondente AWS Security Hub CSPM : EC27.	AWSManagedServices-EncryptEBSByDefault La crittografia Amazon EBS per impostazione predefinita è abilitata per lo specifico Regione AWS	Non sono consentiti parametri preconfigurati. La crittografia predefinita è un'impostazione specifica della regione. Se lo abiliti per una regione, non puoi disabilitarlo per singoli volumi o istantanee in quella regione.
Hs4Ma3G124 - Le istanze EC2 Amazon devono utilizzare Instance Metadata Service versione 2 () IMDSv2 Controllo EC2corrispondente AWS Security Hub CSPM : 8.	AWSManagedServices-TrustedRemediatorAbilita istanza EC2 IMDSv2 EC2 Le istanze Amazon utilizzano Instance Metadata Service versione 2 ()IMDSv2.	• IMDSv1MetricCheckPeriod: Il numero di giorni (`42-455`) in cui analizzare i parametri di IMDSv1 utilizzo. CloudWatch Se l' EC2 istanza Amazon è stata creata entro il periodo di tempo specificato, l'analisi inizia dalla data di creazione dell'istanza. • HttpPutResponseHopLimit: Il numero massimo di hop di rete consentiti per il token di metadati dell'istanza. Questo valore può essere configurato tra 1 e 2 hops. Un limite hop 1 limita l'accesso tramite token ai processi in esecuzione direttamente sull'istanza, mentre un limite hop 2 consente l'accesso dai contenitori in esecuzione sull'istanza. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G207: le EC2 sottoreti non devono assegnare automaticamente indirizzi IP pubblici Controllo corrispondente AWS Security Hub CSPM : EC2.15	AWSManagedServices-UpdateAutoAssignPublicIpv4 indirizzi Le sottoreti VPC sono configurate per non assegnare automaticamente indirizzi IP pubblici.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G209 - Gli elenchi di controllo degli accessi alla rete non utilizzati vengono rimossi Controllo corrispondente AWS Security Hub CSPM : EC2.16	AWSManagedServices-DeleteUnusedNACL Eliminare l'ACL di rete non utilizzato	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G215 - I gruppi di sicurezza Amazon EC2 non utilizzati devono essere rimossi Controllo corrispondente AWS Security Hub CSPM : EC2.22	AWSManagedServices-DeleteSecurityGroups Eliminare i gruppi di sicurezza non utilizzati.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G247 - Amazon Transit EC2 Gateway non dovrebbe accettare automaticamente richieste di allegati VPC Controllo corrispondente AWS Security Hub CSPM EC2: .23	AWSManagedServices-TrustedRemediatorDisableTGWAutoVPCAttach- Disattiva l'accettazione automatica delle richieste di allegati VPC per l'Amazon Transit EC2 Gateway non AMS specificato.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G235 - I repository privati ECR dovrebbero avere l'immutabilità dei tag configurata Controllo corrispondente AWS Security Hub CSPM : ECR.2	AWSManagedServices-TrustedRemediatorSetImageTagImmutability Imposta le impostazioni di mutabilità del tag di immagine su IMMUTABLE per il repository specificato.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G216 - I repository ECR devono avere almeno una politica del ciclo di vita configurata Controllo corrispondente AWS Security Hub CSPM : ECR.3	AWSManagedServices-PutECRRepositoryLifecyclePolicy L'archivio ECR ha una politica del ciclo di vita configurata.	LifecyclePolicyText: Il testo della politica del repository JSON da applicare al repository. Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati: LifecyclePolicyText

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G325 - I cluster EKS devono avere la registrazione di controllo abilitata Controllo corrispondente AWS Security Hub CSPM : EKS.8	AWSManagedServices-TrustedRemediatorEnableEKSAuditLog Il registro di controllo è abilitato per il cluster EKS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G183 - Il bilanciamento del carico delle applicazioni deve essere configurato per eliminare le intestazioni HTTP Controllo corrispondente AWS Security Hub CSPM : ELB.4	AWSConfigRemediation-DropInvalidHeadersForALB Application Load Balancer è configurato per campi di intestazione non validi.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G184 - La registrazione di Application Load Balancer e Classic Load Balancers deve essere abilitata Controllo corrispondente AWS Security Hub CSPM : ELB.5	AWSManagedServices-EnableELBLogging (documento SSM predefinito per la modalità di esecuzione automatica e manuale) La registrazione di Application Load Balancer e Classic Load Balancer è abilitata.	• BucketName: il nome del bucket (non l'ARN). Assicurati che la policy del bucket sia configurata correttamente per la registrazione. • S3KeyPrefix: il prefisso per la posizione nel bucket Amazon S3 per i log Elastic Load Balancing. Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati: • BucketName • S3KeyPrefix Il bucket Amazon S3 deve disporre di una policy relativa ai bucket che conceda a Elastic Load Balancing l'autorizzazione a scrivere i log di accesso al bucket.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G184 - La registrazione di Application Load Balancers e Classic Load Balancers deve essere abilitata Controllo corrispondente AWS Security Hub CSPM : ELB.5	AWSManagedServices-EnableELBLoggingV2 La registrazione di Application Load Balancer e Classic Load Balancer è abilitata.	• TargetBucketTagKey: il nome del tag (con distinzione tra maiuscole e minuscole) utilizzato per identificare il bucket Amazon S3 di destinazione. Usalo insieme `TargetBucketTagValue` per etichettare il bucket che fungerà da bucket di destinazione per la registrazione degli accessi. • TargetBucketTagValue: il valore del tag (con distinzione tra maiuscole e minuscole) utilizzato per identificare il bucket Amazon S3 di destinazione. Usalo insieme `TargetBucketTagKey` per etichettare il bucket che fungerà da bucket di destinazione per la registrazione degli accessi. • S3BucketPrefix: il prefisso (gerarchia logica) per il bucket Amazon S3. Il prefisso specificato non deve includere la stringa `AWSLogs`. Per ulteriori informazioni, consulta Organizzazione degli oggetti utilizzando i prefissi. Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati: • TargetBucketTagKey • TargetBucketTagValue • S3BucketPrefix

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		Il bucket Amazon S3 deve disporre di una policy relativa ai bucket che conceda a Elastic Load Balancing l'autorizzazione a scrivere i log di accesso al bucket.
Hs4Ma3G326 - L'impostazione di accesso pubblico a blocchi di Amazon EMR deve essere abilitata AWS Security Hub CSPM Controllo corrispondente: EMR.2	AWSManagedServices-TrustedRemediatorEnableEMRBlockPublicAccess Le impostazioni di accesso pubblico a blocchi di Amazon EMR sono attivate per l'account.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G135: le chiavi non devono essere cancellate involontariamente AWS KMS Controllo corrispondente AWS Security Hub CSPM : KMS.3	AWSManagedServices-CancelKeyDeletion AWS KMS l'eliminazione della chiave viene annullata.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G299 - Le istantanee manuali dei cluster di Amazon DocumentDB non devono essere pubbliche AWS Security Hub CSPM Controllo corrispondente: Neptune.4	AWSManagedServices-TrustedRemediatorEnableNeptuneDBClusterDeletionProtection Abilita la protezione da eliminazione per il cluster Amazon Neptune.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G319 - I firewall Network Firewall devono avere la protezione da eliminazione abilitata Controllo corrispondente AWS Security Hub CSPM NetworkFirewall: 9.	AWSManagedServices-TrustedRemediatorEnableNetworkFirewallDeletionProtection- Abilita la protezione da eliminazione per AWS Network Firewall.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G223: i domini devono crittografare i dati inviati tra i nodi OpenSearch Controllo corrispondente AWS Security Hub CSPM : OpenSearch.3	AWSManagedServices-EnableOpenSearchNodeToNodeEncryption La crittografia da nodo a nodo è abilitata per il dominio.	Non sono consentiti parametri preconfigurati. Dopo aver abilitato la node-to-node crittografia, non è possibile disabilitare l'impostazione. Invece, scatta un'istantanea manuale del dominio crittografato, crea un altro dominio, migra i dati e quindi elimina il vecchio dominio.
Hs4Ma3G222: la registrazione degli errori del OpenSearch dominio nei registri deve essere abilitata CloudWatch Controllo corrispondente AWS Security Hub CSPM : Opensearch.4	AWSManagedServices-EnableOpenSearchLogging La registrazione degli errori è abilitata per il dominio. OpenSearch	CloudWatchLogGroupArn: L'ARN di un gruppo di log di Amazon CloudWatch Logs. Per abilitare la riparazione automatica, è necessario fornire il seguente parametro preconfigurato:. CloudWatchLogGroupArn La politica CloudWatch delle risorse di Amazon deve essere configurata con le autorizzazioni. Per ulteriori informazioni, consulta la sezione Abilitazione dei log di controllo nella Amazon OpenSearch Service User Guide.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G221: i domini devono avere la registrazione di controllo OpenSearch abilitata Controllo corrispondente AWS Security Hub CSPM : Opensearch.5	AWSManagedServices-EnableOpenSearchLogging OpenSearch i domini sono configurati con la registrazione di controllo abilitata.	CloudWatchLogGroupArn: L'ARN del gruppo CloudWatch Logs in cui pubblicare i log. Per abilitare la riparazione automatica, è necessario fornire il seguente parametro preconfigurato: CloudWatchLogGroupArn La politica CloudWatch delle risorse di Amazon deve essere configurata con le autorizzazioni. Per ulteriori informazioni, consulta la sezione Abilitazione dei log di controllo nella Amazon OpenSearch Service User Guide.
Hs4Ma3G220 - Le connessioni ai OpenSearch domini devono essere crittografate utilizzando TLS 1.2 Controllo corrispondente AWS Security Hub CSPM : Opensearch.8	AWSManagedServices-EnableOpenSearchEndpointEncryptionTLS1.2 La politica TLS è impostata su `Policy-min-TLS-1-2-2019-07` e sono consentite solo le connessioni crittografate tramite HTTPS (TLS).	Non sono consentiti parametri preconfigurati. Le connessioni ai OpenSearch domini sono necessarie per utilizzare TLS 1.2. La crittografia dei dati in transito può influire sulle prestazioni. Testa le tue applicazioni con questa funzionalità per comprendere il profilo delle prestazioni e l'impatto del TLS.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G194 - Lo snapshot di Amazon RDS deve essere privato Controllo corrispondente AWS Security Hub CSPM : RDS.1	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 L'accesso pubblico per lo snapshot di Amazon RDS è disabilitato.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G192 - Le istanze DB RDS dovrebbero vietare l'accesso pubblico, come determinato dalla configurazione PubliclyAccessible AWS Controllo corrispondente AWS Security Hub CSPM : RDS.2	AWSManagedServices-TrustedRemediatorDisablePublicAccessOnRDSInstance Disabilita l'accesso pubblico sull'istanza DB RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G189 - Il monitoraggio avanzato è configurato per le istanze DB di Amazon RDS Controllo corrispondente AWS Security Hub CSPM : RDS.6	AWSManagedServices-TrustedRemediatorEnableRDSEnhancedMonitoring Abilita il monitoraggio avanzato per le istanze DB di Amazon RDS	• MonitoringInterval: L'intervallo, in secondi, tra i punti in cui vengono raccolti i parametri di Enhanced Monitoring per l'istanza DB. Gli intervalli validi sono 0, 1, 5, 10, 15, 30 e 60. Per disabilitare la raccolta dei parametri di monitoraggio avanzato, specifica 0. • MonitoringRoleName: il nome del ruolo IAM che consente ad Amazon RDS di inviare parametri di monitoraggio avanzati ad Amazon Logs. CloudWatch Se un ruolo non è specificato, `rds-monitoring-role` viene utilizzato o creato il ruolo predefinito, se non esiste. Se il monitoraggio avanzato è abilitato prima dell'esecuzione dell'automazione, le impostazioni potrebbero essere sovrascritte da questa automazione con i MonitoringRoleName valori MonitoringInterval e configurati nei parametri preconfigurati.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G190 - I cluster Amazon RDS devono avere la protezione da eliminazione abilitata Controllo corrispondente AWS Security Hub CSPM : RDS.7	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection La protezione da eliminazione è abilitata per i cluster Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G198 - Le istanze database di Amazon RDS devono avere la protezione da eliminazione abilitata Controllo corrispondente AWS Security Hub CSPM : RDS.8	AWSManagedServices-TrustedRemediatorEnableRDSDeletionProtection La protezione da eliminazione è abilitata per le istanze Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G199 - Le istanze DB RDS devono pubblicare i log in Logs CloudWatch Controllo corrispondente AWS Security Hub CSPM : RDS.9	AWSManagedServices-TrustedRemediatorEnableRDSLogExports Le esportazioni dei log RDS sono abilitate per l'istanza DB RDS o il cluster RDS DB.	Non sono consentiti parametri preconfigurati. È richiesto il ruolo AWSServiceRoleForRDS collegato al servizio.
Hs4Ma3G160 - L'autenticazione IAM deve essere configurata per le istanze RDS Controllo corrispondente AWS Security Hub CSPM : RDS.10	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication AWS Identity and Access Management l'autenticazione è abilitata per l'istanza RDS.	ApplyImmediately: indica se le modifiche in questa richiesta e le eventuali modifiche in sospeso vengono applicate in modo asincrono il prima possibile. Per applicare immediatamente la modifica, scegli. `true` Per pianificare la modifica per la prossima finestra di manutenzione, scegliete. `false` Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G161 - L'autenticazione IAM deve essere configurata per i cluster RDS Controllo corrispondente AWS Security Hub CSPM : RDS.12	AWSManagedServices-UpdateRDSIAMDatabaseAuthentication L'autenticazione IAM è abilitata per il cluster RDS.	ApplyImmediately: Indica se le modifiche in questa richiesta e le eventuali modifiche in sospeso vengono applicate in modo asincrono il prima possibile. Per applicare immediatamente la modifica, scegli. `true` Per pianificare la modifica per la prossima finestra di manutenzione, scegliete. `false` Nessun vincolo
Hs4Ma3G162 - Gli aggiornamenti automatici delle versioni minori di RDS devono essere abilitati Controllo corrispondente AWS Security Hub CSPM : RDS.13	AWSManagedServices-UpdateRDSInstanceMinorVersionUpgrade La configurazione automatica di aggiornamento della versione secondaria per Amazon RDS è abilitata.	Non sono consentiti parametri preconfigurati. L'istanza Amazon RDS deve essere nello `available` stato in cui si verifica questa correzione.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G163 - I cluster DB RDS devono essere configurati per copiare i tag nelle istantanee Controllo corrispondente AWS Security Hub CSPM : RDS.16	AWSManagedServices-UpdateRDSCopyTagsToSnapshots `CopyTagtosnapshot` l'impostazione per i cluster Amazon RDS è abilitata.	Non sono consentiti parametri preconfigurati. Le istanze di Amazon RDS devono essere disponibili affinché questa correzione avvenga.
Hs4Ma3G164 - Le istanze DB RDS devono essere configurate per copiare i tag nelle istantanee Controllo corrispondente AWS Security Hub CSPM : RDS.17	AWSManagedServices-UpdateRDSCopyTagsToSnapshots `CopyTagsToSnapshot` l'impostazione per Amazon RDS è abilitata.	Non sono consentiti parametri preconfigurati. Le istanze di Amazon RDS devono essere disponibili affinché questa correzione avvenga.
RSS93 HQwa1 Snapshot pubblici di Amazon RDS	AWSManagedServices-DisablePublicAccessOnRDSSnapshotV2 L'accesso pubblico per lo snapshot di Amazon RDS è disabilitato.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G103 - I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico AWS Security Hub CSPM Controllo corrispondente: Redshift.1	AWSManagedServices-DisablePublicAccessOnRedshiftCluster L'accesso pubblico sul cluster Amazon Redshift è disabilitato.	Non sono consentiti parametri preconfigurati. La disabilitazione dell'accesso pubblico blocca tutti i client provenienti da Internet. Inoltre, il cluster Amazon Redshift rimane in stato di modifica per alcuni minuti, mentre la riparazione disabilita l'accesso pubblico al cluster.
Hs4Ma3G106 - I cluster Amazon Redshift devono avere la registrazione di controllo abilitata AWS Security Hub CSPM Controllo corrispondente: Redshift.4	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterAuditLogging La registrazione di audit è abilitata sul cluster Amazon Redshift durante la finestra di manutenzione.	Non sono consentiti parametri preconfigurati. Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati. BucketName: Il secchio deve essere nello stesso. Regione AWS Il cluster deve disporre dei permessi di lettura per bucket e put object. Se la registrazione del cluster Redshift è abilitata prima dell'esecuzione dell'automazione, le impostazioni di registrazione potrebbero essere sovrascritte da questa automazione con `S3KeyPrefix` i valori `BucketName` e configurati nei parametri preconfigurati.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G105 - Amazon Redshift dovrebbe avere gli aggiornamenti automatici alle versioni principali abilitati AWS Security Hub CSPM Controllo corrispondente: Redshift.6	AWSManagedServices-EnableRedshiftClusterVersionAutoUpgrade-Gli aggiornamenti delle versioni principali vengono applicati automaticamente al cluster durante la finestra di manutenzione. Non ci sono tempi di inattività immediati per il cluster Amazon Redshift, ma il cluster Amazon Redshift potrebbe subire dei tempi di inattività durante la finestra di manutenzione se passa a una versione principale.	Non sono consentiti parametri preconfigurati. Nessun vincolo
Hs4Ma3G104 - I cluster Amazon Redshift devono utilizzare un routing VPC avanzato AWS Security Hub CSPM Controllo corrispondente: Redshift.7	AWSManagedServices-TrustedRemediatorEnableRedshiftClusterEnhancedVPCRouting Il routing VPC avanzato è abilitato per i cluster Amazon Redshift.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G173 - L'impostazione S3 Block Public Access deve essere abilitata a livello di bucket Controllo corrispondente AWS Security Hub CSPM : S3.8	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess I blocchi di accesso pubblico a livello di bucket vengono applicati per il bucket Amazon S3.	Non sono consentiti parametri preconfigurati. Questa correzione potrebbe influire sulla disponibilità degli oggetti S3. Per informazioni su come Amazon S3 valuta l'accesso, consulta Bloccare l'accesso pubblico allo storage Amazon S3.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G230 - La registrazione degli accessi al server bucket S3 deve essere abilitata Controllo corrispondente AWS Security Hub CSPM : S3.9	AWSManagedServices-EnableBucketAccessLogging(documento SSM predefinito per la modalità di esecuzione automatica e manuale) La registrazione degli accessi ai server Amazon S3 è abilitata.	• TargetBucket: il nome del bucket S3 per archiviare i log di accesso al server. • TargetObjectKeyFormat: formato chiave Amazon S3 per oggetti di log (i valori fanno distinzione tra maiuscole e minuscole). Per utilizzare il formato semplice per le chiavi S3 per gli oggetti di registro, scegli. `SimplePrefix` Per utilizzare la chiave S3 partizionata per gli oggetti di registro e utilizzarla EventTime per il prefisso partizionato, scegli. `PartitionedPrefixEventTime` Per utilizzare la chiave S3 partizionata per gli oggetti di registro e utilizzarla per il prefisso partizionato, scegliete . DeliveryTime `PartitionedPrefixDeliveryTime` I valori validi sono `SimplePrefix` , `PartitionedPrefixEventTime` e `PartitionedPrefixDeliveryTime` . Per abilitare la riparazione automatica, è necessario fornire il seguente parametro preconfigurato:. TargetBucket Il bucket di destinazione deve trovarsi nello stesso Regione AWS e

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		Account AWS nel bucket di origine, con le autorizzazioni corrette per la consegna dei log. Per ulteriori informazioni, consulta Attivazione della registrazione degli accessi al server Amazon S3.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G230 — La registrazione degli accessi al server bucket S3 deve essere abilitata Controllo corrispondente AWS Security Hub CSPM : S3.9	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 - La registrazione dei bucket di Amazon S3 è abilitata.	• TargetBucketTagKey: Il nome del tag (con distinzione tra maiuscole e minuscole) per identificare il bucket di destinazione. Utilizzat elo TargetBucketTagValueper etichettare il bucket da utilizzare come bucket di destinazione per la registrazione degli accessi. • TargetBucketTagValue: Il valore del tag (con distinzione tra maiuscole e minuscole) per identificare il bucket di destinazi one, usalo e TargetBucketTagKey per etichettare il bucket da utilizzar e come bucket di destinazione per la registrazione degli accessi. • TargetObjectKeyFormat: Formato chiave Amazon S3 per oggetti di log (i valori fanno distinzione tra maiuscole e minuscole): per utilizzare il formato semplice per le chiavi S3 per gli oggetti di log, scegli. SimplePrefix Per utilizzar e la chiave S3 partizionata per gli oggetti di log e EventTime utilizzarla per il prefisso partizion ato, scegli. PartitionedPrefixE ventTime Per utilizzare la chiave S3 partizionata per gli oggetti di registro e utilizzarla per il prefisso partizionato, scegliete. DeliveryT ime PartitionedPrefixDeliveryTi

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		me Il valore predefinito è Partition edPrefixEventTime. Per abilitare la riparazione automatic a, è necessario fornire i seguenti parametri: TargetBucketTagKeye TargetBucketTagValue. Il bucket di destinazione deve trovarsi nello stesso Regione AWS e Account AWS nel bucket di origine, con le autorizzazioni corrette per la consegna dei log. Per ulteriori informazioni, consulta Attivazione della registrazione degli accessi al server Amazon S3.
Pfx0 RwqBli Autorizzazioni Bucket Amazon S3	AWSManagedServices-TrustedRemediatorBlockS3BucketPublicAccess Blocco dell'accesso pubblico	Non sono consentiti parametri preconfigurati. Questo controllo è costituito da più criteri di avviso. Questa automazione risolve i problemi di accesso pubblico. La risoluzione di altri problemi di configurazione segnalati da Trusted Advisor non è supportata. Questa riparazione supporta la riparazione dei bucket S3 Servizio AWS creati (ad esempio, cf-templates-000000000000).

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G272 - Gli utenti non devono avere accesso root alle istanze dei notebook SageMaker Controllo corrispondente AWS Security Hub CSPM SageMaker: 3.	AWSManagedServices-TrustedRemediatorDisableSageMakerNotebookInstanceRootAccess L'accesso root per gli utenti è disabilitato per l'istanza del SageMaker notebook.	Non sono consentiti parametri preconfigurati. Questa riparazione causa un'interruzione se l'istanza del SageMaker notebook si trova nello stato in cui si trova. InService
Hs4Ma3G179 - Gli argomenti SNS devono essere crittografati a riposo utilizzando AWS KMS Controllo corrispondente AWS Security Hub CSPM : SNS.1	AWSManagedServices-EnableSNSEncryptionAtRest L'argomento SNS è configurato con la crittografia lato server.	KmsKeyId: l'ID di una chiave master del cliente AWS gestita (CMK) per Amazon SNS o di una CMK personalizzata da utilizzare per la crittografia lato server (SSE). `alias/aws/sns` L'impostazione predefinita è impostata su. Se viene utilizzata una AWS KMS chiave personalizzata, deve essere configurata con le autorizzazioni corrette. Per ulteriori informazioni, consulta Attivazione della crittografia lato server (SSE) per un argomento Amazon SNS

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G158 - I documenti SSM non devono essere pubblici Controllo corrispondente AWS Security Hub CSPM : SSM.4	AWSManagedServices-TrustedRemediatorDisableSSMDocPublicSharing- Disabilita la condivisione pubblica del documento SSM.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Hs4Ma3G136 - Le code di Amazon SQS devono essere crittografate quando sono inattive Controllo corrispondente AWS Security Hub CSPM : SQS.1	AWSManagedServices-EnableSQSEncryptionAtRest I messaggi in Amazon SQS sono crittografati.	• SqsManagedSseEnabled: impostato per `true` abilitare la crittografia delle code lato server utilizzando chiavi di crittografia di proprietà di Amazon SQS, impostato per `false` abilitare la crittografia delle code lato server utilizzando una chiave. AWS KMS • KMSKeyId: l'ID o l'alias di una chiave master del cliente AWS gestita (CMK) per Amazon SQS o di una CMK personalizzata da utilizzare per la crittografia lato server per la coda. Se non fornito, viene utilizzato. alias/aws/sqs • KmsDataKeyReusePeriodSeconds: il periodo di tempo, in secondi, durante il quale Amazon SQS può riutilizzare una chiave dati per crittografare o decrittografare i messaggi prima di effettuare una nuova chiamata. AWS KMS Numero intero che rappresenta secondi, tra 60 (1 minuto) e 86.400 (24 ore). Questa impostazione viene ignorata se è impostata su. `SqsManagedSseEnabled` `true` ReceiveMessage Le richieste anonime SendMessage e quelle inviate alla coda crittografata vengono rifiutate. Tutte le richieste

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		alle code con la funzione SSE abilitata devono utilizzare HTTPS e Signature Version 4.

Trusted Advisor controlli di tolleranza agli errori supportati da Trusted Remediator

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c18d2gz138 Ripristino Amazon DynamoDB Point-in-time	AWSManagedServices-TrustedRemediatorEnableDDBPITR Abilita point-in-time il ripristino per le tabelle DynamoDB.	Non sono consentiti parametri preconfigurati. Nessun vincolo
R365S2qddf Amazon S3 Bucket Versioning	AWSManagedServices-TrustedRemediatorEnableBucketVersioning Il controllo delle versioni del bucket Amazon S3 è abilitato.	Non sono consentiti parametri preconfigurati. Questa correzione non supporta la riparazione dei bucket S3 Servizio AWS creati (ad esempio cf-templates-000000000000).
BueAdJ7nRP Registrazione di Bucket Amazon S3	AWSManagedServices-EnableBucketAccessLogging La registrazione dei bucket Amazon S3 è abilitata.	• TargetBucket: il nome del bucket S3 per archiviare i log di accesso al server. • TargetObjectKeyFormat: formato chiave Amazon S3 per oggetti di log, per utilizzare il formato semplice per le chiavi S3 per gli oggetti di log, scegli. `SimplePrefix` Per utilizzare la chiave Partitioned S3 per gli oggetti di log

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		e usarla per il prefisso partizionato, EventTime scegli. `PartitionedPrefixEventTime` Per utilizzare la chiave S3 partizionata per gli oggetti di registro e utilizzarla per il prefisso partizionato, scegliete. DeliveryTime `PartitionedPrefixDeliveryTime` Il valore predefinito è `PartitionedPrefixEventTime` . I valori validi sono `SimplePrefix` e (con distinzione tra maiuscole e minuscole). `PartitionedPrefixEventTime` `PartitionedPrefixDeliveryTime` Per abilitare la riparazione automatica, è necessario fornire i seguenti parametri preconfigurati: • TargetBucket Il bucket di destinazione deve trovarsi nello stesso Regione AWS e Account AWS nel bucket di origine, con le autorizzazioni corrette per la consegna dei log. Per ulteriori informazioni, consulta Attivazione della registrazione degli accessi al server Amazon S3.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
F2ik5r6dep Amazon RDS Multi-AZ	AWSManagedServices-TrustedRemediatorEnableRDSMultiAZ L'implementazione di più zone di disponibilità è abilitata.	Non sono consentiti parametri preconfigurati. C'è un possibile peggioramento delle prestazioni durante questa modifica.
H7 IgTzj TYb Snapshot Amazon EBS	AWSManagedServices-TrustedRemediatorCreateEBSSnapshot Viene creato Amazon EBSsnapshots .	Non sono consentiti parametri preconfigurati. Nessun vincolo
Top ZvH QPADk Backup RDS	AWSManagedServices-EnableRDSBackupRetention La conservazione dei backup di Amazon RDS è abilitata per il DB.	• BackupRetentionPeriod: Il numero di giorni (1-35) per conservare i backup automatici. • ApplyImmediately: Indica se la modifica della conservazione del backup RDS e le eventuali modifiche in sospeso vengono applicate in modo asincrono il prima possibile. Scegli `true` di applicare la modifica immediata mente o di pianificare la modifica `false` per la finestra di manutenzi one successiva. Se il `ApplyImmediately` parametro è impostato su`true`, le modifiche in sospeso sul db vengono applicate insieme all'impostazione di RDSBackup conservazione.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c1qf5bt013 La scalabilità automatica dello storage sulle istanze DB di Amazon RDS è disattivata	AWSManagedServices-TrustedRemediatorEnableRDSInstanceStorageAutoScaling- La scalabilità automatica dello storage è abilitata per le istanze database di Amazon RDS.	• MaxAllocatedStorageIncrease Percentage: La percentuale di aumento della corrente Allocated Storage, per impostare la. MaxAllocatedStorage L'impostazione predefinita è impostata su26. È necessario impostare la soglia massima di archiviazione su almeno il 10% in più rispetto allo spazio di archiviazione attualmente allocato. È consigliabile impostare la soglia massima di archiviazione su almeno il 26% in più. Per maggiori dettagli, consulta Gestire automaticamente la capacità con lo storage autoscaling di Amazon Relational Database Service. Nessun vincolo
7q GXs KIUw Drenaggio della connessione Classic Load Balancer	AWSManagedServices-TrustedRemediatorEnableCLBConnectionDraining Il drenaggio della connessione è abilitato per Classic Load Balancer.	ConnectionDrainingTimeout: Il tempo massimo, in secondi, per mantenere aperte le connessioni esistenti prima di annullare la registrazione delle istanze. L'impostazione predefinita è impostata su secondi. `300` Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c18d2gz106 Amazon EBS non incluso nel piano AWS Backup	AWSManagedServices-TrustedRemediatorAddVolumeToBackupPlan Amazon EBS è incluso nel AWS Backup piano.	Remediation contrassegna il volume Amazon EBS con la seguente coppia di tag. La coppia di tag deve corrispondere ai criteri di selezione delle risorse basati su tag per. AWS Backup • TagKey • TagValue Nessun vincolo
c18d2gz107 Tabella Amazon DynamoDB non inclusa nel piano AWS Backup	AWSManagedServices-TrustedRemediatorAddDynamoDBToBackupPlan Amazon DynamoDB Table è inclusa nel piano. AWS Backup	Remediation contrassegna Amazon DynamoDB con la seguente coppia di tag. La coppia di tag deve corrispondere ai criteri di selezione delle risorse basati su tag per. AWS Backup • TagKey • TagValue Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c18d2gz117 Amazon EFS non incluso nel AWS Backup piano	AWSManagedServices-TrustedRemediatorAddEFSToBackupPlan Amazon EFS è incluso nel AWS Backup piano.	Remediation contrassegna Amazon EFS con la seguente coppia di tag. La coppia di tag deve corrispondere ai criteri di selezione delle risorse basati su tag per. AWS Backup • TagKey • TagValue Nessun vincolo
c18d2gz105 Bilanciamento del carico tra zone di Network Load Balancer	AWSManagedServices-TrustedRemediatorEnableNLBCrossZoneLoadBalancing Il bilanciamento del carico tra zone è abilitato su Network Load Balancer.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt026 Il `synchronous_commit` parametro Amazon RDS è disattivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `synchronous_commit` è attivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt030 Il `innodb_flush_log_at_trx_commit` parametro Amazon RDS non lo è 1	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `innodb_flush_log_at_trx_commit` è impostato su 1 per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c1qf5bt031 Il `sync_binlog` parametro Amazon RDS è disattivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `sync_binlog` è attivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt036 L'impostazione dei `innodb_default_row_format` parametri Amazon RDS non è sicura	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `innodb_default_row_format` è impostato su `DYNAMIC` per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c18d2gz144 Amazon EC2 Detailed Monitoring non abilitato	AWSManagedServices-TrustedRemediatorEnableEC2InstanceDetailedMonitoring Il monitoraggio dettagliato è abilitato per Amazon EC2.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Trusted Advisor controlli delle prestazioni supportati da Trusted Remediator

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
COr6dfpM06 AWS Lambda funzioni non sufficientemente fornite per	AWSManagedServices-ResizeLambdaMemory Le dimensioni della memoria delle funzioni Lambda vengono ridimensionate alla dimensione di memoria	RecommendedMemorySize: l'allocazione di memoria consigliata per la funzione Lambda. L'intervallo di valori è compreso tra 128 e 10240.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
quanto riguarda le dimensioni della memoria	consigliata fornita da. Trusted Advisor	Se la dimensione della funzione Lambda viene modificata prima dell'esecuzione dell'automazione, questa automazione potrebbe sovrascrivere le impostazioni con il valore consigliato da. Trusted Advisor

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
ZRxQlPsb6c Istanze Amazon EC2 ad alto utilizzo	AWSManagedServices-ResizeInstanceByOneLevel Le EC2 istanze Amazon vengono ridimensionate di un tipo di istanza in su nello stesso tipo di famiglia di istanze. Le istanze vengono interrotte e avviate durante l'operazione di ridimensionamento e riportate allo stato iniziale al termine dell'esecuzione. Questa automazione non supporta il ridimensionamento delle istanze che si trovano in un gruppo di Auto Scaling.	• MinimumDaysSinceLastChange: Il numero minimo di giorni trascorsi dall'ultima modifica del tipo di istanza. Se il tipo di istanza è stato modificato entro il tempo specificato, il tipo di istanza non viene modificato. `0`Utilizzatelo per saltare questa convalida. Il valore predefinito è 7. • Crea AMIBefore ridimensionamento: per creare l'AMI dell'istanza come backup prima del ridimensionamento, scegli. `true` Per non creare un backup, scegli. `false` Il valore predefinito è `false`. I valori validi sono `true` e `false` (distinzione tra maiuscole e minuscole). • ResizeIfStopped: Per procedere con la modifica delle dimensioni dell'istanza, anche se l'istanza è in uno stato interrotto, scegliete . `true` Per non ridimensionare automaticamente l'istanza se si trova in uno stato interrotto, sceglietefalse. I valori validi sono `true` e `false` (distinzione tra maiuscole e minuscole). Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c1qf5bt021 `innodb_change_buffering` Parametro Amazon RDS che utilizza un valore inferiore a quello ottimale	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il valore del `innodb_change_buffering` parametro è impostato su `NONE` per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt025 Il `autovacuum` parametro Amazon RDS è disattivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `autovacuum` è attivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt028 Il `enable_indexonlyscan` parametro Amazon RDS è disattivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `enable_indexonlyscan` è attivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt029 Il `enable_indexscan` parametro Amazon RDS è disattivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `enable_indexscan` è attivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c1qf5bt032 Il `innodb_stats_persistent` parametro Amazon RDS è disattivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `innodb_stats_persistent` è attivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt037 Il `general_logging` parametro Amazon RDS è attivato	AWSManagedServices-TrustedRemediatorRemediateRDSParameterGroupParameter Il parametro `general_logging` è disattivato per Amazon RDS.	Non sono consentiti parametri preconfigurati. Nessun vincolo

Trusted Advisor controlli dei limiti di servizio supportati da Trusted Remediator

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
Ln7rr0l7j9 EC2-Indirizzo IP elastico VPC	AWSManagedServices-UpdateVpcElasticIPQuota È richiesto un nuovo limite per gli indirizzi IP elastici EC2 -VPC. Per impostazione predefinita, il limite viene aumentato di 3.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
KM7qq0l7j9 Gateway Internet VPC	AWSManagedServices-IncreaseServiceQuota- È richiesto un nuovo limite per i gateway Internet VPC. Per impostazione predefinita, il limite viene aumentato di tre.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.
JL7pP0L7J9 VPC	AWSManagedServices-IncreaseServiceQuota È richiesto un nuovo limite per il VPC. Per impostazione predefinita, il limite viene aumentato di 3.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.
Fw7hh0l7j9 Gruppi Auto Scaling	AWSManagedServices-IncreaseServiceQuota È richiesto un nuovo limite per i gruppi di Auto Scaling. Per impostazi one predefinita, il limite viene aumentato di 3.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.

Controlla l'ID e il nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
3 Njm0 DJQO9 Gruppi di opzioni RDS	AWSManagedServices-Increase ServiceQuota È richiesto un nuovo limite per i gruppi di opzioni Amazon RDS. Per impostazione predefinita, il limite viene aumentato di 3.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.
EM8b3yLRTr Application Load Balancer ELB	AWSManagedServices-Increase ServiceQuota È richiesto un nuovo limite per ELB Application Load Balancers. Per impostazione predefinita, il limite viene aumentato di 3.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.
8 WiQ K YSt25 Bilanciatori del carico di rete ELB	AWSManagedServices-Increase ServiceQuota È richiesto un nuovo limite per ELB Network Load Balancer. Per impostazione predefinita, il limite viene aumentato di 3.	Incremento: il numero per aumentare la quota corrente. Il valore predefinito è 3. Se questa automazione viene eseguita più volte prima che il Trusted Advisor controllo venga aggiornato con lo 0K stato, potrebbe verificarsi un aumento del limite più elevato.

Trusted Advisor controlli di eccellenza operativa supportati da Trusted Remediator

Controlla ID e nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c18d2gz125 Il Gateway Amazon API non registra log di esecuzione	AWSManagedServices-TrustedRemediatorEnableAPIGateWayExecutionLogging La registrazione dell'esecuzione è abilitata nella fase API.	Non sono consentiti parametri preconfigurati. Devi concedere ad API Gateway l'autorizzazione a leggere e scrivere i log del tuo account CloudWatch per abilitare il log di esecuzione. Per maggiori dettagli, consulta CloudWatch Configurare la registrazione per REST APIs in API Gateway.
c18d2gz168 Protezione dall'eliminazione Elastic Load Balancing non abilitata per i sistemi di bilanciamento del carico	AWSManagedServices-TrustedRemediatorEnableELBDeletionProtection- La protezione da eliminazione è attivata per Elastic Load Balancer.	Non sono consentiti parametri preconfigurati. Nessun vincolo
c1qf5bt012 Amazon RDS Performance Insights è disattivato	AWSManagedServices-TrustedRemediatorEnableRDSPerformanceInsights Performance Insights è attivato per Amazon RDS.	• PerformanceInsightsRetentionPeriod: il numero di giorni per conservare i dati di Performance Insights. Valori validi: 7 o mese * 31, dove mese è un numero di mesi compreso tra 1 e 23. Esempi: 93 (3 mesi* 31), 341 (11 mesi* 31), 589 (19 mesi* 31) oppure731. • PerformanceInsightsKMSKeyId: l'ID AWS KMS chiave per la crittografia dei dati di Performan

Controlla ID e nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		ce Insights. Se non specifichi un valore per PerformanceInsights KMSKey Id, Amazon RDS utilizza la tua AWS KMS chiave predefini ta. Nessun vincolo

Controlla ID e nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
c1fd6b96l4 Registri di accesso Amazon S3 abilitati	AWSManagedServices-TrustedRemediatorEnableBucketAccessLoggingV2 La registrazione degli accessi ai bucket Amazon S3 è abilitata.	• TargetBucketTagValue: Il valore del tag (con distinzione tra maiuscole e minuscole) per identificare il bucket di destinazione, utilizzalo e TargetBucketTagKey contrassegna il bucket da utilizzare come bucket di destinazione per la registrazione degli accessi. • TargetObjectKeyFormat: formato chiave Amazon S3 per oggetti di log (i valori fanno distinzione tra maiuscole e minuscole). Per utilizzare il formato semplice per le chiavi S3 per gli oggetti di registro, scegli. `SimplePrefix` Per utilizzare la chiave S3 partizionata per gli oggetti di registro e utilizzarla EventTime per il prefisso partizionato, scegli. `PartitionedPrefixEventTime` Per utilizzare la chiave S3 partizionata per gli oggetti di registro e utilizzarla per il prefisso partizionato, scegliete . DeliveryTime `PartitionedPrefixDeliveryTime` I valori validi sono `SimplePrefix` , `PartitionedPrefixEventTime` e `PartitionedPrefixDeliveryTime` .

Controlla ID e nome	Nome del documento SSM e risultato previsto	Parametri e vincoli preconfigurati supportati
		Per abilitare la riparazione automatic a, è necessario fornire il seguente parametro preconfigurato: TargetBuc ketTagKeye. TargetBucketTagValue Il bucket di destinazione deve trovarsi nello stesso Regione AWS e Account AWS nel bucket di origine, con le autorizzazioni corrette per la consegna dei log. Per ulteriori informazioni, consulta Attivazione della registrazione degli accessi al server Amazon S3.

Configurare Trusted Advisor la correzione degli assegni in Trusted Remediator

Le configurazioni vengono archiviate AWS AppConfig come parte dell'applicazione Trusted Remediator. Ogni categoria di Trusted Advisor controllo ha un profilo di configurazione separato. Per ulteriori informazioni sulle Trusted Advisor categorie, consulta Visualizza le categorie di controllo.

È possibile richiedere di configurare le riparazioni in base alla risorsa o alla verifica. Trusted Advisor È possibile applicare eccezioni utilizzando i tag delle risorse.

> **Note**
>
> La correzione dei Trusted Advisor risultati è attualmente configurata utilizzando AWS AppConfig e questa funzionalità è attualmente completamente supportata. AMS prevede che questo cambierà in futuro. È consigliabile evitare di creare automazioni che dipendono da AWS AppConfig, poiché questo metodo è soggetto a modifiche. Tieni presente che in futuro potrebbe essere necessario aggiornare o modificare le automazioni basate sull' AWS AppConfig implementazione attuale per motivi di compatibilità.
> Il flag di funzionalità Compute Optimizer EC2 -> instances ha parametri aggiuntivi:

- allow-upscale Per consentire istanze di alto livello non ottimizzate e sottodimensionate. EC2 Il valore di default è "false".
- min-savings-opportunity-percentageL'opportunità percentuale minima di risparmio per la riparazione automatica. Il valore predefinito è 10%

Configurazioni di riparazione predefinite

Le configurazioni per i singoli Trusted Advisor controlli vengono memorizzate come flag. AWS AppConfig Il nome della bandiera corrisponde al nome dell'assegno. Ogni configurazione di controllo contiene i seguenti attributi:

- modalità di esecuzione: determina in che modo Trusted Remediator esegue la correzione predefinita:
  - Automatico: Trusted Remediator corregge automaticamente le risorse creando un documento SSM OpsItem, eseguendo il documento SSM e quindi risolvendo il problema dopo un'esecuzione riuscita. OpsItem
  - Manuale: OpsItem viene creato un documento SSM, ma il documento SSM non viene eseguito automaticamente. Esaminate OpsItem ed eseguite la riparazione utilizzando la RFC automatizzata. Per ulteriori informazioni, consulta Lavora con le riparazioni in Trusted Remediator.
  - Condizionale: la riparazione è disabilitata per impostazione predefinita. È possibile abilitarlo per risorse specifiche utilizzando i tag. Per ulteriori informazioni, vedere le seguenti sezioni Personalizza la riparazione con i tag delle risorse ePersonalizza la riparazione con i tag Resource Override.
  - Inattivo: la riparazione non viene eseguita e non viene creata alcuna OpsItem . Non è possibile ignorare la modalità di esecuzione per il Trusted Advisor controllo impostato su inattivo.
- parametri preconfigurati: immettete i valori per i parametri del documento SSM necessari per la riparazione automatica, nel formato di, separati da una virgola (`Parameter=Value`,). Trusted Advisor controlli supportati da Trusted RemediatorPer ogni controllo, vedere i parametri preconfigurati supportati per il documento SSM associato.
- alternative-automation-document: Questo attributo aiuta a sovrascrivere il documento di automazione esistente con un altro documento supportato (se disponibile per il controllo specifico). Per impostazione predefinita, questo attributo non è selezionato.

> **Note**
>
> L'`alternative-automation-document`attributo non supporta documenti di automazione personalizzati. È possibile utilizzare i documenti di automazione Trusted Remediator supportati esistenti elencati in[Trusted Advisor controlli supportati da Trusted Remediator](#).
> Ad esempio, a scopo di controllo`Qch7DwouX1`, ci sono tre documenti SSM associati: AWSManagedServices-StopEC 2Instance, AWSManagedServices-ResizeInstanceByOneLevel e. AWSManagedServices-TerminateInstance Il valore per `alternative-automation-document` può essere AWSManagedServices-ResizeInstanceByOneLevel o AWSManagedServices-TerminateInstance (AWSManagedServices-StopEC2Instance è il documento SSM predefinito da correggere).
> `Qch7DwouX1`

Il valore di ogni attributo deve corrispondere ai vincoli di tale attributo.

> **Tip**
>
> Prima di applicare le configurazioni predefinite per i Trusted Advisor controlli, è consigliabile prendere in considerazione l'utilizzo delle funzionalità Resource tagging e Resource override descritte nelle sezioni seguenti. Le configurazioni predefinite si applicano a tutte le risorse all'interno dell'account, il che potrebbe non essere consigliabile in tutti i casi.

Di seguito è riportato un esempio di schermata della console con la modalità di esecuzione impostata su Manuale e gli attributi corrispondenti ai relativi vincoli.

Personalizza la riparazione con i tag delle risorse

manual-for-tagged-onlyGli attributi automated-for-tagged-onlyand nella configurazione del controllo consentono di specificare i tag delle risorse relativi al modo in cui si desidera correggere i singoli controlli. È consigliabile utilizzare questo metodo quando è necessario applicare un comportamento di correzione coerente a un gruppo di risorse che condividono lo stesso tag o gli stessi tag. Di seguito sono riportate le descrizioni di questi tag:

- automated-for-tagged-only: Specificate i tag delle risorse (una o più coppie di tag, separate da virgole) per la correzione automatica dei controlli, indipendentemente dalla modalità di esecuzione predefinita.
- manual-for-tagged-only: Specificate i tag delle risorse (una o più coppie di tag, separate da virgole) per le riparazioni che devono essere eseguite manualmente, indipendentemente dalla modalità di esecuzione predefinita.

Ad esempio, se si desidera abilitare la riparazione automatica per tutte le risorse non di produzione e applicare la riparazione manuale per le risorse di produzione, è possibile impostare la configurazione come segue:

```
"execution-mode": "Conditional",
"automated-for-tagged-only": "Environment=Non-Production",
"manual-for-tagged-only": "Environment=Production",
```

Con le configurazioni precedenti impostate sulle risorse, verificate che il comportamento di riparazione sia il seguente:

- Le risorse contrassegnate con 'Environment=Non-Production' vengono corrette automaticamente.
- Le risorse contrassegnate con 'Environment=Production' richiedono un intervento manuale per la riparazione.
- Le risorse senza il tag 'Environment' seguono la modalità di esecuzione predefinita (`Conditional`, in questo caso. Quindi, non viene intrapresa alcuna azione sulle risorse rimanenti).

Per ulteriore assistenza con le configurazioni, contatta il tuo Cloud Architect.

Personalizza la riparazione con i tag Resource Override

I tag Resource override consentono di personalizzare il comportamento di riparazione per le singole risorse, indipendentemente dai relativi tag. Aggiungendo un tag specifico a una risorsa, si sostituisce la modalità di esecuzione predefinita per quella risorsa e il controllo. Trusted Advisor Il tag resource override ha la precedenza sulla configurazione predefinita e sulle impostazioni di tagging delle risorse. Pertanto, se impostate la modalità di esecuzione predefinita su Automatizzata, Manuale o Condizionale per una risorsa che utilizza il tag Resource Override, questa sovrascrive la modalità di esecuzione predefinita e qualsiasi configurazione di etichettatura delle risorse.

Per sovrascrivere la modalità di esecuzione di una risorsa, completa i seguenti passaggi:

1. Identifica le risorse per le quali desideri sostituire la configurazione di riparazione.
2. Determina l' Trusted Advisor ID del controllo che desideri sostituire. Puoi trovare il controllo IDs per i check-in supportati Trusted Advisor in[Trusted Advisor controlli supportati da Trusted Remediator](#).
3. Aggiungi un tag alle risorse con la chiave e il valore seguenti utilizzando il tipo di modifica [Tag | Update](#) o [Tag | Bulk Update](#):

   - Chiave tag: `TR-`*`Trusted Advisor check ID`*`-Execution-Mode` (con distinzione tra maiuscole e minuscole)

     Nell'esempio di chiave del tag precedente, sostituiscilo `Trusted Advisor check ID` con l'identificativo univoco del Trusted Advisor controllo che desideri sovrascrivere.
   - Valore del tag: utilizzate uno dei seguenti valori per il valore del tag:
     - Automatico: Trusted Remediator corregge automaticamente la risorsa per questo Trusted Advisor controllo.
     - Manuale: OpsItem viene creato un file per la risorsa, ma la riparazione non viene eseguita automaticamente. La correzione viene esaminata ed eseguita utilizzando la procedura automatica. Per ulteriori informazioni, consulta [Lavora con le riparazioni in Trusted Remediator](#).
     - Inattivo: la riparazione e la OpsItem creazione non vengono eseguite per questa risorsa e per il controllo specificato. Trusted Advisor

Ad esempio, per correggere automaticamente un volume Amazon EBS con l'ID di Trusted Advisor controllo, `DAvU99Dc4C` aggiungi un tag al volume EBS. La chiave del tag è `TR-DAvU99Dc4C-Execution-Mode` e il valore del tag è. `Automated`

Di seguito è riportato un esempio di console che mostra la sezione Tags:

Workflow decisionale in modalità di esecuzione

Esistono diversi livelli per configurare la modalità di esecuzione per le risorse e per ogni Trusted Advisor controllo. Il diagramma seguente mostra come Trusted Remediator decide quale modalità di esecuzione utilizzare in base alle configurazioni:

Configurazione dei tutorial di riparazione

I seguenti tutorial forniscono esempi di creazione di rimedi comuni in Trusted Remediator

Ripristina tutte le risorse manualmente

Questo esempio configura la riparazione manuale per tutti i volumi Amazon EBS con l'ID di Trusted Advisor controllo DAv U99Dc4C (Underutilized Amazon EBS Volumes).

Configura la riparazione manuale per i volumi Amazon EBS con ID di controllo U99Dc4C DAv

1. Usa Remediation Configuration|Update, cambia tipo per richiedere l'aggiornamento della configurazione.
2. Immetti i seguenti parametri:
   - CheckIds: U99Dc4C DAv
   - ExecutionMode: Manuale

   > **Note**
   >
   > È possibile configurare più controlli in un'unica richiesta. Per i controlli che richiedono la stessa configurazione, includi più controlli IDs nel CheckIdsparametro. Per i controlli che richiedono una configurazione diversa, create un nuovo RemediationConfigurationoggetto.

3. Invia la RFC.

Ripristina automaticamente tutte le risorse, ad eccezione di quelle selezionate

Questo esempio configura la riparazione automatica per tutti i volumi Amazon EBS con l'ID di Trusted Advisor controllo DAv U99Dc4C (Underutilized Amazon EBS Volumes), ad eccezione dei volumi specificati che non verranno corretti (designati come inattivi).

Configura la riparazione automatica per i volumi Amazon EBS con ID di controllo DAv U99Dc4C, ad eccezione di risorse inattive selezionate

1. Sostituisci la riparazione automatica per volumi Amazon EBS selezionati:

Usa il tipo di modifica Tag | Update o Tag | Bulk Update per applicare il seguente tag ai volumi da escludere dalla riparazione automatica:

- Chiave: TR - U99Dc4C-Execution-Mode DAv
- Valore: inattivo

2. Utilizza il tipo di modifica Remediation Configuration|Update per richiedere l'aggiornamento della configurazione.
3. Immetti i seguenti parametri:

- CheckIds: U99Dc4C DAv
- ExecutionMode: Automatizzato

4. Invia la RFC.

Correggi automaticamente le risorse contrassegnate

Questo esempio configura la riparazione automatica per tutti i volumi Amazon EBS con il tag `Stage=NonProd` con l'ID di Trusted Advisor controllo DAv U99Dc4C (Underutilized Amazon EBS Volumes). Tutte le altre risorse prive di questo tag non vengono corrette.

Configura la riparazione automatica per i volumi Amazon EBS con il tag **`Stage=NonProd`** per l'ID di controllo U99Dc4C DAv

1. Usa Remediation Configuration | Update, cambia tipo per richiedere l'aggiornamento della configurazione.
2. Immetti i seguenti parametri:

- CheckIds: DAv U99Dc4C
- ExecutionMode: Condizionale
- AutomatedForTaggedOnly: {"Fase»:» NonProd «}

> **Note**
>
> Il valore specificato per il AutomatedForTaggedOnlyparametro sostituisce il valore configurato in precedenza. Per mantenere i tag esistenti, includeteli nel nuovo valore.

3. Invia la RFC.

Ripristina la configurazione ai valori predefiniti

Questo esempio rimuove la automated-for-tagged-onlyconfigurazione esistente per il controllo Hs4Ma3G104. Per rimuovere la configurazione di tag applicata in precedenza, impostate il AutomatedForTaggedOnlyvalore del parametro su {}.

Reimposta la configurazione ai valori predefiniti per controllare Hs4Ma3G104

1. Utilizza il tipo di modifica Remediation Configuration | Update per richiedere l'aggiornamento della configurazione.
2. Immetti i seguenti parametri:
   - CheckIds: Hs4Ma3G104
   - ExecutionMode: Inserire il valore attualmente utilizzato
   - AutomatedForTaggedOnly: {}
3. Invia la RFC.

Lavora con le riparazioni in Trusted Remediator

Tieni traccia delle riparazioni in Trusted Remediator

Per tenere traccia delle OpsItems riparazioni, completa i seguenti passaggi:

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Scegli Operations Management, OpsCenter.
3. (Facoltativo) Filtrate l'elenco per Source=Trusted Remediator per includere solo Trusted OpsItems Remediator nell'elenco.

   Di seguito è riportato un esempio della OpsCenter schermata filtrata da Source=Trusted Remediator:

> **Note**
>
> Oltre alla visualizzazione OpsItems da OpsCenter, è possibile visualizzare i registri delle riparazioni nel bucket AMS S3. Per ulteriori informazioni, consulta Registri di riparazione in Trusted Remediator.

Esegui riparazioni manuali in Trusted Remediator

Trusted Remediator crea controlli configurati OpsItems per la riparazione manuale. È necessario rivedere questi controlli e iniziare il processo di riparazione manualmente.

Per rimediare manualmente OpsItem, completa i seguenti passaggi:

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.
2. Scegli Operations Management, OpsCenter.
3. (Facoltativo) Filtrate l'elenco per Source=Trusted Remediator per includere solo Trusted OpsItems Remediator nell'elenco.
4. Scegli quello OpsItem che desideri rivedere.
5. Rivedi i dati operativi di OpsItem. I dati operativi includono i seguenti elementi:
   - trustedAdvisorCheckCategoria: la categoria dell'ID dell' Trusted Advisor assegno. Ad esempio, tolleranza ai guasti
   - trustedAdvisorCheckId: l'ID univoco dell' Trusted Advisor assegno.
   - trustedAdvisorCheckMetadati: i metadati della risorsa, incluso l'ID della risorsa.
   - trustedAdvisorCheckNome: il nome dell'assegno. Trusted Advisor
   - trustedAdvisorCheckStato: lo stato del Trusted Advisor controllo rilevato per la risorsa.
   - trustedAdvisorCheckManualRemediation: i dati personalizzati che forniscono i dettagli di riferimento per la riparazione manuale.
     - ManualExecutionInput: Un oggetto che definisce i parametri per i quali è possibile modificare i valori durante l'esecuzione della riparazione manuale.
       - DocumentName: il nome del runbook (documento SSM).
       - CustomizableParameters: nomi dei parametri che è possibile modificare.

- DefaultInput: un oggetto che definisce i nomi e i valori dei parametri da utilizzare per la riparazione manuale. I valori vengono inseriti in base a parametri preconfigurati.

6. Per rimediare manualmente, completa i seguenti passaggi OpsItem:

   a. Usa Trusted Remediator | Finding | Risolvi il tipo di modifica ct-1c7ch8z5phrjp

   b. Immettete i valori per i seguenti parametri:

      - DocumentName: Deve essere`AWSManagedServices-RemediateTrustedRemediatorFinding`.
      - Regione: La Regione AWS, nel formato us-east-1.
      - Parametri: Immettere i parametri di riparazione manuale:
        - OpsItemId: L'ID dell'elemento Ops.
        - RemediationDocumentName: il nome del documento di automazione SSM da utilizzare. Il documento deve essere associato all'elemento Ops. Se all'elemento Ops sono associati più documenti, è DocumentNamenecessario specificarli.
        - RemediationParameters: Una key/value mappa di parametri per l'esecuzione dell'automazione, nel formato:`{\"`*`ParameterName1`*`\":[\"`*`ParameterValue1`*`\"], \"`*`ParameterName2`*`\":[\"`*`ParameterValue2`*`\"]}`. È possibile utilizzare solo i parametri presenti nell'elemento Ops trustedAdvisorCheckManualRemediation CustomizableParameters. Se non specificato, i parametri e i valori vengono recuperati dall'elemento Ops.

   c. Seleziona Esegui. Se non ci sono errori, viene visualizzata la pagina RFC creata correttamente con i dettagli RFC inviati e l'output Run iniziale.

   d. Monitora l'avanzamento dell'esecuzione RFC.

   e. Una volta completata l'esecuzione, OpsItem viene risolto. Se la RFC non è riuscita, segui i passaggi indicati. Risolvi i problemi relativi alle riparazioni in Trusted Remediator Per ulteriore assistenza nella risoluzione dei problemi, contatta AMS.

Risolvi i problemi relativi alle riparazioni in Trusted Remediator

Per assistenza sulle riparazioni manuali e sugli errori di riparazione, contatta AMS.

Per visualizzare lo stato e i risultati della riparazione, completa i seguenti passaggi:

1. Apri la AWS Systems Manager console all'indirizzo https://console.aws.amazon.com/systems-manager/.

2. Scegli Operations Management, OpsCenter.
3. (Facoltativo) Filtrate l'elenco per Source=Trusted Remediator per includere solo Trusted OpsItems Remediator nell'elenco.
4. Scegli quello OpsItem che desideri rivedere.
5. Nella sezione Automation Executions, esamina il nome, lo stato del documento e i risultati.
6. Esamina i seguenti errori di automazione comuni. Se i tuoi problemi non sono elencati qui, contatta il tuo CSDM per ricevere assistenza.

Errori di riparazione comuni

Nessuna esecuzione è elencata in Automation Executions

Nessuna esecuzione associata a OpsItem potrebbe indicare che l'esecuzione non è stata avviata a causa di valori dei parametri errati.

Fasi per la risoluzione dei problemi

1. Nei Dati operativi, esamina il valore della `trustedAdvisorCheckAutoRemediation` proprietà.
2. Verificate che i valori DocumentNamee Parameters siano corretti. Per i valori corretti, Configurare Trusted Advisor la correzione degli assegni in Trusted Remediator consulta i dettagli su come configurare i parametri SSM. Per esaminare i parametri di controllo supportati, vedere Trusted Advisor controlli supportati da Trusted Remediator
3. Verifica che i valori nel documento SSM corrispondano ai modelli consentiti. Per visualizzare i dettagli dei parametri nel contenuto del documento, seleziona il nome del documento nella sezione Runbooks.
4. Dopo aver esaminato e corretto i parametri, correggi manualmente il. OpsItem Per le fasi di riparazione, vedere. Esegui riparazioni manuali in Trusted Remediator
5. Per evitare che questo errore si ripresenti, assicuratevi di configurare la riparazione con i valori dei parametri corretti nella configurazione. Per ulteriori informazioni, consulta Configurare Trusted Advisor la correzione degli assegni in Trusted Remediator

Esecuzioni non riuscite in Automation Executions

I documenti di riparazione contengono più passaggi che interagiscono con l' Servizi AWS esecuzione di varie azioni. APIs Per identificare una causa specifica dell'errore, completa i seguenti passaggi:

Fasi per la risoluzione dei problemi

1. Per visualizzare i singoli passaggi di esecuzione, scegli l'ID di esecuzione, link nella sezione Automation Executions. Di seguito è riportato un esempio della console Systems Manager che mostra i passaggi di esecuzione per un'automazione selezionata:

2. Scegli il passaggio con lo stato Non riuscito. Di seguito sono riportati alcuni esempi di messaggi di errore:

   - `NoSuchBucket - An error occurred (NoSuchBucket) when calling the GetPublicAccessBlock operation: The specified bucket does not exist`

     Questo errore indica che il nome errato del bucket è stato specificato nei parametri preconfigurati della configurazione di riparazione.

     Per risolvere questo errore, esegui manualmente l'automazione utilizzando il nome del bucket corretto. Per evitare che questo problema si ripresenti, aggiorna la configurazione di riparazione con il nome del bucket corretto.

   - `DB instance my-db-instance-1 is not in available status for modification.`

     Questo errore indica che l'automazione non è riuscita ad apportare le modifiche previste perché l'istanza DB si trovava in uno stato non valido.

     Per risolvere questo errore, esegui manualmente l'automazione.

Registri di riparazione in Trusted Remediator

Trusted Remediator crea log in formato JSON e li carica su Amazon Simple Storage Service. I file di log vengono caricati in un bucket S3 creato da AMS e denominato. `ams-trusted-remediator-{your-account-id}-logs` AMS crea il bucket S3 nell'account Delegated Administrator. È possibile importare i file di registro in QuickSight modo da generare report di riparazione personalizzati.

Registro degli elementi di riparazione

Trusted Remediator crea il `Remediation item log` momento in cui viene creata una riparazione OpsItem . Questo registro contiene la riparazione manuale OpsItem e la riparazione automatica.

OpsItem È possibile utilizzare il file `Remediation item log` per tenere traccia della panoramica di tutte le riparazioni.

Posizione del registro degli elementi di riparazione per i consigli di Compute Optimizer

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/compute_optimizer_remediation_items/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`-`*`Resource ID`*`.json`

Posizione del registro degli elementi di riparazione per i controlli Trusted Advisor

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs/remediation_items/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`- `*`Resource ID`*`.json`

URL di esempio del file di registro dell'elemento di riparazione

`s3:///ams-trusted-remediator-`*`111122223333`*`-logs/remediation_items/`*`2023-02-06`*`/`*`1675660464-DAvU99Dc4C-vol-00bd8965660b4c16d.json`*

Formato di registro degli elementi di Compute Optimizer Remediation

```
{
  "AccountID": "Account_ID",
  "ComputeOptimizerCheckID": "Compute Optimizer check ID",
  "ComputeOptimizerCheckName": "Compute Optimizer check name",
  "ResourceID": "Resource ID",
  "RemediationTime": Remediation creation time,
  "ExecutionMode": "Automated or Manual",
  "OpsItemID": "OpsItem ID"
}
```

Trusted Advisor Formato del registro degli elementi di riparazione

```
{
   "TrustedAdvisorCheckID": Trusted Advisor check ID,
   "TrustedAdvisorCheckName": Trusted Advisor check name,
   "TrustedAdvisorCheckResultTime": 10 digits epoch time or unix timestamp,
   "ResourceID": Resource ID,
   "RemediationTime": Remediation creation time,
```

```
    "ExecutionMode": Automated or Manual,
    "OpsItemID": OpsItem ID
}
```

Contenuto di esempio in formato di log dell'elemento Compute Optimizer Remediation

```
{
  "AccountID": "123456789012",
  "ComputeOptimizerCheckID": "compute-optimizer-ebs",
  "ComputeOptimizerCheckName": "EBS volumes",
  "ResourceID": "vol-1235589366f77aca7",
  "RemediationTime": 1755044783,
  "ExecutionMode": "Manual",
  "OpsItemID": "oi-b8888b38fe78"
}
```

Trusted Advisor Contenuto di esempio del formato del registro degli elementi di riparazione

```
{
    "TrustedAdvisorCheckID": "DAvU99Dc4C",
    "TrustedAdvisorCheckName": "Underutilized Amazon EBS Volumes",
    "TrustedAdvisorCheckResultTime": 1675614749,
    "ResourceID": "vol-00bd8965660b4c16d",
    "RemediationTime": 1675660464,
    "OpsItemID": "oi-cca5df7af718"
}
```

Registro di esecuzione della riparazione automatizzata, Compute Optimizer e Trusted Advisor

Trusted Remediator crea il `Automated remediation execution log` quando viene completata l'esecuzione automatica di un documento SSM. Questo registro contiene i dettagli dell'esecuzione di SSM solo per la riparazione automatica. OpsItem È possibile utilizzare questo file di registro per tenere traccia delle riparazioni automatiche.

Compute Optimizer Posizione del registro di correzione automatizzata

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Compute Optimizer recommendation ID`*`.json`

Trusted Advisor Posizione del registro di riparazione automatizzato

`s3://ams-trusted-remediator-`*`delegated-administrator-account-id`*`-logs//remediation_executions/`*`remediation creation time in yyyy-mm-dd format`*`/`*`10 digits epoch time or unix timestamp`*`-`*`Trusted Advisor check ID`*`-`*`Resource ID`*`.json`

Esempio di posizione del registro di correzione automatizzato di Compute Optimizer

`s3://ams-trusted-remediator-`*`111122223333`*`-logs/remediation_executions/2025-06-26/1750908858-123456789012-compute-optimizer-ec2-i-1235173471d2cd789.json`

Trusted Advisor Esempio di posizione del registro di riparazione automatizzato

`s3://ams-trusted-remediator-`*`111122223333`*`-logs/remediation_executions/2023-02-06/1675660573-DAvU99Dc4C-vol-00bd8965660b4c16d.json`

Contenuto di esempio in formato registro di riparazione automatizzato

```
{
    "OpsItemID": "oi-767c77e05301",
    "SSMExecutionID": "93d091b2-778a-4cbc-b672-006954d76b86",
    "SSMExecutionStatus": "Success"}
```

Le migliori pratiche in Trusted Remediator

Di seguito sono riportate le best practice per aiutarti a utilizzare Trusted Remediator:

- Se non sei sicuro dei risultati della correzione, inizia con la modalità di esecuzione manuale. A volte, applicare l'esecuzione automatizzata per le riparazioni sin dall'inizio potrebbe causare risultati imprevisti.
- Esegui una revisione settimanale delle correzioni e approfondisci OpsItems i risultati di Trusted Remediator.
- Gli account membro ereditano le configurazioni dall'account amministratore delegato. Pertanto, è importante strutturare gli account in modo da gestire più account con le stesse configurazioni. È possibile esentare le risorse dalla configurazione predefinita utilizzando i tag.

Trusted Remediator FAQs

Di seguito sono riportate le domande frequenti su Trusted Remediator:

Che cos'è Trusted Remediator e quali sono i miei vantaggi?

Quando viene identificata una non conformità Trusted Advisor o viene emessa una raccomandazione da Compute Optimizer, Trusted Remediator risponde in base alle preferenze specificate dall'utente, applicando la correzione, richiedendo l'approvazione tramite riparazioni manuali o segnalando le correzioni durante l'imminente Monthly Business Review (MBR). La riparazione avviene all'orario o alla pianificazione prescelti. Trusted Remediator offre la possibilità di eseguire operazioni self-service e intervenire in base ai Trusted Advisor controlli con la flessibilità necessaria per configurare e correggere i controlli singolarmente o in blocco. Con una libreria di documenti di correzione testati, AMS aumenta costantemente la tua reputazione applicando controlli di sicurezza e seguendo le migliori pratiche. AWS Riceverete una notifica solo se specificate di farlo nella configurazione. Gli utenti AMS possono optare per Trusted Remediator senza costi aggiuntivi.

In che modo Trusted Remediator si relaziona e funziona con gli altri? Servizi AWS

Hai accesso ai Trusted Advisor controlli e ai consigli di Compute Optimizer come parte del tuo piano Enterprise Support esistente. Trusted Remediator si integra con Trusted Advisor Compute Optimizer per sfruttare le funzionalità di automazione AMS esistenti. In particolare, AMS utilizza documenti di AWS Systems Manager automazione (runbook) per le riparazioni automatiche. AWS AppConfig viene utilizzato per configurare i flussi di lavoro di riparazione. È possibile visualizzare tutte le riparazioni attuali e passate tramite Systems Manager OpsCenter. I log di riparazione sono archiviati in un bucket Amazon S3. Puoi utilizzare i log per importare e creare dashboard di reporting personalizzate. QuickSight

Chi configura le riparazioni?

Le configurazioni del tuo account sono di tua proprietà. La gestione delle configurazioni è responsabilità dell'utente. Puoi anche contattare AMS per le modifiche alla configurazione, il supporto, le riparazioni manuali e la risoluzione dei problemi di riparazione.

Come posso installare i documenti di automazione SSM?

I documenti di automazione SSM vengono condivisi automaticamente con gli account AMS registrati.

Verranno ripristinate anche le risorse di proprietà di AMS?

Le risorse di proprietà di AMS non sono contrassegnate da Trusted Remediator. Trusted Remediator si concentra solo sulle tue risorse.

In cosa Regioni AWS è disponibile Trusted Remediator e chi può utilizzarlo?

Trusted Remediator è disponibile per i clienti AMS Advanced. Per un elenco aggiornato delle regioni di supporto, vedi Servizi AWS per regione.

Trusted Remediator causerà la deriva delle risorse?

Poiché i documenti di automazione SSM aggiornano direttamente le risorse tramite l' AWS API, potrebbe verificarsi una deriva delle risorse. È possibile utilizzare i tag per separare le risorse create tramite i pacchetti esistenti. CI/CD È possibile configurare Trusted Remediator in modo che ignori le risorse contrassegnate continuando a correggere le altre risorse.

Come posso mettere in pausa o interrompere Trusted Remediator?

Utilizza Management | Trusted Remediator | State | Abilita o disabilita il tipo di modifica per interrompere il servizio Trusted Remediator. Utilizza lo stesso tipo di modifica per riattivare Trusted Remediator.

Come posso correggere i controlli che non sono supportati da Trusted Remediator?

Puoi continuare a contattare AMS tramite Operations On Demand (OOD) per i controlli non supportati. AMS ti aiuta a correggere questi controlli. Per ulteriori informazioni, consulta Operations On Demand.

Quali risorse distribuisce Trusted Remediator ai tuoi account?

Trusted Remediator distribuisce le seguenti risorse nell'account amministratore delegato di Trusted Remediator:

- Un bucket Amazon S3 denominato. `ams-trusted-remediator-{your-account-id}-logs` Trusted Remediator crea il file `Remediation item log` in formato JSON quando OpsItem viene creata una correzione e carica i file di registro in questo bucket.
- Un' AWS AppConfig applicazione per contenere le configurazioni di riparazione per i Trusted Advisor controlli supportati e i consigli di Compute Optimizer.

Trusted Remediator non distribuisce risorse nell'account membro di Trusted Remediator.

Gestione dei registri

Argomenti

AMS log management raccoglie, aggrega e controlla la conservazione dei log dall'account gestito. AWS la gestione dei log aggrega i log delle EC2 istanze e AWS delle risorse Amazon distribuite all'interno del tuo account in Logs. CloudWatch L'elenco completo dei servizi da cui i log sono attualmente aggregati è disponibile in. Log di servizio aggregati AMS

Cos'è la gestione dei log?

La gestione dei log è il processo di gestione degli eventi di log generati da istanze, applicazioni e servizi AWS. Questa funzionalità definisce il modo in cui AMS elabora, archivia e ruota gli eventi di log generati nel tuo account AWS gestito. I log dell'infrastruttura vengono utilizzati durante la risoluzione degli incidenti e per supportare gli audit di sistema.

Come funziona la registrazione AMS

La gestione dei log di AMS single-account landing zone (SALZ) utilizza una varietà di agenti e strumenti preinstallati che vengono implementati al momento dell'onboarding o del provisioning di istanze e applicazioni.

La registrazione viene configurata durante il processo di onboarding dell'account e quando viene avviato uno stack.

I log AMS multi-account landing zone (MALZ) prodotti dalle istanze e dai servizi AWS sono disponibili in CloudWatch Logs o Amazon Simple Storage Service (Amazon S3), all'interno di ciascun account gestito da AMS. La landing zone multi-account AMS fornisce un account di registrazione centrale che funge da posizione di aggregazione centrale per alcuni log prodotti dai singoli account delle applicazioni.

Le tabelle nelle Accesso ai tuoi log sottosezioni descrivono quali registri sono disponibili nei singoli account e quali sono disponibili nell'account di registrazione centrale.

Accesso ai tuoi log

Per accedere ai tuoi log, assicurati di avere uno dei ruoli IAM richiesti e di essere registrato nel tuo account AMS. Quindi vai alla directory mostrata.

Multi-Account Landing Zone (MALZ)

Fornisce cinque ruoli IAM predefiniti, ognuno dei quali consente l'accesso a tutti i log del tuo account (tutti sono preceduti da): `AWSManagedServices`

- `AdminRole`
- `CaseRole`
- `ChangeManagementRole`
- `ReadOnlyRole`
- `SecurityOpsRole`

L'accesso a questi ruoli è configurato tramite federazione, con ogni ruolo mappato a un gruppo all'interno del dominio Active Directory.

Per ulteriori informazioni su questi ruoli, consultaRuolo utente IAM in AMS.

Single-Account Landing Zone (SALZ)

L'impostazione predefinita `Customer_ReadOnly_Role` per la landing zone con account singolo AMS consente l'accesso a tutti i log all'interno del proprio account. L'accesso ai log è controllato utilizzando i ruoli di AWS Identity and Access Management (IAM) mappati su gruppi Active Directory.

Log di servizio aggregati AMS

Ogni AWS servizio accede a CloudWatch Logs o a una posizione specifica in un bucket Amazon S3.

> **Note**
>
> Se non diversamente specificato, tutte le posizioni dei log sono locali dell'account che ha generato i log e non sono aggregate nell'account di registrazione centrale.

Per trovare i nomi dei CloudTrail trail AMS predefiniti negli account SALZ e MALZ, vai alla Console AWS per CloudTrail , quindi alla pagina Trails e cerca AMS. Poiché le risorse AMS hanno dei tag, puoi trovare i percorsi in questo modo. Esempio di CloudTrail tag AMS:

```
Environment   AMSInfrastructure
```

Per accedere ai tuoi log, assicurati di avere uno dei ruoli IAM richiesti e di essere registrato nel tuo account AMS. Quindi vai alla directory mostrata.

Multi-Account Landing Zone

Registri di servizio aggregati per più zone di atterraggio AMS con più account

	Nome servizio	Dettagli del registro	Posizione del registro
1	Amazon Aurora	Log generali, di interrogazioni lente e di errori.	CloudWatch LogGroup: /aws/rds/cluster/{*database_name* }/{*log_name*}
2	AWS CloudFormation (CFN)	Solo registrazione delle chiamate API.	AWS CloudFormation Le chiamate API sono documentate tramite CloudTrail, che invia i log a CloudWatch LogGroup e quindi li sincronizza in un bucket S3. I log vengono conservati per 14 giorni per impostazione predefinita nel bucket S3 e vengono conservati a tempo indeterminato nel CloudWatch LogGroup bucket S3. CloudWatch LogGroup:CloudTrail//Landing Zone-Logs Bucket S3 [nell'account di registrazione centrale]: -ams-a {} -log-management- {} aws-landing-zone-logs *account_ID region*

	Nome servizio	Dettagli del registro	Posizione del registro
			AWSLogsPercorso:/{ }//*account_ID* CloudTrail
3	Amazon CloudFront (CloudFront)	Registrazione delle richieste degli utenti. CloudFront la registrazione deve essere abilitata in modo esplicito. Per informazioni, consulta Abilitazione della registrazione per i servizi supportati.	Bucket S3: ams-a {} -log-mana gement- {} *account_ID region* Percorso: AWS/RedShift/{} *CloudFront distribution ID*
4	Amazon CloudWatch (CloudWatch)	Solo registrazione delle chiamate API.	CloudWatch LogGroup://Landing-Zone-Logs CloudTrail Bucket S3 [nell'account di registrazione centrale]: - {} - {} aws-landing-zone-logs *account_ID region* Percorso:/{} AWSLogs*account_ID* //CloudTrail
5	Amazon Elastic Block Store (Amazon EBS)	Il servizio EBS non produce alcun registro.	Non applicabile
6	Amazon Elastic Compute Cloud (Amazon EC2)	Log di sistema e delle applicazioni. Per informazioni, consultare la Amazon Elastic Compute Cloud (Amazon EC2) - log a livello di sistema.	CloudWatch Registri:/{} *instance ID*

	Nome servizio	Dettagli del registro	Posizione del registro
7	Amazon Elastic File System (Amazon EFS)	Solo registrazione delle chiamate API.	CloudWatch LogGroup://Landing-Zone-Logs CloudTrail Bucket S3 [nell'account di registrazione centrale]: - {} - {} aws-landing-zone-logs *account_ID region* Percorso:/{} AWSLogs*account_ID* //CloudTrail
8	Elastic Load Balancing (ELB)	Voci del registro degli accessi e degli errori. Gli Elastic Load Balancer registrano tutte le richieste loro inviate, comprese le richieste che non vengono indirizzate alle istanze di back-end. Ad esempio, se un client invia una richiesta con formato errato o non ci sono istanze integre a cui rispondere, la richiesta viene comunque registrata. Per ulteriori informazioni sulle voci di registro di Elastic Load Balancing, vedere • Classic Load Balancers: accesso alle voci di registro. • Application Load Balancers: accesso alle voci di registro. • Network Load Balancer: accesso alle voci di registro.	Registri delle chiamate API: CloudWatch LogGroup:/CloudTrail/Log delle zone di destinazione Bucket S3 [nell'account di registrazione centrale]: - {} - {} aws-landing-zone-logs *account_ID region* Percorso:/{} AWSLogs*account_ID* //CloudTrail Registri di accesso: Bucket S3: mc-a {} -logs {} *account_ID region* Percorso: aws/elbaccess

	Nome servizio	Dettagli del registro	Posizione del registro
9	OpenSearch Servizio Amazon (OpenSearch servizio)	Registri degli errori del servizio. È necessario abilitare OpenSearch esplicitamente la registrazione. Per informazioni, consultare, Abilitazione della registrazione per i servizi supportati	CloudWatch LogGroup://Landing-Zone-Logs CloudTrail Bucket S3 [nell'account di registrazione centrale]: - {} - {} aws-landing-zone-logs *account_ID region* Percorso:/{} AWSLogs*account_ID* //CloudTrail
10	Amazon ElastiCache	Solo registrazione delle chiamate API.	CloudWatch LogGroup:///Landing-Zone-Logs CloudTrail Bucket S3 [nell'account di registrazione centrale]: - {} - {} aws-landing-zone-logs *account_ID region* Percorso:/{} AWSLogs*account_ID* //CloudTrail
11	Amazon GuardDuty		
12	Amazon Inspector		
13	Amazon Macie		
14	Amazon Redshift	Registri di connessioni, utenti e attività. La registrazione è abilitata per impostazione predefinita quando crei il tuo cluster Redshift richiamando il Create Redshift cluster CT (ct-1malj7snzxrkr). Per informazioni, consulta Database Audit Logging.	Bucket S3: ams-a {} -log-management- {} *account_ID region* Percorso: /AWS//{} RedShift *CloudFront Distribution ID*

	Nome servizio	Dettagli del registro	Posizione del registro
15	Amazon Relational Database Service (RDS)	Registri specifici per tipo di database. È necessario abilitare esplicitamente la registrazione RDS. Per informazioni, consultare, Abilitazione della registrazione per i servizi supportati È possibile accedere ai log MSSQL solo tramite una procedura memorizzata; per informazioni, vedere Archiviazione dei file di registro.	CloudWatch LogGroup: /aws/rds/ (o)/{}/{} *instance cluster database_name log_name*
16	Amazon S3 (S3)	Registri di accesso ai bucket. Ogni record del registro di accesso fornisce dettagli su una singola richiesta di accesso, ad esempio il richiedente, il nome del bucket, l'ora della richiesta, l'azione della richiesta, lo stato della risposta e il codice di errore (se presente). Il log di accesso può essere utile nei controlli di accesso e di sicurezza. Può essere utile anche per comprendere la base clienti e la fattura Amazon S3. Per ulteriori informazioni sulle voci di S3 Access Log, consulta S3 Server Access Log Format.	Bucket S3: mc-a {} -log-management- {} *account_ID region* Percorso: *bucket_name* /aws/s3access/ {} Bucket S3 [nell'account di registrazione centrale]: 3-access-logs- {} - {} aws-landing-zone-s *account_ID region* Percorso:/

	Nome servizio	Dettagli del registro	Posizione del registro
17	Amazon Simple Email Service (SES)	Chiamate al servizio API SES.	CloudWatch LogGroup:/CloudTrail/Log della zona di destinazione Bucket S3 [nell'account di registrazione centrale]: - {} - {} aws-landing-zone-logs *account_ID region* Percorso:/{} AWSLogs*account_ID* //CloudTrail
18	Amazon Virtual Private Cloud (VPC)	Dati sul flusso VPC (informazioni sul traffico IP in entrata e in uscita dalle interfacce di rete del tuo VPC).	CloudWatch LogGroup: /aws/vpcflow/ {} *VPC_ID*
19	Auto Scaling	Solo registrazione delle chiamate API.	CloudWatch LogGroup://Landing-Zone-Logs CloudTrail Bucket S3 [nell'account di registrazione centrale]: - {} - {} aws-landing-zone-logs *account_ID region* Percorso:/{} AWSLogs*account_ID* //CloudTrail
20	AWS Certificate Manager		
21	AWS CodeDeploy	Registri di distribuzione specifici dell'istanza.	A istanza

	Nome servizio	Dettagli del registro	Posizione del registro
22	AWS Config	Chiamate al servizio API AWS Config.	CloudWatch LogGroup://Landing-Zone-Logs CloudTrail Bucket S3 [nell'account di registrazione centrale]: - {} - {} aws-landing-zone-logs *account_ID region* Percorso:/{} AWSLogs*account_ID* //CloudTrail
		Modifiche alla configurazione delle risorse, come rilevato da AWS Config.	Bucket S3 [nell'account di registrazione centrale]: aws-landing-zone-logs - {} - {} *account_ID region* Percorso:AWSLogs/{*account_ID* } /Config/
23	AWS Database Migration Service	Registri di migrazione del database. Per informazioni, consulta Introduzione alla gestione dei log in AWS Database Migration Service.	Console di migrazione del database
24	AWS Direct Connect (DX)	Solo registrazione delle chiamate API.	CloudWatch LogGroup://Landing-Zone-Logs CloudTrail
25	AWS Glacier		Bucket S3 [nell'account di registrazione centrale]: - {} - {} aws-landing-zone-logs *account_ID region* Percorso:/{} AWSLogs*account_ID* //CloudTrail
26	AWS IAM (IAM)		
27	AWS Key Management Service		

	Nome servizio	Dettagli del registro	Posizione del registro
28	Console di gestione AWS (console o console AWS)		
29	AWS Simple Notification Service (SNS)		
30	AWS Simple Queueing Service (SQS)		

Single-Account Landing Zone

Registri di servizio aggregati AMS per conto singolo delle landing zone

	Nome servizio	Dettagli del registro	Posizione del registro
1	Amazon Aurora	Log generali, di interrogazioni lente e di errori.	CloudWatch LogGroup: /aws/rds/cluster/{*database_name* }/{*log_name*}
2	Amazon CloudFormation (CloudFormation o CFN)	Solo registrazione delle chiamate API.	CloudFormation Le chiamate API sono documentate tramite CloudTrail, che invia i log a CloudWatch LogGroup e quindi li sincronizza in un bucket S3. CloudWatch LogGroup: /aws/ams/cloudtrail Bucket S3: ams-a {} -log-management- {} *account_ID region*

	Nome servizio	Dettagli del registro	Posizione del registro
3	Amazon CloudFront (CloudFront)	Registrazione delle richieste degli utenti. È necessario abilitare CloudFront esplicitamente la registrazione. Per informazioni, consultare, Abilitazione della registrazione per i servizi supportati	Bucket S3: ams-a {} -log-management- {} *account_ID region* Percorso: AWS/RedShift/{} *CloudFront_distribution_ID*
4	Amazon CloudWatch (CloudWatch)	Solo registrazione delle chiamate API.	CloudWatch LogGroup: /aws/ams/cloudtrail
5	Amazon Elastic Block Store (EBS)	Il servizio EBS non produce alcun registro.	Non applicabile
6	Amazon Elastic Compute Cloud () EC2	Log di sistema e delle applicazioni. Per informazioni, consultare la Amazon Elastic Compute Cloud (Amazon EC2) - log a livello di sistema.	CloudWatch Registri:/{} *instance_ID*
7	Amazon Elastic File System (Amazon EFS)	Solo registrazione delle chiamate API.	CloudWatch LogGroup: /aws/ams/cloudtrail

	Nome servizio	Dettagli del registro	Posizione del registro
8	Elastic Load Balancing (ELB)	Voci del registro degli accessi e degli errori. Gli Elastic Load Balancer registrano tutte le richieste loro inviate, comprese le richieste che non vengono indirizzate alle istanze di back-end. Ad esempio, se un client invia una richiesta con formato errato o non ci sono istanze integre a cui rispondere, la richiesta viene comunque registrata. Per ulteriori informazioni sulle voci di registro di Elastic Load Balancer, vedere • Classic Load Balancers: accesso alle voci di registro. • Application Load Balancers: accesso alle voci di registro. • Network Load Balancer: accesso alle voci di registro.	CloudWatch LogGroup: /aws/ams/cloudtrail Bucket S3: mc-a {} -logs- {} *account_ID region* Percorso: aws/elbaccess
9	OpenSearch Servizio Amazon (OpenSearch servizio)	Registri degli errori del servizio. È necessario abilitare OpenSearch esplicitamente la registrazione. Per informazioni, consultare, Abilitazione della registrazione per i servizi supportati	CloudWatch LogGroup: /aws/ams/cloudtrail
10	Amazon ElastiCache	Solo registrazione delle chiamate API.	CloudWatch LogGroup: /aws/ams/cloudtrail

	Nome servizio	Dettagli del registro	Posizione del registro
11	Amazon GuardDuty		
12	Amazon Inspector		
13	Amazon Macie		
14	Amazon Redshift	Registri di connessioni, utenti e attività. La registrazione è abilitata per impostazione predefinita quando crei il tuo cluster Redshift richiamando il Create Redshift cluster CT (ct-1malj7snzxrkr). Per informazioni, consulta Database Audit Logging.	Bucket S3: ams-a {} -log-management- {} *account_ID region* Percorso: /AWS//{} RedShift *CloudFront_Distribution_ID*
15	Amazon Relational Database Service (RDS)	Registri specifici per tipo di database. La registrazione RDS deve essere abilitata in modo esplicito. Per informazioni, consultare, Abilitazione della registrazione per i servizi supportati È possibile accedere ai log MSSQL solo tramite una procedura memorizzata; per informazioni, vedere Archiviazione dei file di registro.	CloudWatch LogGroup: /aws/rds/ (instance|cluster)/{nome del database}/{nome log}

	Nome servizio	Dettagli del registro	Posizione del registro
16	Amazon S3 (S3)	Registri di accesso ai bucket. Ogni record del log di accesso fornisce dettagli su una singola richiesta di accesso, ad esempio: richieden te, nome del bucket, ora della richiesta, azione della richiesta , stato della risposta e codice di errore (se presente). Le informazi oni sui log di accesso possono essere utili per i controlli di sicurezza e di accesso; possono anche aiutarti a conoscere la tua base di clienti e a comprendere la tua fattura Amazon S3. Per ulteriori informazioni sulle voci del registro di accesso di S3, consulta S3 Server Access Log Format.	Bucket S3: mc-a {} -log-mana gement- {} *account_ID region* Percorso: *bucket_name* /aws/ s3access/ {}
17	Amazon Simple Email Service (SES)	Chiamate al servizio API SES.	CloudWatch LogGroup: /aws/ams/ cloudtrail Bucket S3: ams-a {} -log-mana gement- {*account_ID* } *region* Percorso:/{}/{} AWS/Cloud Trail/AWSLogs *account_ID* CloudTrail *region*
18	Amazon Virtual Private Cloud (VPC)	Dati sul flusso VPC (informazioni sul traffico IP in entrata e in uscita dalle interfacce di rete del tuo VPC).	CloudWatch LogGroup: /aws/vpcf low/ {vpc_id}

	Nome servizio	Dettagli del registro	Posizione del registro
19	Auto Scaling	Solo registrazione delle chiamate API.	CloudWatch LogGroup: /aws/ams/cloudtrail
20	AWS Certificate Manager		
21	AWS CodeDeploy	Registri di distribuzione specifici dell'istanza.	Ad esempio
22	AWS Config	Chiamate al servizio API AWS Config.	CloudWatch LogGroup: /aws/ams/cloudtrail Bucket S3: ams-a {} -log-management- {} *account_ID region* Percorso:/{}/{} AWS/CloudTrail/AWSLogs *account_ID* CloudTrail *region*
23	AWS Database Migration Service	Registri di migrazione del database. Per informazioni, consulta Introduzione alla gestione dei log in AWS Database Migration Service.	Console di migrazione del database
24	AWS Direct Connect (DX)	Solo registrazione delle chiamate API.	CloudWatch LogGroup: /aws/ams/cloudtrail
25	AWS Glacier		
26	AWS IAM (IAM)		
27	AWS Key Management Service		

	Nome servizio	Dettagli del registro	Posizione del registro
28	Console di gestione AWS (console o console AWS)		
29	AWS Simple Notification Service (SNS)		
30	AWS Simple Queueing Service (SQS)		

Log dei servizi condivisi AMS

La tabella seguente descrive i log e la posizione dei log per gli AMS Shared Services presenti nel tuo account.

Per accedere ai tuoi log, assicurati di avere uno dei ruoli IAM richiesti e di essere nel tuo account AMS. Quindi vai alla directory mostrata.

Registrazione dei servizi condivisi per zona di atterraggio con account singolo AMS

	Nome del servizio condiviso	Dettagli del registro	Posizione del registro
1	Host bastione	Informazioni relative agli utenti che accedono all'host bastion.	Linux Bastions: CloudWatch Registri:/{instance id}/var/log/secure CloudWatch Registri:/{instance id}/.log var/log/audit/audit Bastioni di Windows:

	Nome del servizio condiviso	Dettagli del registro	Posizione del registro
			CloudWatch Registri:/{instance id}/SecurityEventLog
2	Host di gestione	Produzione di script, che aiutano nelle azioni automatizzate di gestione degli accessi all'interno dell'account.	CloudWatch Registri:/{instance id}/ApplicationEventLog
4	Host EPS (DSM)	Informazioni relative alla registrazione delle istanze sulla piattaforma Deep Security Management.	CloudWatch Registri:/{instance id}/.log var/log/DSM
5	Servizi di directory	Informazioni relative all'accesso all'account, alla gestione dell'account, al tracciamento dettagliato, all'accesso agli oggetti, alla modifica delle politiche e all'uso dei privilegi all'interno della directory dell'account. È necessario abilitare esplicitamente la registrazione dei servizi di directory. Per informazioni, consulta Abilitazione della registrazione per i servizi supportati.	CloudWatch Registri: /aws/directoryservice/ {directory id} - {directory dns name}
6	Lambda	Emissione di vari lambda, che facilitano le azioni operative automatizzate all'interno dell'account.	CloudWatch Registri: /aws/lambda/{lambda name}

Registrazione dei servizi condivisi per zone di atterraggio con più account AMS

	Nome del servizio condiviso	Dettagli del registro	Posizione del registro
1	Bastioni	Emissione degli accessi alle istanze e degli errori di autenticazione.	Registri di Linux Bastions:/{}/ CloudWatch .log *instance_ID* var/log/secure CloudWatch Registri di Windows Bastions:/{}/*instance_ID* SecurityEventLog
2	Host di gestione	Output di scriptsy, che aiuta nelle azioni automatizzate di gestione degli accessi all'interno dell'account.	CloudWatch Registri:/{}*instance_ID* /ApplicationEventLog
3	Host EPS (DSM)	Informazioni relative alla registrazione delle istanze sulla piattaforma Deep Security Management.	CloudWatch Registri:/{}/.log *instance_ID* var/log/DSM
4	Servizi di directory	Informazioni relative all'accesso all'account, alla gestione dell'account, al tracciamento dettagliato, all'accesso agli oggetti, alla modifica delle politiche e all'uso dei privilegi all'interno della directory dell'account. È necessario abilitare esplicitamente la registrazione dei servizi di directory. Per informazioni, consulta Abilitazione della registrazione per i servizi supportati.	CloudWatch Registri: /aws/directoryservice/ {} - {} *directory_ID directory_DNS_name*

	Nome del servizio condiviso	Dettagli del registro	Posizione del registro
5	Lambda	Emissione di vari lambda, che facilitano le azioni operative automatizzate all'interno dell'account.	CloudWatch Registri: /aws/lambda/ {} *Lambda_name*

Amazon Elastic Compute Cloud (Amazon EC2) - log a livello di sistema

I log delle istanze vengono raccolti da un agente CloudWatch Logs in esecuzione sull'istanza e sono accessibili tramite un gruppo di CloudWatch log con lo stesso nome dell'istanza. Ad esempio, se l'ID dell'istanza è i-0123456789abcdef0 e il nome del file di registro è/. var/log/messages, the Log Group would be i-0123456789abcdef0 and the Log Stream /var/log/messages

Consulta anche Log di servizio aggregati AMS.

Per accedere ai tuoi log, assicurati di avere uno dei ruoli IAM richiesti e di essere registrato nel tuo account AMS. Quindi vai alla directory mostrata.

> **Note**
>
> I seguenti registri vengono raccolti per impostazione predefinita.

Amazon Linux/ Red Hat Linux/Centos Linux/Ubunt/SUSE Linux

File di registro//Flusso di registro

```
/var/log/amazon/ssm/amazon-ssm-agent.log
/var/log/amazon/ssm/errors.log
/var/log/audit/audit.log
/var/log/cloud-init-output.log
/var/log/cfn-init.log
/var/log/cfn-init-cmd.log
/var/log/cloud-init.log (Amazon Linux 1 / Amazon Linux 2 only)
/var/log/cron
/var/log/dnf.log
/var/log/maillog
/var/log/messages
```

```
/var/log/secure
/var/log/spooler
/var/log/yum.log
/var/log/aws/ams/bootstrap.log
/var/log/aws/ams/build.log
/var/log/syslog
/var/log/dpkg.log
/var/log/auth.log
/var/log/zypper.log
```

> **Note**
>
> Per informazioni sull'accesso ai log per Amazon Linux 2023, consulta Perché nella directory /var/log mancano i log nella mia istanza EC2 Amazon Linux 2023?

Windows

File di log/Stream di log

```
SecurityEventLog
SystemEventLog
AmazonSSMAgentLog
MicrosoftWindowsAppLockerMSIAndScriptEventLog
MicrosoftWindowsAppLockerEXEAndDLLEventLog
AmazonCloudWatchAgentLog
EC2ConfigServiceEventLog (Windows Server 2012 R2 Only)
ApplicationEventLog
AmazonCloudFormationLog
MicrosoftWindowsGroupPolicyOperationalEventLog
AmazonSSMErrorLog
```

Integrazione con Splunk

AMS supporta i servizi di analisi push to customer log basati su AWS Lambda, come Splunk.

AMS sfrutta il componente aggiuntivo Splunk per i servizi Web Amazon, che consente lo streaming di dati AWS su Splunk. Vedi Requisiti hardware e software.

Fai riferimento a questo post del blog Splunk Come eseguire lo streaming di AWS CloudWatch Logs su Splunk (suggerimento: è più facile di quanto pensi). Poiché lo streaming dei CloudWatch

log è abilitato di default per i clienti AMS e AMS configura la funzione AWS Lambda per te, tuttavia devi configurare l'input Splunk HTTP Event Collector (HEC) e inviare una richiesta ad AMS per le funzionalità aggiuntive.

Ecco come potrebbero apparire le impostazioni di immissione dei dati:

Personalizzazione della configurazione dei registri

È possibile modificare la conservazione dei dati di CloudWatch log per i log e abilitare la registrazione per servizi AWS aggiuntivi.

Alterazione della conservazione dei CloudWatch log

È possibile modificare l'impostazione di conservazione dei dati di registro per i CloudWatch registri. Per impostazione predefinita, i log vengono conservati a tempo indeterminato e non scadono mai. Puoi modificare la policy di conservazione per ogni gruppo di log mantenendo la conservazione a tempo indeterminato o scegliendo periodi di conservazione compresi tra 10 anni e un giorno. Per visualizzare il periodo di conservazione minimo consentito in AMS, consulta il documento sugli standard tecnici AMS disponibile tramite AWS Artifact. Per accedere ad AWS Artifact, contatta il tuo CSDM per ricevere istruzioni o consulta la sezione Getting Started with AWS Artifact.

La funzionalità di conservazione CloudWatch dei log elimina gli eventi di registro in un flusso in base alla politica di conservazione. Non elimina i flussi di log o i gruppi di log. Per informazioni generali, consulta la Amazon CloudWatch Logs User Guide What is Amazon CloudWatch Logs? .

Per informazioni sulla personalizzazione di un periodo di conservazione dei log e per ulteriori informazioni, consulta Change Log Data Retention in CloudWatch Logs.

Abilitazione della registrazione per i servizi supportati

Per impostazione predefinita, alcuni servizi non hanno la registrazione abilitata e richiedono un'abilitazione esplicita.

Per abilitare la registrazione per Amazon RDS e Route53 CloudFront OpenSearch, invia una RFC con il tipo Management | Other | Other | Create change (ct-1e1xtak34nx76) con i seguenti valori, sostituendoli se necessario: *`variables`*

```
Subject: Enable logging for SERVICE_NAME
```

```
Description: Service ARN: SERVICE_ARN
```

Gestione della sicurezza

La gestione della sicurezza di AWS Managed Services (AMS) è il processo mediante il quale AMS identifica le risorse di un'organizzazione e implementa politiche e procedure per proteggere tali risorse.

> **Note**
>
> AMS ora dispone di un certificato di modifica del tipo (CT), Deployment | Advanced stack components | ACM con certificato aggiuntivo SANs | Create (ct-3l14e139i5p50), che puoi utilizzare per inviare una richiesta di certificato. AWS Certificate Manager Per informazioni, consulta AWS::CertificateManager::Certificate. Questo CT prevede la creazione di un nome alternativo del soggetto (SAN) aggiuntivo.

Per comprendere meglio la AWS sicurezza generale, consulta Best Practices for Security, Identity and Compliance.

AMS classifica i rischi per la sicurezza come segue:

- Rischi noti rilevati dall'antimalware, gestiti dal processo di mitigazione del malware.
- Eventi di sicurezza, incluse le violazioni dell'accesso, gestite dal processo di gestione degli eventi di sicurezza.

Argomenti

Protezione dei dati in AMS

AMS monitora continuamente gli account gestiti sfruttando AWS servizi nativi come Amazon GuardDuty, Amazon Macie (opzionalmente) e altri strumenti e processi proprietari interni. Dopo l'attivazione di un allarme, AMS si assume la responsabilità della valutazione iniziale e della risposta

all'allarme. I nostri processi di risposta si basano sugli standard NIST. AMS testa regolarmente i propri processi di risposta utilizzando Security Incident Response Simulation con voi per allineare il flusso di lavoro ai programmi di risposta alla sicurezza dei clienti esistenti.

Quando AMS rileva una violazione o una minaccia imminente di violazione delle vostre politiche di AWS sicurezza, raccoglie informazioni, comprese le risorse interessate e qualsiasi modifica relativa alla configurazione. AMS fornisce follow-the-sun assistenza 24 ore su 24, 7 giorni su 7, 365 giorni all'anno, con operatori dedicati che esaminano e esaminano attivamente le dashboard di monitoraggio, la coda degli incidenti e le richieste di assistenza su tutti gli account gestiti. AMS esamina i risultati con i nostri esperti di sicurezza per analizzare l'attività e inviarti notifiche tramite i contatti di sicurezza indicati nel tuo account.

Sulla base dei nostri risultati, AMS interagisce con te in modo proattivo. Se ritieni che l'attività non sia autorizzata o sospetta, AMS collabora con te per indagare e risolvere o contenere il problema. Alcuni tipi di risultati generati da AMS richiedono la conferma dell'impatto prima GuardDuty che AMS sia in grado di intraprendere qualsiasi azione. Ad esempio, il tipo di GuardDuty risultato UnauthorizedAccess:IAMUser/ConsoleLoginindica che uno dei tuoi utenti ha effettuato l'accesso da una posizione insolita; AMS ti avvisa e ti chiede di esaminare i risultati per confermare se questo comportamento è legittimo.

Amazon Macie

AWS Managed Services consiglia di utilizzare Macie per rilevare un elenco ampio e completo di dati sensibili, come informazioni sanitarie personali (PHI), informazioni di identificazione personale (PII) e dati finanziari.

Macie può essere configurato per essere eseguito periodicamente su qualsiasi bucket Amazon S3, automatizzando nel tempo la valutazione di qualsiasi oggetto nuovo o modificato all'interno di un bucket. Man mano che vengono generati i risultati di sicurezza, AMS ti avviserà e collaborerà con te per correggerli, se necessario.

Per ulteriori informazioni, consulta Analizzare i risultati di Amazon Macie.

Sicurezza di Amazon Macie

Macie è un servizio di sicurezza intelligence/AI alimentato artificialmente che aiuta a prevenire la perdita di dati rilevando, classificando e proteggendo automaticamente i dati sensibili archiviati in AWS. Macie utilizza l'apprendimento automatico per riconoscere dati sensibili come le informazioni di identificazione personale (PII) o la proprietà intellettuale, assegna un valore aziendale e fornisce

visibilità su dove sono archiviati questi dati e su come vengono utilizzati nell'organizzazione. Macie monitora continuamente l'attività di accesso ai dati per rilevare eventuali anomalie e invia avvisi quando rileva il rischio di accessi non autorizzati o fughe involontarie di dati. Il servizio Macie supporta Amazon S3 AWS CloudTrail e fonti di dati.

AMS monitora continuamente gli avvisi provenienti da Macie e, se viene avvisato, intraprende azioni rapide per proteggere le risorse e l'account. Con l'aggiunta di Macie all'elenco dei servizi supportati da AMS, ora siamo anche responsabili dell'abilitazione e della configurazione di Macie in tutti i tuoi account, secondo le tue istruzioni. Puoi visualizzare gli avvisi di Macie e le nostre azioni man mano che si svolgono nella console AWS o nelle integrazioni supportate. Durante l'onboarding dell'account, puoi indicare gli account che usi per archiviare le informazioni personali. Per tutti i nuovi account con PII, consigliamo di utilizzare Macie. Per gli account esistenti con PII, contattaci e provvederemo ad attivarli nel tuo account. Di conseguenza, puoi avere a disposizione un ulteriore livello di protezione e usufruire di tutti i vantaggi di Macie nel tuo ambiente AWS gestito da AMS.

AMS Macie FAQs

- Perché ho bisogno di Macie quando tutti gli account AMS dispongono di Trend Micro e GuardDuty sono abilitati?

  Macie ti aiuta a proteggere i tuoi dati in Amazon S3 aiutandoti a classificare i dati di cui disponi, il valore che i dati hanno per l'azienda e il comportamento associato all'accesso a tali dati. Amazon GuardDuty offre un'ampia protezione degli account, dei carichi di lavoro e dei dati AWS aiutando a identificare minacce come la ricognizione degli attori delle minacce, il problema delle istanze e l'attività problematica dell'account. Entrambi i servizi incorporano l'analisi del comportamento degli utenti, l'apprendimento automatico e il rilevamento delle anomalie per rilevare le minacce nelle rispettive categorie. Trend Micro non si concentra sull'identificazione delle informazioni personali e delle relative minacce.

- Come faccio ad attivare Macie nel mio account AMS?

  Se l'hai PII/PHI archiviato nei tuoi account o hai intenzione di archiviarlo, contatta il tuo CSDM o invia una richiesta di assistenza per abilitare Macie per i tuoi account nuovi o esistenti gestiti da AMS.

- Quali sono le implicazioni in termini di costi dell'attivazione di Macie nel mio account AMS?

  I prezzi di Macie funzionano per AMS in modo simile ad altri servizi come Amazon Elastic Compute Cloud (Amazon EC2). Paghi per Amazon Macie in base all'utilizzo e un upgrade AMS in base al tuo. SLAs Le tariffe di Macie si basano sull'utilizzo, consulta i prezzi di Amazon Macie, calcolati

in AWS CloudTrail base agli eventi e allo storage Amazon S3. Tieni presente che i costi di Macie tendono a diminuire a partire dal secondo mese dopo l'attivazione, perché si basano sui dati incrementali aggiunti ai bucket Amazon S3.

Per ulteriori informazioni su Macie, consulta Amazon Macie.

GuardDuty

GuardDuty è un servizio di monitoraggio continuo della sicurezza che utilizza feed di intelligence sulle minacce, come elenchi di indirizzi IP e domini dannosi, e l'apprendimento automatico per identificare attività impreviste e potenzialmente non autorizzate e dannose all'interno dell'ambiente AWS. Ciò può includere problemi come l'aumento dei privilegi, l'uso di credenziali esposte o la comunicazione con indirizzi IP o domini dannosi. GuardDuty monitora anche il comportamento di accesso all'account Amazon Web Services per rilevare segnali di compromissione, come installazioni di infrastrutture non autorizzate, come istanze distribuite in una regione che non è mai stata utilizzata, o chiamate API insolite, come una modifica della politica delle password per ridurre la sicurezza delle password. Per ulteriori informazioni, consulta la Guida per l'utente. GuardDuty

Per visualizzare e analizzare i GuardDuty risultati, utilizzare la procedura seguente.

1. Apri la GuardDuty console.
2. Scegliete Risultati, quindi scegliete un risultato specifico per visualizzare i dettagli. I dettagli di ogni risultato variano a seconda del tipo di scoperta, delle risorse coinvolte e della natura dell'attività.

Per ulteriori informazioni sui campi di ricerca disponibili, vedere i dettagli dei GuardDuty risultati.

GuardDuty sicurezza

Amazon GuardDuty offre il rilevamento delle minacce che ti consente di monitorare e proteggere continuamente i tuoi account e carichi di lavoro AWS. Amazon GuardDuty analizza i flussi continui di metadati generati dall'account e dall'attività di rete presenti negli eventi, nei log di flusso di AWS CloudTrail Amazon VPC e nei log di Domain Name System (DNS). Utilizza anche informazioni integrate sulle minacce, come indirizzi IP malevoli noti, rilevamento delle anomalie e apprendimento automatico per identificare le minacce con maggiore precisione. GuardDuty è un servizio AMS monitorato. Per ulteriori informazioni sul GuardDuty monitoraggio di Amazon, consultaGuardDuty monitoraggio. Per ulteriori informazioni GuardDuty, consulta Amazon GuardDuty.

Tutti i nuovi account AMS sono GuardDuty abilitati per impostazione predefinita. AMS si configura GuardDuty durante l'onboarding dell'account. È possibile inviare richieste di modifica per modificare le impostazioni in qualsiasi momento. GuardDuty i prezzi funzionano per AMS in modo simile ad altri servizi come Amazon Elastic Compute Cloud (Amazon EC2). Paghi GuardDuty in base all'utilizzo e un upgrade AMS in base al tuo. SLAs GuardDuty le tariffe si basano sull'utilizzo (Amazon GuardDuty Pricing), misurato in base AWS CloudTrail agli eventi e al volume del log di flusso Amazon VPC.

Per GuardDuty AMS, sono abilitate le seguenti categorie di rilevamento primarie:

- Ricognizione: attività che suggeriscono la ricognizione da parte di un autore della minaccia, ad esempio attività insolite delle API, scansione delle porte intra-VPC, modelli insoliti di richieste di accesso non riuscite o sondaggio delle porte sbloccato da un IP noto non valido.
- Problema relativo all'istanza: attività problematica delle istanze, come il mining di criptovalute, il malware che utilizza algoritmi di generazione del dominio (DGA), attività di tipo Denial of Service in uscita, volume di traffico di rete insolitamente elevato, protocolli di rete insoliti, comunicazione tra istanze in uscita con un IP malevolo noto, EC2 credenziali Amazon temporanee utilizzate da un indirizzo IP esterno ed esfiltrazione di dati tramite DNS.
- Attività dell'account: i modelli più comuni indicativi dell'attività dell'account includono chiamate API da un proxy di geolocalizzazione o anonimizzazione insolito, tentativi di disabilitare la AWS CloudTrail registrazione, lanci insoliti di istanze o infrastrutture, implementazioni di infrastrutture in una regione AWS insolita e chiamate API da indirizzi IP dannosi noti.

AMS utilizza i GuardDuty tuoi account gestiti per monitorare continuamente i risultati e gli avvisi e, se viene avvisato, AMS Operations intraprende azioni proattive per proteggere le tue risorse GuardDuty e il tuo account. Puoi visualizzare GuardDuty i risultati e le nostre azioni man mano che si svolgono nella console AWS o nelle integrazioni supportate.

GuardDuty funziona con Trend Micro Deep Security Manager nel tuo account. Trend Micro Deep Security Manager fornisce servizi di rilevamento delle intrusioni e prevenzione delle intrusioni basati su host. I servizi Trend Micro Web Reputation hanno alcune GuardDuty somiglianze con la capacità di rilevare quando un host sta tentando di comunicare con un host o un servizio Web noto per essere una minaccia. Tuttavia, GuardDuty fornisce ulteriori categorie di rilevamento delle minacce e lo fa monitorando il traffico di rete, un metodo complementare al rilevamento basato su host di Trend Micro. Il rilevamento delle minacce basato sulla rete consente una maggiore sicurezza evitando che i controlli falliscano se l'host mostra un comportamento problematico. AMS consiglia di utilizzarlo GuardDuty in tutti gli account AMS.

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.

GuardDuty monitoraggio

GuardDuty ti informa sullo stato del tuo ambiente AWS producendo risultati di sicurezza che AMS acquisisce e può segnalare.

Amazon GuardDuty monitora la sicurezza del tuo ambiente AWS analizzando ed elaborando i log di flusso VPC, i log degli AWS CloudTrail eventi e i log del Domain Name System. Puoi ampliare questo ambito di monitoraggio configurando l'utilizzo anche GuardDuty di elenchi di IP e di minacce personalizzati e affidabili.

- Gli elenchi di IP affidabili sono costituiti da indirizzi IP a cui hai consentito la comunicazione sicura con l'infrastruttura e le applicazioni AWS. GuardDuty non genera risultati per gli indirizzi IP negli elenchi di IP affidabili. In qualsiasi momento, puoi avere soltanto un elenco di IP affidabili caricati per account AWS per regione.
- Gli elenchi di minacce sono costituiti da indirizzi IP dannosi noti. GuardDuty genera risultati basati su elenchi di minacce. In qualsiasi momento, puoi avere fino a sei elenchi di minacce caricati per account AWS per regione.

Per l'implementazione GuardDuty, utilizza AMS CT Deployment | Monitoraggio e notifica | GuardDuty IP set | Create (ct-08avsj2e9mc7g) per creare un set di indirizzi IP approvati. Puoi anche utilizzare AMS CT Deployment | Monitoring and notification | GuardDuty threat intel set | Create (ct-25v6r7t8gvkq5) per creare un set di indirizzi IP negati.

Per un elenco Cosa monitora il sistema di monitoraggio AMS? dei servizi monitorati da AMS, consulta.

Firewall DNS Amazon Route 53 Resolver

Amazon Route 53 Resolver risponde in modo ricorsivo alle richieste DNS provenienti da risorse AWS per record pubblici, nomi DNS specifici di Amazon VPC e zone ospitate private di Amazon Route 53 ed è disponibile per impostazione predefinita in tutti. VPCs Con il DNS Firewall per Route 53 Resolver è possibile filtrare e regolare il traffico DNS in uscita per il proprio cloud privato virtuale. A tale scopo, è possibile creare raccolte riutilizzabili di regole di filtro nei gruppi di regole di DNS Firewall, associare i gruppi di regole al VPC e quindi monitorare l'attività nei record e nei parametri di DNS Firewall. In base all'attività, è possibile regolare di conseguenza il comportamento di DNS Firewall. Per ulteriori informazioni, consulta Usare DNS Firewall per filtrare il traffico DNS in uscita.

Per visualizzare e gestire la configurazione del firewall DNS di Route 53 Resolver, utilizzare la seguente procedura:

1. Accedi Console di gestione AWS e apri la console Amazon VPC all'indirizzo. https://console.aws.amazon.com/vpc/
2. In DNS Firewall, scegli Gruppi di regole.
3. Rivedi, modifica o elimina la configurazione esistente o crea un nuovo gruppo di regole. Per ulteriori informazioni, consulta Come funziona Route 53 Resolver DNS Firewall.

Monitoraggio e sicurezza del firewall DNS di Amazon Route 53 Resolver

Amazon Route 53 DNS Firewall utilizza i concetti di associazione di regole, azione delle regole e priorità di valutazione delle regole. Un elenco di domini è un insieme riutilizzabile di specifiche di dominio utilizzate in una regola DNS Firewall all'interno di un gruppo di regole. Quando associ un gruppo di regole a un VPC, DNS Firewall confronta le query DNS con gli elenchi di dominio utilizzati nelle regole. Se DNS Firewall trova una corrispondenza, gestisce la query DNS in base all'azione della regola corrispondente. Per ulteriori informazioni sui gruppi di regole e sulle regole, consulta Gruppi di regole e regole del firewall DNS.

Gli elenchi di domini rientrano in due categorie principali:

- Elenchi di domini gestiti, che AWS creano e gestiscono per te.
- Elenchi di domini personalizzati, creati e gestiti dall'utente.

I gruppi di regole vengono valutati in base all'indice di priorità delle associazioni.

Per impostazione predefinita, AMS implementa una configurazione di base costituita dalle seguenti regole e gruppi di regole:

- Un gruppo di regole denominato. `DefaultSecurityMonitoringRule` Il gruppo di regole ha la massima priorità di associazione disponibile al momento della creazione per ogni VPC esistente in ogni VPC abilitato. Regione AWS
- Una regola denominata `DefaultSecurityMonitoringRule` con priorità 1 all'interno del gruppo di `DefaultSecurityMonitoringRule` regole, utilizzando l'elenco dei domini `AWSManagedDomainsAggregateThreatList` gestiti con l'azione ALERT.

Se si dispone di una configurazione esistente, la configurazione di base viene distribuita con una priorità inferiore rispetto alla configurazione esistente. La configurazione esistente è quella predefinita. La configurazione di base di AMS viene utilizzata come soluzione generica se la configurazione esistente non fornisce istruzioni con priorità più elevata su come gestire la risoluzione delle query. Per modificare o rimuovere la configurazione di base, esegui una delle seguenti operazioni:

- Contatta il tuo Cloud Service Delivery Manager (CSDM) o Cloud Architect (CA).
- Crea una richiesta di modifica (RFC) utilizzando Management | Other | Other | Create CT (ct-1e1xtak34nx76).
- Crea una richiesta di servizio.

Se il tuo account è gestito in modalità Sviluppatore o in modalità Direct Change, puoi eseguire tu stesso le modifiche.

AWS Certificate Manager Certificato (ACM)

AMS dispone di un certificato CT, Deployment | Advanced stack components | ACM con un certificato aggiuntivo SANs | Create (ct-3l14e139i5p50), che puoi utilizzare per inviare una richiesta di certificato AWS Certificate Manager, con un massimo di cinque nomi alternativi Subject (SAN) aggiuntivi (come example.com, example.net ed example.org). Per i dettagli, consulta What Is? AWS Certificate Manager e ACM Certificate Characteristic.

> **Note**
>
> Questa impostazione di timeout non riguarda solo l'esecuzione, ma anche la convalida del certificato ACM tramite la convalida via e-mail. Senza la tua convalida, la RFC fallisce.

Crittografia dei dati in AMS

AMS utilizza diversi AWS servizi per la crittografia dei dati, in particolare Amazon Simple Storage Service, AWS Key Management Service (AWS KMS), Amazon Elastic Block Store, Amazon Relational Database Service Amazon Redshift e Amazon OpenSearch Service. Amazon ElastiCache AWS Lambda

Amazon S3

Amazon S3 offre diverse opzioni di crittografia degli oggetti che proteggono i dati in transito e inattivi. La crittografia lato server crittografa l'oggetto prima di salvarlo su disco nei suoi data center e quindi lo decrittografa al momento del download. Se la richiesta è autenticata e sono disponibili le autorizzazioni per l'accesso, non c'è differenza nelle modalità di accesso agli oggetti, crittografati o meno. Per ulteriori informazioni, consulta Protezione dei dati in Amazon S3.

Amazon EBS

Con la crittografia Amazon EBS, non è necessario creare, mantenere e proteggere la propria infrastruttura di gestione delle chiavi. La crittografia Amazon EBS utilizza AWS KMS le chiavi durante la creazione di volumi e istantanee crittografati. Le operazioni di crittografia avvengono sui server che ospitano EC2 le istanze Amazon. Questo viene fatto per garantire che sia data-at-rest l'istanza che data-in-transit tra un'istanza e lo storage Amazon EBS collegato siano sicuri. A un'istanza possono essere collegati contemporaneamente sia volumi crittografati che non crittografati. Per ulteriori informazioni, consulta Crittografia Amazon EBS.

Amazon RDS

Amazon RDS può crittografare le tue istanze database di Amazon RDS. I dati crittografati a riposo includono lo storage sottostante per le istanze DB, i relativi backup automatici, le repliche di lettura e le istantanee. Le istanze DB crittografate con Amazon RDS utilizzano l'algoritmo di crittografia AES-256 standard del settore per crittografare i dati sul server che ospita le istanze database di Amazon RDS. Dopo la crittografia dei dati, Amazon RDS gestisce l'autenticazione dell'accesso e la decrittografia dei dati in modo trasparente con un impatto minimo sulle prestazioni. Non è quindi necessario modificare le applicazioni client di database per utilizzare la crittografia. Per ulteriori informazioni, consulta Crittografia delle risorse Amazon RDS.

Amazon Simple Queue Service

Oltre all'opzione predefinita di crittografia lato server gestita (SSE) di Amazon SQS, Amazon SQS-Managed SSE (SSE-SQS) consente di creare una crittografia lato server gestita personalizzata che utilizza chiavi di crittografia gestite da Amazon SQS per proteggere i dati sensibili inviati tramite code di messaggi. La crittografia lato server (SSE) consente di trasmettere dati sensibili in code crittografate. SSE protegge il contenuto dei messaggi nelle code utilizzando chiavi di crittografia gestite da Amazon SQS (SSE-SQS) o chiavi gestite in (SSE-KMS). AWS KMS Per informazioni sulla gestione di SSE tramite Encryption at rest, consulta Encryption at rest. Console di gestione AWS

Crittografia dei dati a riposo

OpenSearch I domini di servizio offrono la crittografia dei dati inattivi, una funzionalità di sicurezza che aiuta a prevenire l'accesso non autorizzato ai dati. La funzionalità utilizza AWS Key Management Service (AWS KMS) per archiviare e gestire le chiavi di crittografia e l'algoritmo Advanced Encryption Standard con chiavi a 256 bit (AES-256) per eseguire la crittografia. Per ulteriori informazioni, consulta Encryption of Data at Rest for Amazon OpenSearch Service.

Gestione delle chiavi

AWS KMS è un servizio gestito che semplifica la creazione e il controllo delle chiavi master dei clienti (CMKs), le chiavi di crittografia utilizzate per crittografare i dati. AWS KMS CMKs sono protetti da moduli di sicurezza hardware (HSMs) convalidati dal programma di convalida dei moduli crittografici FIPS 140-2 tranne nelle regioni Cina (Pechino) e Cina (Ningxia). Per ulteriori informazioni, consulta Che cos'è AWS Key Management Service?

Gestione dell'identità e degli accessi

AWS Identity and Access Management (IAM) è un servizio web che consente di controllare in modo sicuro l'accesso alle AWS risorse. Utilizza IAM per controllare chi è autenticato (accesso effettuato) e autorizzato (dispone di autorizzazioni) per l'utilizzo di risorse. Durante l'onboarding di AMS, sei responsabile della creazione di ruoli di amministratore IAM su più account all'interno di ciascuno dei tuoi account gestiti.

Protezioni IAM Multi-Account Landing Zone (MALZ)

AMS multi-account landing zone (MALZ) richiede un trust Active Directory (AD) come obiettivo di progettazione principale della gestione degli accessi AMS per consentire a ciascuna organizzazione (sia AMS che cliente) la gestione dei cicli di vita delle proprie identità. In questo modo si evita la necessità di avere le credenziali nelle rispettive directory. L'attendibilità unidirezionale è configurata in modo che l'Active Directory gestita all'interno della piattaforma Account AWS affidi l'AD di proprietà o gestito dal cliente per l'autenticazione degli utenti. Poiché la fiducia è solo unidirezionale, ciò non significa che l'AD gestito sia considerato attendibile dal cliente Active Directory.

In questa configurazione, la directory dei clienti che gestisce le identità degli utenti è nota come User Forest, mentre l'AD gestito a cui sono collegate EC2 le istanze Amazon è nota come Resource Forest. Si tratta di un modello di progettazione Microsoft comunemente utilizzato per l'autenticazione di Windows; per ulteriori informazioni, vedere Forest Design Models.

Questo modello consente a entrambe le organizzazioni di automatizzare i rispettivi cicli di vita e consente sia ad AMS che a te di revocare rapidamente l'accesso se un dipendente lascia

l'organizzazione. Senza questo modello, se entrambe le organizzazioni utilizzassero una directory comune (o la creassero users/groups nelle rispettive directory), entrambe dovrebbero inserire flussi di lavoro aggiuntivi e sincronizzare gli utenti per tenere conto dei dipendenti che iniziano e escono. Ciò comporta dei rischi, in quanto tale processo è latente e può essere soggetto a errori.

Prerequisiti di accesso MALZ

Integrazione con MALZ Identity Provider per l'accesso alla console AWS/AMS, CLI, SDK.

Affidabilità unidirezionale per EC2 le istanze Amazon nel tuo account AMS.

Autenticazione con identità

AMS utilizza i ruoli IAM, che sono un tipo di identità IAM. Un ruolo IAM è molto simile a quello di un utente, in quanto è un'identità con politiche di autorizzazione che determinano ciò che l'identità può e non può fare AWS. Tuttavia, a un ruolo non sono associate credenziali e, invece di essere associato in modo univoco a una persona, un ruolo è pensato per essere assunto da chiunque ne abbia bisogno. Un utente IAM può assumere un ruolo per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.

I ruoli di accesso sono controllati dall'appartenenza al gruppo interno, che viene amministrata e rivista periodicamente da Operations Management.

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 EC2 istanze Amazon per un lungo periodo di tempo, puoi chiamarle. APIs Per ulteriori informazioni, consulta Amazon EC2 Reserved Instances.

> **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
	AWSSupportAccesso
	AMSChangeManagementReadOnlyPolicy
	AMSChangeManagementInfrastructurePolicy

Ruolo	Politica o politiche
	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).

Ruolo	Politica o politiche
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). Questa policy fornisce l'accesso a tutte le operazioni e le risorse di supporto. Per informazioni, consulta Getting Started with AWS Support.

Ruolo	Politica o politiche
	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 EC2 riservate di Amazon; per informazioni sui prezzi, consulta Amazon EC2 Reserved Instances.

JSON

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

AMSS3Politica

`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.

`AWSCertificateManagerFullAccess`informazioni, (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.

`AWSWAFFullAccess`informazioni, (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 o agli EC2 host del database.

Se ne hai uno attivo Account AWS, puoi utilizzare questo link ReadOnlyAccessper visualizzare l'intera ReadOnlyAccess politica. 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": [
        "*"
      ]
    }
  ]
}
```

Registrazione e monitoraggio degli eventi di sicurezza

AMS monitora continuamente l'ambiente gestito per rilevare eventuali minacce alla sicurezza. Gli eventi di sicurezza potrebbero essere rilevati da AMS o da te. AMS aggiorna regolarmente il proprio processo di automazione, basato sulla Computer Security Incident Handling Guide del National Institute of Standards and Technology (NIST), per rilevare meglio le minacce alla sicurezza.

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

Impostazione	Default
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 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/)

Impostazione	Default
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 Ogni giorno (24 ore) Day/All	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.
Scansione manuale	Scansiona tutto	Deve essere richiesto, quindi segue la configurazione di 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

Impostazione	Default	Note
Notifica di eventi locali	Sì	N/D

Processo di mitigazione del malware

AMS utilizza la Deep Security Platform (sistema antimalware) di Trend Micro per rilevare e rispondere al malware sulle istanze gestite da AMS. Per impostazione predefinita, l'agente di rilevamento Trend Micro viene eseguito su tutte le EC2 istanze Amazon, incluse quelle nei servizi condivisi e nelle sottoreti private, per i sistemi operativi Windows e Linux. Il sistema antimalware è collegato al monitoraggio AMS in modo che venga generato un evento ogni volta che viene rilevato un malware. Se c'è un impatto sui clienti, l'evento viene inoltrato al processo di gestione degli incidenti (per i dettagli, vedere). Risposta agli incidenti AMS Mentre AMS valuta l'impatto, l'utente riceve una notifica e si tenta di mitigare l'impatto.

Le definizioni antimalware di Trend Micro vengono aggiornate automaticamente quando Trend Micro pubblica gli aggiornamenti.

Durante l'onboarding delle applicazioni, si indica l'azione che si desidera che AMS intraprenda quando viene rilevato un malware su un'istanza:

- Assicurati che il file in quarantena sia nell'elenco dei file consentiti, rimuovilo dalla quarantena e rilascialo nuovamente nel file system.
- Elimina il file in quarantena, rimuovendolo dall'istanza.
- Sospendi l'istanza e sostituiscila. L'istanza sospesa è quindi disponibile per essere montata per la ricerca forense.

Dopo l'onboarding dell'applicazione:

- Quando il sistema antimalware rileva un malware su un'istanza, AMS lo mette automaticamente in quarantena. Ciò innesca un evento e un'indagine di follow-up.
- AMS notifica l'evento tramite una notifica di servizio e inizia a seguire l'azione di mitigazione predefinita selezionata.
- Se non hai scelto un'azione predefinita, AMS ti chiede quale azione intraprendere. Dopo aver ricevuto le istruzioni, AMS esegue l'azione selezionata e ti avvisa. AMS ti avvisa nuovamente una volta completata l'azione, inclusi i dettagli necessari per l'analisi forense, se applicabile.

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.

Scansioni antimalware complete del sistema

Il Payment Card Industry Data Security Standard (PCI DSS) richiede scansioni antimalware complete del sistema, abilitate per impostazione predefinita sul VPC gestito da AMS. Le scansioni complete del sistema sono impostate per essere eseguite alle 2 del mattino (nel fuso orario impostato sul server) perché utilizzano molta CPU. Le scansioni complete del sistema si aggiungono alle normali scansioni antimalware che non utilizzano molta CPU.

È disponibile un nuovo tipo di modifica della gestione (CT), Disable Malware Sans, che consente di disabilitare le scansioni antimalware complete del sistema. Puoi trovare il CT in Gestione | Sicurezza dell'host | Scansione completa del sistema | Disabilita la classificazione, modifica l'ID ct-1pybwg08h8qsz. Per riattivare le scansioni, usa Gestione | Altro | Altro | Aggiorna CT. La disabilitazione delle scansioni complete del sistema non disattiva le normali scansioni antimalware.

Sicurezza di Amazon Inspector

Il servizio Amazon Inspector monitora la sicurezza degli stack gestiti da AMS. Amazon Inspector è un servizio di valutazione della sicurezza automatizzato che aiuta a identificare le lacune nella sicurezza e nella conformità dell'infrastruttura distribuita. AWS Le valutazioni di sicurezza di Amazon Inspector ti consentono di valutare automaticamente gli stack in base all'esposizione, alle vulnerabilità e alle deviazioni dalle best practice verificando l'accessibilità e le vulnerabilità di rete non intenzionali nelle tue istanze Amazon. EC2 Dopo aver eseguito una valutazione, Amazon Inspector produce un elenco dettagliato di risultati di sicurezza con priorità in base al livello di gravità. Le valutazioni di Amazon Inspector sono offerte come pacchetti di regole predefiniti mappati su best practice e definizioni di

sicurezza comuni. Queste regole vengono aggiornate regolarmente dai ricercatori di sicurezza. AWS Per ulteriori informazioni su Amazon Inspector, consulta Amazon Inspector.

AMS Amazon Inspector FAQs

- Amazon Inspector è installato per impostazione predefinita sui miei account AMS?

  No. Amazon Inspector non fa parte della build o dell'inserimento di carichi di lavoro predefiniti dell'AMI.

- Come posso accedere e installare Amazon Inspector?

  Invia una richiesta RFC (Management | Other | Other | Create) per richiedere l'accesso all'account e l'installazione a Inspector e il team operativo AMS modificherà il ReadOnly Customer_ _Role per fornire l'accesso alla console Amazon Inspector (senza accesso SSM).

- L'agente Amazon Inspector deve essere installato su tutte le EC2 istanze Amazon che voglio valutare?

  No, le valutazioni di Amazon Inspector con il pacchetto di regole di raggiungibilità della rete possono essere eseguite senza un agente per nessuna istanza Amazon. EC2 L'agente è necessario per i pacchetti di regole di valutazione dell'host. Per ulteriori informazioni sull'installazione degli agenti, consulta Installazione degli agenti Amazon Inspector.

- È previsto un costo aggiuntivo per questo servizio?

  Sì. I prezzi di Amazon Inspector sono disponibili sul sito dei prezzi di Amazon Inspector.

- Quali sono i risultati di Amazon Inspector?

  I risultati sono potenziali problemi di sicurezza scoperti durante la valutazione di Amazon Inspector dell'obiettivo di valutazione selezionato. I risultati vengono visualizzati nella console Amazon Inspector o nell'API e contengono sia una descrizione dettagliata dei problemi di sicurezza sia consigli per risolverli.

- Sono disponibili i report della valutazione di Amazon Inspector?

  Sì. Un report di valutazione è un documento contenente i dettagli degli elementi sottoposti a test durante l'esecuzione di valutazioni e i risultati della valutazione. I risultati della valutazione vengono formattati come report standard. Tali report possono essere generati per condividere i risultati all'interno del team con lo scopo di individuare le azioni correttive, corredare i dati relativi all'audit della conformità o archiviare dati per riferimenti futuri. Un report di valutazione di Amazon Inspector può essere generato per un'esecuzione di valutazione una volta completato con successo.

- Posso usare i tag per identificare gli stack su cui voglio eseguire i report di Amazon Inspector?

  Sì.

- I team AMS Operations avranno accesso ai risultati della valutazione di Amazon Inspector?

  Sì. Chiunque abbia accesso alla console Amazon Inspector in AWS è in grado di visualizzare risultati e report di valutazione.

- I team operativi di AMS consiglieranno o agiranno in base ai risultati dei report di Amazon Inspector?

  No. Se desideri apportare modifiche in base ai risultati del rapporto Amazon Inspector, devi richiedere le modifiche tramite un RFC (Management | Other | Other | Update).

- AMS riceverà una notifica quando eseguo un rapporto Amazon Inspector?

  Quando richiedi l'accesso ad Amazon Inspector, l'operatore AMS che esegue la RFC notifica la richiesta al tuo CSDM.

Per ulteriori informazioni, consulta Amazon Inspector FAQs.

Risposta agli incidenti AMS

AMS utilizza le migliori pratiche tradizionali di gestione dei servizi IT (ITSM) per ripristinare il servizio, quando necessario, il più rapidamente possibile.

Forniamo follow-the-sun assistenza 24 ore su 24, 7 giorni su 7, 365 giorni all'anno attraverso diversi centri operativi in tutto il mondo con operatori dedicati che monitorano attivamente i dashboard e le code degli incidenti.

I nostri tecnici operativi utilizzano strumenti interni di tracciamento degli incidenti per identificare, registrare, classificare, assegnare priorità, diagnosticare, risolvere e chiudere gli incidenti e fornirti aggiornamenti su tutte queste attività tramite la console AMS o tramite l'API. Supporto I nostri operatori, molti dei quali hanno lavorato in AWS Premium Support ricoprendo diversi profili e ruoli tecnologici, sfruttano una varietà di Supporto strumenti interni per aiutarli in tutte queste attività. Questi operatori hanno una profonda familiarità con le infrastrutture supportate da AMS e dispongono di competenze tecniche di livello esperto per risolvere tutti i problemi di supporto identificati. Nei rari casi in cui i nostri operatori necessitino di assistenza, i team di Premium Support and AWS Service sono disponibili per fornire assistenza secondo necessità.

Nei casi in cui incidenti ad alta priorità abbiano un impatto sui carichi di lavoro critici, AMS consiglierà il ripristino dell'infrastruttura. Spesso c'è un compromesso tra la risoluzione di un problema o il ripristino da un backup funzionante e i rischi e gli impatti dei tempi di inattività del servizio per i clienti sono i fattori decisivi. Se hai tempo da dedicare alla risoluzione dei problemi, AMS ti assisterà, ma se l'urgenza del ripristino è elevata, possiamo avviare immediatamente un ripristino.

> **Note**
>
> I dati effimeri che non fanno parte del modello di stack o del ripristino dei dati vengono persi. AMS compie ogni ragionevole sforzo per eseguire il ripristino dell'infrastruttura quando le offerte di AWS servizi non sono disponibili. Il ripristino dell'infrastruttura viene completato una volta che le offerte AWS di servizi sono disponibili.
> Se non autorizzi il ripristino dell'infrastruttura come consigliato da AMS, non avrai diritto a un credito di servizio per l'impegno di AMS relativo ai tempi di risoluzione degli incidenti.

Convalida della conformità

AMS implementa e gestisce una libreria di AWS Config regole e azioni correttive, per proteggere da configurazioni errate che potrebbero ridurre la sicurezza e l'integrità operativa degli account.

Ad esempio, quando viene creato un bucket Amazon S3, AWS Config può valutare il bucket Amazon S3 in base a una regola che richiede ai bucket Amazon S3 di negare l'accesso pubblico in lettura. Se la policy o la lista di controllo degli accessi ai bucket (ACL) di Amazon S3 consentono l'accesso pubblico in lettura, AWS Config contrassegna sia il bucket che la regola come non conformi. Questi Regole di AWS Config contrassegnano le risorse come conformi, non conformi o non applicabili, in base al risultato della loro valutazione. Per ulteriori informazioni sul AWS Config servizio, consulta la Guida per gli sviluppatori.AWS Config

Puoi utilizzare la AWS Config console, la AWS CLI o l' AWS Config API per visualizzare le regole distribuite nel tuo account e lo stato di conformità delle tue regole e risorse. Per ulteriori informazioni, consulta la AWS Config documentazione: Visualizzazione della conformità della configurazione.

> **Note**
>
> Ulteriori informazioni su questo argomento sono disponibili accedendo ai report di AWS Artifact. Per ulteriori informazioni, consulta l'argomento Download dei rapporti in AWS Artifact. Per accedere ad AWS Artifact, puoi contattare il tuo CSDM per ricevere istruzioni o andare

alla pagina Getting Started with AWS Artifact. Queste informazioni non sono incluse in questa guida per l'utente perché contengono contenuti di sicurezza sensibili.

Multi-Account Landing Zone che visualizza lo stato di conformità del tuo Regole di AWS Config

La landing zone multi-account AMS utilizza il servizio di AWS Config aggregazione per creare una visione centralizzata della conformità per tutti i tuoi account. Ciò significa che puoi vedere lo stato di conformità di Regole di AWS Config tutto il tuo ambiente di landing zone multi-account AMS nell' AWS Config aggregatore del tuo account di sicurezza.

Di seguito è riportato un esempio dell' AWS Config aggregatore che mostra lo stato di conformità centralizzato di tutti gli account. Regole di AWS Config

Per ulteriori informazioni, consulta la documentazione AWS per Config Aggregator.

- In che modo AMS utilizza le regole di AWS Config?

  AMS crea Regole di AWS Config per dare visibilità alla configurazione delle AWS risorse rispetto alle condizioni specificate nelle regole. Se una regola non è conforme, puoi richiedere una modifica e il team AMS Ops collaborerà con te per intraprendere azioni correttive.
- In tal caso, vedrai apparire le seguenti modifiche nei tuoi account AMS:
  - Regole di AWS Config in AWS Config > Regole
  - Nel tuo account sono presenti regole di Config personalizzate con le relative funzioni Lambda
  - Config Aggregator nell'account Security e Config Authorization in tutti gli account (solo Multi-Account Landing Zone)

Di seguito è riportato un esempio Regole di AWS Config e i relativi risultati della valutazione della conformità sono riportati di seguito:

Per ulteriori informazioni su AWS Config, consulta:

- AWS Config: cos'è Config?
- AWS Config Rules: valutazione delle risorse con regole

- AWS Config Rules: Controllo dinamico della conformità: AWS Config Rules — Controllo dinamico della conformità per le risorse cloud
- AWS Config Aggregator: aggregazione di dati multi-account e più regioni

Restrizioni della politica di controllo del servizio AMS multi-account landing zone

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.

Resilienza

L'infrastruttura AWS globale è costruita attorno a zone Regioni AWS di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni su AWS regioni e zone di disponibilità, consulta infrastruttura globale.AWS

Sicurezza dell'infrastruttura

> **Note**
>
> Ulteriori informazioni su questo argomento sono disponibili accedendo ai report di AWS Artifact. Per ulteriori informazioni, consulta l'argomento Download dei rapporti in AWS Artifact. Per accedere ad AWS Artifact, puoi contattare il tuo CSDM per ricevere istruzioni o andare alla pagina Getting Started with AWS Artifact. Queste informazioni non sono incluse in questa guida per l'utente perché contengono contenuti di sicurezza sensibili.

Controllo di sicurezza per sistemi end-of-support operativi

I sistemi operativi che non rientrano nel periodo di supporto generale previsto da "end-of-support" o EOS del produttore del sistema operativo e che non ricevono aggiornamenti di sicurezza presentano un rischio maggiore per la sicurezza.

AWS offre alcuni servizi per facilitare la gestione del sistema operativo. end-of-support Per informazioni su Windows end-of-support, vedere Programma di End-of-Support migrazione per Windows Server.

> **Note**
>
> Ulteriori informazioni su questo argomento sono disponibili accedendo ai report di AWS Artifact. Per ulteriori informazioni, consulta l'argomento Download dei rapporti in AWS Artifact. Per accedere ad AWS Artifact, puoi contattare il tuo CSDM per ricevere istruzioni o andare alla pagina Getting Started with AWS Artifact. Queste informazioni non sono incluse in questa guida per l'utente perché contengono contenuti di sicurezza sensibili.

Utilizzo dei gruppi di sicurezza

Un gruppo di sicurezza funge da firewall virtuale che controlla il traffico di una o più istanze. I gruppi di sicurezza AMS consentono di impostare le regole del traffico in entrata e in uscita a livello di istanza. Puoi creare un gruppo di sicurezza e specificare le risorse nel tuo account AMS, nelle istanze Amazon, nelle EC2 istanze DB di Amazon RDS, nei Load Balancers, nelle istanze di replica Deep Security Manager (DSM), negli obiettivi di montaggio EFS e nei ElastiCache cluster, da associare al gruppo di sicurezza. Una volta associato, il traffico da o verso tali istanze è vincolato dalle regole impostate nel gruppo di sicurezza.

Per comprendere meglio la sicurezza generale di AWS, consulta Best Practices for Security, Identity, & Compliance e Amazon EC2 Security Groups for Linux Instances.

AMS dispone ora di una serie di tipi di modifiche per la creazione e la gestione di gruppi di sicurezza:

- Distribuzione | Componenti dello stack avanzati | Gruppo di sicurezza | Crea (ct-1oxx2g2d7hc90)
- Gestione | Componenti avanzati dello stack | Gruppo di sicurezza | Elimina (ct-3cp96z7r065e4)
- Gestione | Componenti avanzati dello stack | Gruppo di sicurezza | Aggiornamento (ct-3memthlcmvc1b)

Per esempi, vedi Gruppi di sicurezza.

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, come EC2 creare o OpenSearch creare un dominio, 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 EC2 console AWS 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	

Tipo	Protocollo	Intervallo porte	Origine
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, come EC2 creare o OpenSearch creare un dominio, 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 EC2 console AWS 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

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 (review required)` 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 «review required» CTs, 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 EC2 console. 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`.

Libreria di controlli preventivi e investigativi AMS

AWS Managed Services (AMS) ti offre una serie di policy di controllo library/catalog dei servizi comprovate (SCPs) ConfigRules che possono essere sfruttate per migliorare il tuo livello di sicurezza e mitigare le lacune di conformità nei tuoi account AMS.

Argomenti

Regole curate SCPs e di Config

Regole curate SCPs e di Config per AMS Advanced.

- Politiche di controllo del servizio (SCPs): quelle fornite SCPs si aggiungono a quelle AMS predefinite.

  È possibile utilizzare questi controlli della libreria insieme a quelli predefiniti per soddisfare requisiti di sicurezza specifici.
- Regole di configurazione: come misura di base, AMS consiglia di applicare i Conformance Pack (vedi Conformance Pack nella AWS Config guida) oltre alle regole di configurazione AMS predefinite (vedi Artefatti AMS per le regole predefinite). I Conformance Pack coprono la maggior parte dei requisiti di conformità e AWS li aggiorna regolarmente.

  Le regole elencate qui possono essere utilizzate per colmare lacune specifiche dei casi d'uso che non sono coperte dai Conformance Pack

> **Note**
>
> Man mano che le regole e i pacchetti di conformità predefiniti di AMS vengono aggiornati nel tempo, potresti vedere dei duplicati di queste regole.
> In generale, AMS consiglia di eseguire una pulizia periodica delle regole di Config duplicate.
> Per AMS Advanced, Config Rules non deve utilizzare riparazioni automatiche (vedi Remediating Noncompliant AWS Resources by AWS Config Rules) per evitare modifiche. out-of-band

SCP-AMS-001: Limita la creazione di EBS

Impedisci la creazione di volumi EBS se la crittografia non è abilitata.

```
{
      "Condition": {
        "Bool": {
          "ec2:Encrypted": "false"
        }
      },
      "Action": "ec2:CreateVolume",
      "Resource": "*",
      "Effect": "Deny"
    }
```

SCP-AMS-002: Limita il lancio EC2

Impedisci l'avvio di un' EC2 istanza se il volume EBS non è crittografato. Ciò include la negazione di un EC2 avvio da dati non crittografati, AMIs poiché questo SCP si applica anche ai volumi root.

```
{
      "Condition": {
        "Bool": {
          "ec2:Encrypted": "false"
        }
      },
      "Action": "ec2:RunInstances",
      "Resource": "arn:aws:ec2:*:*:volume/*",
      "Effect": "Deny"
    }
```

SCP-ADV-001: Limita gli invii RFC

Impedisci ai ruoli AMS predefiniti di inviare dati automatici specifici RFCs come Create VPC o Delete VPC. Ciò è utile se desideri applicare autorizzazioni più granulari ai ruoli federati.

Ad esempio, potresti volere che l'impostazione predefinita `AWSManagedServicesChangeManagement Role` sia in grado di inviare la maggior parte delle informazioni disponibili RFCs tranne quelle che consentono la creazione e l'eliminazione di un VPC, la creazione di sottoreti aggiuntive, l'offboarding di un account dell'applicazione, l'aggiornamento o l'eliminazione dei provider di identità SAML:

SCP-AMS-003: Limita o crea RDS in AMS EC2

Impedisci la creazione di istanze Amazon EC2 e RDS prive di tag specifici, permettendo al `AMS Backup IAM` ruolo predefinito di AMS di farlo. Ciò è necessario per il disaster recovery o il DR.

```
{
    "Sid": "DenyRunInstanceWithNoOrganizationTag",
    "Effect": "Deny",
    "Action": [
        "ec2:RunInstances",
        "rds:CreateDBInstance"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*",
        "arn:aws:rds:*:*:db:*"
    ],
    "Condition": {
        "Null": {
            "aws:RequestTag/organization": "true"
        },
        "StringNotLike": {
            "aws:PrincipalArn": [
                "arn:aws:iam::<Account_Number>:role/ams-backup-iam-role"
            ]
        }
    }
}
```

SCP-AMS-004: Limita i caricamenti su S3

Impedisci il caricamento di oggetti S3 non crittografati.

```
{
            "Sid": "DenyUnencryptedS3Uploads",
            "Effect": "Deny",
            "Action": "s3:PutObject",
            "Resource": "*",
            "Condition": {
                "StringNotLike": {
                    "s3:x-amz-server-side-encryption": ["aws:kms", "AES256"]
                },
                "Null": {
```

```
                    "s3:x-amz-server-side-encryption": "false"
                }
            }
        }
    ]
}
```

SCP-AMS-005: Limita l'accesso all'API e alla console

Impedisci l'accesso alla console AWS e all'API per le richieste provenienti da indirizzi IP noti non validi come cliente determinato InfoSec.

SCP-AMS-006: Impedisci all'entità IAM di rimuovere l'account membro dall'organizzazione

Impedire a un' AWS Identity and Access Management entità di rimuovere gli account dei membri dall'organizzazione.

```
{
  "Effect": "Deny",
  "Action": ["organizations:LeaveOrganization"],
  "Resource": ["*"]
}
```

SCP-AMS-007: Impedisci la condivisione di risorse con account esterni alla tua organizzazione

Impedite la condivisione di risorse con account esterni all' AWS organizzazione

```
  {
    "Effect": "Deny",
    "Action": [
      "ram:*"
    ],
    "Resource": [
      "*"
    ],
    "Condition": {
      "Bool": {
        "ram:AllowsExternalPrincipals": "true"
      }
    }
  },
  {
```

```
    "Effect": "Deny",
    "Action": [
      "ram:CreateResourceShare",
      "ram:UpdateResourceShare"
    ],
    "Resource": "*",
    "Condition": {
      "Bool": {
        "ram:RequestedAllowsExternalPrincipals": "true"
      }
    }
  }
```

SCP-AMS-008: Impedisci la condivisione con organizzazioni o unità organizzative () OUs

Impedisci la condivisione di risorse con un' and/or unità organizzativa dell'account appartenente a un'organizzazione.

```
{
  "Effect": "Deny",
  "Action": [
    "ram:CreateResourceShare",
    "ram:AssociateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "ForAnyValue:StringLike": {
      "ram:Principal": [
        "arn:aws:organizations::*:account/o-${OrganizationId}/${AccountId}",
        "arn:aws:organizations::*:ou/o-${OrganizationId}/ou-${OrganizationalUnitId}"
      ]
    }
  }
}
```

SCP-AMS-009: Impedisci agli utenti di accettare inviti alla condivisione di risorse

Impedisci agli account dei membri di accettare inviti AWS RAM a partecipare alla condivisione di risorse. Questa API non supporta alcuna condizione e impedisce le condivisioni solo da account esterni.

```
{
```

```
  "Effect": "Deny",
  "Action": ["ram:AcceptResourceShareInvitation"],
  "Resource": ["*"]
}
```

SCP-AMS-010: Impedisci che la regione dell'account abiliti e disabiliti le azioni

Impedisci l'attivazione o la disabilitazione di nuove AWS regioni per i tuoi AWS account.

```
{
  "Effect": "Deny",
  "Action": [
    "account:EnableRegion",
    "account:DisableRegion"
  ],
  "Resource": "*"
}
```

SCP-AMS-011: Impedisci le azioni di modifica della fatturazione

Impedisci modifiche alla configurazione di fatturazione e pagamento.

```
{
  "Effect": "Deny",
  "Action": [
    "aws-portal:ModifyBilling",
    "aws-portal:ModifyAccount",
    "aws-portal:ModifyPaymentMethods"
  ],
  "Resource": "*"
}
```

SCP-AMS-012: Impedisci la cancellazione o la modifica di specifiche CloudTrails

Impedisci modifiche a AWS CloudTrail percorsi specifici.

```
{
  "Effect": "Deny",
  "Action": [
    "cloudtrail:DeleteEventDataStore",
    "cloudtrail:DeleteTrail",
    "cloudtrail:PutEventSelectors",
    "cloudtrail:PutInsightSelectors",
```

```
    "cloudtrail:UpdateEventDataStore",
    "cloudtrail:UpdateTrail",
    "cloudtrail:StopLogging"
  ],
  "Resource": [
    "arn:${Partition}:cloudtrail:${Region}:${Account}:trail/${TrailName}"
  ]
}
```

SCP-AMS-013: Impedisci di disabilitare la crittografia EBS predefinita

Impedisci la disabilitazione della crittografia Amazon EBS predefinita.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:DisableEbsEncryptionByDefault"
  ],
  "Resource": "*"
}
```

SCP-AMS-014: Impedisci la creazione di VPC e sottorete predefiniti

Impedisci la creazione di un Amazon VPC e di sottoreti predefiniti.

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateDefaultSubnet",
    "ec2:CreateDefaultVpc"
  ],
  "Resource": "*"
}
```

SCP-AMS-015: Impedisci la disabilitazione e la modifica GuardDuty

Impedisci che Amazon GuardDuty venga modificato o disabilitato.

```
{
  "Effect": "Deny",
  "Action": [
    "guardduty:AcceptInvitation",
    "guardduty:ArchiveFindings",
```

```
    "guardduty:CreateDetector",
    "guardduty:CreateFilter",
    "guardduty:CreateIPSet",
    "guardduty:CreateMembers",
    "guardduty:CreatePublishingDestination",
    "guardduty:CreateSampleFindings",
    "guardduty:CreateThreatIntelSet",
    "guardduty:DeclineInvitations",
    "guardduty:DeleteDetector",
    "guardduty:DeleteFilter",
    "guardduty:DeleteInvitations",
    "guardduty:DeleteIPSet",
    "guardduty:DeleteMembers",
    "guardduty:DeletePublishingDestination",
    "guardduty:DeleteThreatIntelSet",
    "guardduty:DisableOrganizationAdminAccount",
    "guardduty:DisassociateFromMasterAccount",
    "guardduty:DisassociateMembers",
    "guardduty:InviteMembers",
    "guardduty:StartMonitoringMembers",
    "guardduty:StopMonitoringMembers",
    "guardduty:TagResource",
    "guardduty:UnarchiveFindings",
    "guardduty:UntagResource",
    "guardduty:UpdateDetector",
    "guardduty:UpdateFilter",
    "guardduty:UpdateFindingsFeedback",
    "guardduty:UpdateIPSet",
    "guardduty:UpdateMalwareScanSettings",
    "guardduty:UpdateMemberDetectors",
    "guardduty:UpdateOrganizationConfiguration",
    "guardduty:UpdatePublishingDestination",
    "guardduty:UpdateThreatIntelSet"
  ],
  "Resource": "*"
}
```

SCP-AMS-016: Impedisci l'attività degli utenti root

Impedisci all'utente root di eseguire qualsiasi azione.

```
{
  "Action": "*",
  "Resource": "*",
```

```
  "Effect": "Deny",
  "Condition": {
    "StringLike": {
      "aws:PrincipalArn": [
        "arn:aws:iam::*:root"
      ]
    }
  }
}
```

SCP-AMS-017: Impedisci di creare chiavi di accesso per l'utente root

Impedisci la creazione di chiavi di accesso per l'utente root.

```
{
  "Effect": "Deny",
  "Action": "iam:CreateAccessKey",
  "Resource": "arn:aws:iam::*:root"
}
```

SCP-AMS-018: Impedisci di disabilitare il blocco di accesso pubblico all'account S3

Impedisci la disabilitazione del blocco di accesso pubblico a un account Amazon S3. In questo modo si evita che qualsiasi bucket dell'account diventi pubblico.

```
{
  "Effect": "Deny",
  "Action": "s3:PutAccountPublicAccessBlock",
  "Resource": "*"
}
```

SCP-AMS-019: Impedisci di disabilitare AWS Config o modificare le regole di Config

Impedisci la disabilitazione o la modifica delle regole. AWS Config

```
{
  "Effect": "Deny",
  "Action": [
    "config:DeleteConfigRule",
    "config:DeleteConfigurationRecorder",
    "config:DeleteDeliveryChannel",
    "config:DeleteEvaluationResults",
```

```
    "config:StopConfigurationRecorder"
  ],
  "Resource": "*"
}
```

SCP-AMS-020: Impedisci tutte le azioni IAM

Impedisci tutte le azioni IAM.

```
{
  "Effect": "Deny",
  "Action": [
    "iam:*"
  ],
  "Resource": "*"
}
```

SCP-AMS-021: Impedisci l'eliminazione di log, gruppi e flussi CloudWatch

Impedisci l'eliminazione di gruppi e stream Amazon CloudWatch Logs.

```
{
  "Effect": "Deny",
  "Action": [
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream"
  ],
  "Resource": "*"
}
```

SCP-AMS-022: Impedisci la cancellazione di Glacier

Impedisci l'eliminazione di Amazon Glacier.

```
{
  "Effect": "Deny",
  "Action": [
    "glacier:DeleteArchive",
    "glacier:DeleteVault"
  ],
  "Resource": "*"
}
```

SCP-AMS-023: Impedisci l'eliminazione di IAM Access Analyzer

Impedisci l'eliminazione di IAM Access Analyzer.

```
{
  "Action": [
    "access-analyzer:DeleteAnalyzer"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-024: Impedisci modifiche al Security Hub

Impedire l'eliminazione di. AWS Security Hub CSPM

```
{
  "Action": [
    "securityhub:DeleteInvitations",
    "securityhub:DisableSecurityHub",
    "securityhub:DisassociateFromMasterAccount",
    "securityhub:DeleteMembers",
    "securityhub:DisassociateMembers"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-025: Impedisci la cancellazione sotto Directory Service

Impedisci l'eliminazione delle risorse sotto Directory Service.

```
{
  "Action": [
    "ds:DeleteDirectory",
    "ds:DeleteLogSubscription",
    "ds:DeleteSnapshot",
    "ds:DeleteTrust",
    "ds:DeregisterCertificate",
    "ds:DeregisterEventTopic",
    "ds:DisableLDAPS",
    "ds:DisableRadius",
```

```
    "ds:DisableSso",
    "ds:UnshareDirectory"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-026: Impedisci l'uso del servizio negato

Impedire l'uso dei servizi negati.

> **Note**
>
> Sostituisci *service1* e *service2* con i nomi dei tuoi servizi. Esempio *access-analyzer* o*IAM*.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:*", "service2:*"]
}
```

SCP-AMS-027: Impedisci l'uso di servizi negati in regioni specifiche

Impedire l'uso di servizi negati in aree geografiche specifiche. AWS

> **Note**
>
> Sostituisci *service1* e *service2* con i nomi dei tuoi servizi. Esempio *access-analyzer* o*IAM*.
> Sostituisci *region1* e *region2* con i nomi dei tuoi servizi. Esempio *us-west-2* o*use-east-1*.

```
{
  "Effect": "Deny",
  "Resource": "*",
  "Action": ["service1:*", "service2:*"],
  "Condition": {
```

```
    "StringEquals": {
      "aws:RequestedRegion": [
        "region1",
        "region2"
      ]
    }
  }
}
```

SCP-AMS-028: Impedisci che i tag vengano modificati se non da mandanti autorizzati

Impedisci la modifica dei tag da parte di qualsiasi utente ad eccezione dei principali autorizzati. Usa i tag di autorizzazione per autorizzare i principali. I tag di autorizzazione devono essere associati alle risorse e ai presidi. A user/role è considerato autorizzato solo se il tag sulla risorsa e sul principale corrispondono. Per ulteriori informazioni, consulta le seguenti risorse:

- Protezione dei tag delle risorse utilizzati per l'autorizzazione utilizzando una politica di controllo del servizio in AWS Organizations
- Impedisci che i tag vengano modificati se non da responsabili autorizzati

```
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "ec2:ResourceTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
    },
    "Null": {
      "ec2:ResourceTag/access-project": false
    }
  }
},
{
  "Effect": "Deny",
```

```
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:RequestTag/access-project": "${aws:PrincipalTag/access-project}",
      "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
    },
    "ForAnyValue:StringEquals": {
      "aws:TagKeys": [
        "access-project"
      ]
    }
  }
},
{
  "Effect": "Deny",
  "Action": [
    "ec2:CreateTags",
    "ec2:DeleteTags"
  ],
  "Resource": [
    "*"
  ],
  "Condition": {
    "StringNotEquals": {
      "aws:PrincipalArn": "arn:aws:iam::{ACCOUNT_ID}:{RESOURCE_TYPE}/{RESOURCE_NAME}"
    },
    "Null": {
      "aws:PrincipalTag/access-project": true
    }
  }
}
```

SCP-AMS-029: Impedisci agli utenti di eliminare i log di flusso di Amazon VPC

Impedisci l'eliminazione di Amazon VPC Flow Logs.

```
{
  "Action": [
```

```
    "ec2:DeleteFlowLogs",
    "logs:DeleteLogGroup",
    "logs:DeleteLogStream",
    "s3:DeleteBucket",
    "s3:DeleteObject",
    "s3:DeleteObjectVersion",
    "s3:PutLifecycleConfiguration",
    "firehose:DeleteDeliveryStream"
  ],
  "Resource": "*",
  "Effect": "Deny"
}
```

SCP-AMS-030: Impedisci la condivisione della sottorete VPC con account diversi dall'account di rete

Impedisci la condivisione di sottoreti Amazon VPC con account diversi dall'account di rete.

> **Note**
>
> Sostituiscilo *NETWORK_ACCOUNT_ID* con l'ID del tuo account di rete.

```
{
  "Effect": "Deny",
  "Action": [
    "ram:AssociateResourceShare",
    "ram:CreateResourceShare"
  ],
  "Resource": "*",
  "Condition": {
    "StringNotEquals": {
      "ram:Principal": "NETWORK_ACCOUNT_ID"
    },
    "StringEquals": {
      "ram:RequestedResourceType": "ec2:Subnet"
    }
  }
}
```

SCP-AMS-031: Impedisci il lancio di istanze con tipi di istanze proibiti

Impedisci il lancio di tipi di EC2 istanze Amazon proibiti.

> **Note**
>
> Sostituisci *instance_type1* e *instance_type2* con i tipi di istanza che desideri limitare, ad esempio *t2.micro* o una stringa jolly come. **.nano*

```
{
  "Effect": "Deny",
  "Action": "ec2:RunInstances",
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Condition": {
    "ForAnyValue:StringLike": {
      "ec2:InstanceType": [
        "instance_type1",
        "instance_type2"
      ]
    }
  }
}
```

SCP-AMS-032: Impedisci il lancio di istanze senza IMDSv2

Previeni EC2 le istanze Amazon senza IMDSv2.

```
[
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
      "StringNotEquals": {
        "ec2:MetadataHttpTokens": "required"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:RunInstances",
    "Resource": "arn:aws:ec2:*:*:instance/*",
    "Condition": {
```

```
      "NumericGreaterThan": {
        "ec2:MetadataHttpPutResponseHopLimit": "3"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "*",
    "Resource": "*",
    "Condition": {
      "NumericLessThan": {
        "ec2:RoleDelivery": "2.0"
      }
    }
  },
  {
    "Effect": "Deny",
    "Action": "ec2:ModifyInstanceMetadataOptions",
    "Resource": "*"
  }
]
```

SCP-AMS-033: Impedisci modifiche a un ruolo IAM specifico

Impedisci le modifiche a ruoli IAM specifici.

```
{
  "Action": [
    "iam:AttachRolePolicy",
    "iam:DeleteRole",
    "iam:DeleteRolePermissionsBoundary",
    "iam:DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:PutRolePermissionsBoundary",
    "iam:PutRolePolicy",
    "iam:TagRole",
    "iam:UntagRole",
    "iam:UpdateAssumeRolePolicy",
    "iam:UpdateRole",
    "iam:UpdateRoleDescription"
  ],
  "Resource": [
     "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
```

```
  "Effect": "Deny"
}
```

SCP-AMS-034: Impedisci la modifica di ruoli IAM specifici AssumeRolePolicy

Impedisci le modifiche ai ruoli IAM AssumeRolePolicy per specifici.

```
{
  "Action": [
    "iam:UpdateAssumeRolePolicy"
  ],
  "Resource": [
     "arn:aws:iam::{ACCOUNT_ID}:role/{RESOURCE_NAME}"
  ],
  "Effect": "Deny"
}
```

ConfigRule: tag obbligatori

Verifica se EC2 le istanze hanno i tag personalizzati che hai richiesto. Inoltre InfoSec, questo è utile anche per la gestione dei costi

```
ConfigRuleName: required-tags
      Description: >-
        A Config rule that checks whether EC2 instances have the required tags.
      Scope:
        ComplianceResourceTypes:
          - 'AWS::EC2::Instance'
      InputParameters:
        tag1Key: COST_CENTER
        tag2Key: APP_ID
      Source:
        Owner: AWS
        SourceIdentifier: REQUIRED_TAGS
```

ConfigRule: Chiave di accesso ruotata

Verifica che le chiavi di accesso vengano ruotate entro il periodo di tempo specificato. In genere, tale periodo è impostato su 90 giorni in base ai requisiti di conformità tipici.

```
ConfigRuleName: access-keys-rotated
```

```
      Description: >-
        A config rule that checks whether the active access keys are rotated
        within the number of days specified in maxAccessKeyAge. The rule is
        NON_COMPLIANT if the access keys have not been rotated for more than
        maxAccessKeyAge number of days.
      InputParameters:
        maxAccessKeyAge: '90'
      Source:
        Owner: AWS
        SourceIdentifier: ACCESS_KEYS_ROTATED
      MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: chiave di accesso root IAM in AMS

Verifica che non sia presente una chiave di accesso root su un account. Per gli account AMS Advanced, si prevede che ciò sia conforme out-of-the-box.

```
ConfigRuleName: iam-root-access-key-check
      Description: >-
        A config rule that checks whether the root user access key is available. The
 rule is COMPLIANT if the user access key does not exist.
      Source:
        Owner: AWS
        SourceIdentifier: IAM_ROOT_ACCESS_KEY_CHECK
      MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: SSM gestito EC2

Verifica che la tua gestione EC2s sia affidata a SSM Systems Manager.

```
ConfigRuleName: ec2-instance-managed-by-systems-manager
      Description: >-
        A Config rule that checks whether the EC2 instances in the
        account are managed by AWS Systems Manager.
      Scope:
        ComplianceResourceTypes:
          - 'AWS::EC2::Instance'
          - 'AWS::SSM::ManagedInstanceInventory'
      Source:
        Owner: AWS
        SourceIdentifier: EC2_INSTANCE_MANAGED_BY_SSM
```

ConfigRule: utente IAM non utilizzato in AMS

Verifica le credenziali utente IAM che non sono state utilizzate per una durata specificata. Analogamente al controllo della rotazione delle chiavi, il valore predefinito è di 90 giorni in base ai requisiti di conformità tipici.

```
ConfigRuleName: iam-user-unused-credentials-check
      Description: >-
        A config rule that checks whether IAM users have passwords
        or active access keys that have not been used within the
        specified number of days provided.
      InputParameters:
        maxCredentialUsageAge: '90'
      Source:
        Owner: AWS
SourceIdentifier: IAM_USER_UNUSED_CREDENTIALS_CHECK
      MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: registrazione del bucket S3

Verifica che la registrazione sia stata abilitata per i bucket S3 nell'account.

```
ConfigRuleName: s3-bucket-logging-enabled
      Description: >-
        A Config rule that checks whether logging is enabled for S3 buckets.
      Scope:
        ComplianceResourceTypes:
          - 'AWS::S3::Bucket'
      Source:
        Owner: AWS
SourceIdentifier: S3_BUCKET_LOGGING_ENABLED
```

ConfigRule: controllo delle versioni del bucket S3

Verifica che il controllo delle versioni e l'eliminazione dell'MFA (opzionale) siano abilitati su tutti i bucket S3

```
ConfigRuleName: s3-bucket-versioning-enabled
      Description: >-
        A Config rule that checks whether versioning is enabled for S3
        buckets. Optionally, the rule checks if MFA delete is enabled for S3 buckets.
      Scope:
```

```
        ComplianceResourceTypes:
          - 'AWS::S3::Bucket'
      Source:
        Owner: AWS
SourceIdentifier: S3_BUCKET_VERSIONING_ENABLED
```

ConfigRule: accesso pubblico a S3

Verifica che le impostazioni di accesso pubblico (Public ACL, Public Policy, Public Buckets) siano limitate in tutto l'account

```
ConfigRuleName: s3-account-level-public-access-blocks
      Description: >-
        A Config rule that checks whether the required public access block
        settings are configured from account level. The rule is only
        NON_COMPLIANT when the fields set below do not match the corresponding
        fields in the configuration item.
      Scope:
        ComplianceResourceTypes:
          - 'AWS::S3::AccountPublicAccessBlock'
      InputParameters:
        IgnorePublicAcls: 'True'
        BlockPublicPolicy: 'True'
        BlockPublicAcls: 'True'
        RestrictPublicBuckets: 'True'
      Source:
        Owner: AWS
SourceIdentifier: S3_ACCOUNT_LEVEL_PUBLIC_ACCESS_BLOCKS
```

ConfigRule: risultati non archiviati GuardDuty

Verifica la presenza di eventuali GuardDuty risultati non archiviati più vecchi della durata specificata. La durata predefinita è di 30 giorni per i risultati a bassa risoluzione, 7 giorni per i risultati a media e 1 giorno per i risultati ad alto livello.

```
ConfigRuleName: guardduty-non-archived-findings
      Description: >-
        A Config rule that checks whether the Amazon GuardDuty has findings that
        are non archived. The rule is NON_COMPLIANT if GuardDuty has non
        archived low/medium/high severity findings older than the specified number.
      InputParameters:
        daysLowSev: '30'
        daysMediumSev: '7'
```

```
        daysHighSev: '1'
      Source:
        Owner: AWS
        SourceIdentifier: GUARDDUTY_NON_ARCHIVED_FINDINGS
      MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: eliminazione CMK

Verifica la presenza di eventuali chiavi master AWS Key Management Service personalizzate (CMKs) di cui è prevista l'eliminazione (ovvero in sospeso). Questo è fondamentale in quanto l'inconsapevolezza sull'eliminazione da CMK può portare all'irrecuperabilità dei dati

```
ConfigRuleName: kms-cmk-not-scheduled-for-deletion
      Description: >-
        A config rule that checks whether customer master keys (CMKs) are not
        scheduled for deletion in AWS Key Management Service (AWS KMS). The rule is
        NON_COMPLIANT if CMKs are scheduled for deletion.
      Source:
        Owner: AWS
SourceIdentifier: KMS_CMK_NOT_SCHEDULED_FOR_DELETION
      MaximumExecutionFrequency: TwentyFour_Hours
```

ConfigRule: Rotazione CMK

Verifica che la rotazione automatica sia abilitata per ogni CMK dell'account

```
ConfigRuleName: cmk-backing-key-rotation-enabled
      Description: >-
        A config rule that checks that key rotation is enabled for each customer
        master key (CMK). The rule is COMPLIANT, if the key rotation is enabled
        for specific key object. The rule is not applicable to CMKs that have
        imported key material.
      Source:
        Owner: AWS
SourceIdentifier: CMK_BACKING_KEY_ROTATION_ENABLED
      MaximumExecutionFrequency: TwentyFour_Hours
```

Notifica personalizzata per le regole di Config

Possono verificarsi casi di regole di Config critiche non conformi che richiedono una maggiore consapevolezza direttamente con il tuo team dirigenziale. InfoSec Per tali scenari, AMS consiglia di configurare una notifica personalizzata basata sugli eventi di non conformità.

Ad esempio:

```
ConfigRuleName: required-tags
      Description: >-
        A Config rule that checks whether EC2 instances have the mandated tags.
      Scope:
        ComplianceResourceTypes:
          - 'AWS::EC2::Instance'
      InputParameters:
        tag1Key: COST_CENTER
        tag2Key: APP_ID
      Source:
        Owner: AWS
SourceIdentifier: REQUIRED_TAGS
  NotificationEventRule:
    Type: 'AWS::Events::Rule'
    Properties:
      Name: CWEventForrequired-tags
      Description: >-
        SNS Notification for Non-Compliant Events of Config Rule:
        required-tags
      State: ENABLED
      EventPattern:
        detail-type:
          - Config Rules Compliance Change
        source:
          - aws.config
        detail:
          newEvaluationResult:
            complianceType:
              - NON_COMPLIANT
          configRuleARN:
            - 'Fn::GetAtt':
                - RequiredEC2Tags
                - Arn
      Targets:
        - Id: RemediationNotification
          Arn:
            Ref: SnsTopic
          InputTransformer:
            InputTemplate: >-
              "EC2 Instance <Instance_ID> is non-compliant. Please add required tags:
 COST_CENTER, APP_ID, Name, and Backup."
            InputPathsMap:
```

```
            instance_id: $.detail.resourceId
  SnsTopic:
    Type: 'AWS::SNS::Topic'
    Properties:
      Subscription:
        - Endpoint: Cloud_Ops_Leaders@customer.com
          Protocol: email
      TopicName: noncompliant-instance-notification
  SnsTopicPolicy:
    Type: 'AWS::SNS::TopicPolicy'
    Properties:
      PolicyDocument:
        Statement:
          - Sid: __default_statement_ID
            Effect: Allow
            Principal:
              AWS: '*'
            Action:
              - 'SNS:GetTopicAttributes'
              - 'SNS:SetTopicAttributes'
              - 'SNS:AddPermission'
              - 'SNS:RemovePermission'
              - 'SNS:DeleteTopic'
              - 'SNS:Subscribe'
              - 'SNS:ListSubscriptionsByTopic'
              - 'SNS:Publish'
              - 'SNS:Receive'
            Resource:
              Ref: SnsTopic
            Condition:
              StringEquals:
                'AWS:SourceOwner':
                  Ref: 'AWS::AccountId'
          - Sid: TrustCWEToPublishEventsToMyTopic
            Effect: Allow
            Principal:
              Service: events.amazonaws.com
            Action: 'sns:Publish'
            Resource:
              Ref: SnsTopic
      Topics:
        - Ref: SnsTopic
```

Amazon EventBridge regola il ruolo collegato ai servizi per AMS Advanced

AMS Advanced utilizza il ruolo collegato ai servizi (SLR) denominato AWSServiceRoleForManagedServices_Events: questo ruolo si affida a uno dei responsabili del servizio AWS Managed Services (events.managedservices.amazonaws.com) affinché assuma il ruolo al posto tuo. Il servizio utilizza il ruolo per creare regole gestite. EventBridge Questa regola è l'infrastruttura richiesta nel tuo AWS account per fornire informazioni sulla modifica dello stato di allarme dal tuo account a AWS Managed Services.

Autorizzazioni per EventBridge SLR for AMS Advanced

Ai fini dell'assunzione del ruolo, il ruolo collegato ai servizi AWSServiceRoleForManagedServices_Events considera attendibili i seguenti servizi:

- events.managedservices.amazonaws.com

A questo ruolo è associata la policy AWSManagedServices_EventsServiceRolePolicy AWS gestita (vedi AWS managed policy: AWSManagedServices_EventsServiceRolePolicy). Il servizio utilizza il ruolo per fornire informazioni sulla modifica dello stato di allarme dall'account a AWS Managed Services. Per consentire a un'entità IAM (come un utente, un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato ai servizi devi configurare le relative autorizzazioni. Per ulteriori informazioni, consulta Service-Linked Role Permissions nella AWS Identity and Access Management User Guide.

Puoi scaricare il codice JSON AWSManagedServices_EventsServiceRolePolicyin questo ZIP: .zip. EventsServiceRolePolicy

Creazione di una EventBridge reflex per AMS Advanced

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando effettui l'onboarding su AMS nella console di AWS gestione AWS CLI, o nell' AWS API, AMS Advanced crea automaticamente il ruolo collegato al servizio.

> **Important**
>
> Questo ruolo collegato al servizio può apparire nel tuo account se utilizzavi il servizio AMS Advanced prima del 7 febbraio 2023, quando ha iniziato a supportare i ruoli collegati ai servizi, quindi AMS Accelerate ha creato il ruolo nel tuo account.

AWSServiceRoleForManagedServices_Events Per ulteriori informazioni, consulta Un nuovo ruolo è apparso nel mio account IAM.

Se elimini questo ruolo collegato ai servizi, è possibile ricrearlo seguendo lo stesso processo utilizzato per ricreare il ruolo nell'account. Quando effettui l'accesso ad AMS, AMS Advanced crea nuovamente il ruolo collegato ai servizi per te.

Modifica di una EventBridge reflex per AMS Advanced

AMS Advanced non consente di modificare il ruolo collegato al AWSServiceRoleForManagedServices_Events servizio. Dopo aver creato un ruolo collegato al servizio, non potrai modificarne il nome perché varie entità potrebbero farvi riferimento. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di una EventBridge reflex per AMS Advanced

Non è necessario eliminare manualmente il ruolo AWSServiceRoleForManagedServices_Events . Quando esci da AMS tramite la console di AWS gestione AWS CLI o l' AWS API, AMS Advanced ripulisce le risorse ed elimina automaticamente il ruolo collegato ai servizi.

Puoi anche utilizzare la console IAM, AWS CLI o l' AWS API per eliminare manualmente il ruolo collegato al servizio. Per farlo, sarà necessario prima eseguire manualmente la pulizia delle risorse associate al ruolo collegato ai servizi e poi eliminarlo manualmente.

> **Note**
>
> Se il servizio AMS Advanced utilizza il ruolo quando si tenta di eliminare le risorse, l'eliminazione potrebbe non riuscire. In questo caso, attendi alcuni minuti e quindi ripeti l'operazione.

Per eliminare le risorse AMS Advanced utilizzate dal ruolo AWSServiceRoleForManagedServices_Events collegato al servizio

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, l'o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForManagedServices_Events servizio.

Per ulteriori informazioni, consultare Eliminazione del ruolo collegato ai servizi nella Guida per l'utente di IAM.

Best practice relative alla sicurezza

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.

Impostazioni non predefinite EPS della landing zone multi-account 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.

Guardrail AMS

Un guardrail è una regola di alto livello che fornisce una governance continua per l'intero ambiente 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.

Politiche di controllo del servizio MALZ

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.

Risposta agli incidenti di sicurezza in AMS

La sicurezza è la massima priorità di AWS Managed Services (AMS). AMS distribuisce risorse e controlli nei tuoi account per gestirli. AWS ha un modello di responsabilità AWS condivisa: gestisce

la sicurezza del cloud e tu sei responsabile della sicurezza nel cloud. AMS protegge i tuoi dati e le tue risorse e aiuta a mantenere la tua AWS infrastruttura sicura utilizzando controlli di sicurezza e il monitoraggio attivo dei problemi di sicurezza. Queste funzionalità ti aiutano a stabilire una base di sicurezza per le applicazioni in esecuzione nel AWS cloud. AMS collabora con voi tramite Security Incident Response per valutare l'effetto e quindi effettuare misure di contenimento e correzione sulla base delle raccomandazioni delle migliori pratiche.

Quando si verifica una deviazione dalla linea di base, ad esempio a causa di un'errata configurazione o di un cambiamento di fattori esterni, è necessario rispondere e indagare. Per farlo con successo, è necessario comprendere i concetti di base di Security Incident Response all'interno del proprio ambiente AMS. È inoltre necessario comprendere i requisiti per preparare, istruire e formare i team cloud prima che si verifichino problemi di sicurezza. È importante conoscere i controlli e le funzionalità che è possibile utilizzare, preparare piani di risposta per problemi di sicurezza comuni, come la compromissione di un account utente o l'uso improprio di account privilegiati, e identificare metodi di riparazione che utilizzano l'automazione per migliorare la velocità e la coerenza di risposta. Inoltre, è necessario comprendere i requisiti normativi e di conformità relativi alla creazione di un programma di Security Incident Response per soddisfare tali requisiti.

Security Incident Response può essere complesso, ma implementando un approccio iterativo è possibile semplificare il processo e consentire al team di risposta agli incidenti di soddisfare le parti interessate delle risorse fornendo un rilevamento e una risposta tempestivi e continui. In questa guida, ti forniamo la metodologia utilizzata da AMS per la risposta agli incidenti, la matrice di responsabilità AMS (RACI), come prepararti per un evento di sicurezza, come coinvolgere AMS durante gli incidenti di sicurezza e alcuni dei runbook di risposta agli incidenti utilizzati da AMS.

Come funziona AMS Security Incident Response

AWS Managed Services si allinea alla Guida alla gestione degli incidenti di sicurezza informatica NIST 800-61 per la risposta agli incidenti di sicurezza. Allineandoci a questo standard di settore, forniamo un approccio coerente alla gestione degli eventi di sicurezza e aderiamo alle migliori pratiche per proteggere e rispondere agli incidenti di sicurezza nel tuo cloud.

Ciclo di vita della risposta agli incidenti

Quando il rilevamento identifica e genera un avviso di sicurezza o richiedi assistenza per la sicurezza, il team di AWS Managed Services Operations si assicura che venga condotta un'indagine tempestiva, esegue automazioni per eseguire la raccolta, il triage e l'analisi dei dati, ti informa dell'analisi, esegue indagini e qualsiasi attività di contenimento e quindi pubblica l'analisi degli eventi.

Le attività di raccolta, triage, analisi e contenimento dei dati eseguite durante la risposta all'incidente variano a seconda del tipo di evento di sicurezza oggetto di indagine. Alla fine di questo documento sono riportati esempi di flussi di lavoro di Security Incident Response per scenari selezionati.

Durante gli incidenti, AMS determina dinamicamente la linea d'azione corretta, il che potrebbe comportare il riordino o l'aggiramento appropriato delle fasi documentate per garantire che si verifichi il risultato giusto.

Preparazione

Con l'evolversi del panorama delle minacce, AMS continua a espandere le capacità di rilevamento e risposta. Man mano che vengono aggiunti nuovi rilevamenti, AMS incorpora gli avvisi di questi nuovi rilevamenti nella piattaforma di rilevamento e risposta. I soccorritori di sicurezza AMS sono formati per indagare e collaborare con voi durante tutto il ciclo di vita del Security Incident Response.

Grazie a questo approccio basato sulla partnership, è importante che i team addetti alla sicurezza e alle applicazioni siano preparati a collaborare con AMS per gestire gli eventi di sicurezza man mano che si verificano tali eventi. Questa documentazione spiega cosa aspettarsi durante un evento di sicurezza e aiuta a prepararsi per una risposta rapida quando si verifica un incidente di sicurezza.

Questa documentazione utilizza la definizione NIST 800-61 di evento come qualsiasi evento osservabile in un sistema o in una rete e un incidente come violazione o minaccia imminente di violazione delle politiche, delle politiche di utilizzo accettabile o delle pratiche di sicurezza standard.

Lista di controllo per la preparazione

Completa la seguente lista di controllo con il tuo AMS cloud solution delivery manager (CSDM) e l'architetto cloud AMS (CA):

- Scopri quali carichi di lavoro vengono eseguiti in quali account.
- Scopri quali team interni sono responsabili dei vari carichi di lavoro e etichettali in modo appropriato nei carichi di lavoro.
- Gestisci internamente i dati di contatto di altri team che potrebbero essere necessari durante un'indagine su un evento di sicurezza e per le decisioni di contenimento.
- Verifica che i contatti di sicurezza siano aggiornati e aggiunti a tutti gli account gestiti AWS . I contatti vengono gestiti per account.
- Scopri come segnalare un incidente di sicurezza ad AMS e conosci la gravità e i tempi di risposta previsti.

- Assicurati che, quando le notifiche di sicurezza vengono ricevute, vengano indirizzate alle persone e ai sistemi appropriati, come i cercapersone o il centro operativo di sicurezza.
- Scopri quali fonti di registro sono disponibili, dove sono archiviate nei tuoi account e chi può accedervi.
- Scopri come utilizzare CloudWatch Insights to Query Logs durante le indagini.
- Comprendi le opzioni di contenimento disponibili per risorsa (IAMEC2, S3 e così via) e le conseguenze sulla disponibilità del carico di lavoro durante il contenimento.

Rilevamento

Durante la gestione degli AWS account, AMS monitora eventuali anomalie nel comportamento degli utenti, nelle attività degli account e nei potenziali eventi di sicurezza utilizzando i dati raccolti da fonti e controlli di rilevamento, tra cui, a titolo esemplificativo ma non esaustivo, CloudWatch Amazon, GuardDuty VPC Flow Logs, Amazon Macie AWS Config e i feed interni di Amazon Threat Intelligence.

AMS utilizza sia AWS servizi nativi che altre tecnologie di rilevamento per rispondere agli eventi di sicurezza creati da:

- Tipi di ricerca della conformità di Config
- GuardDuty Tipi di ricerca
- Tipi di ricerca di Macie
- Eventi del firewall DNS di Amazon Route 53 Resolver
- Eventi di sicurezza AMS (allarmi cloud watch)

Ulteriori risultati vengono aggiunti man mano che i servizi, i prodotti e gli ecosistemi di minacce si evolvono.

Segnala gli eventi di sicurezza ad AMS

Segnala un incidente tramite l'AMS Support Portal o Supporto Center per notificare ad AMS un incidente di sicurezza o per richiedere indagini.

Analizzare

Dopo aver identificato e segnalato un evento di sicurezza, il passaggio successivo consiste nell'analizzare se l'evento segnalato è un falso positivo o un incidente reale. AMS utilizza

l'automazione e le tecniche investigative manuali per gestire gli eventi di sicurezza. L'analisi include l'analisi dei log provenienti da diverse fonti di rilevamento, come i registri del traffico di rete, i registri degli host, CloudTrail gli eventi, i registri dei AWS servizi e così via. L'analisi cerca anche modelli che mostrano un comportamento anomalo per correlazione.

La collaborazione è necessaria per comprendere il contesto specifico dell'ambiente dell'account e stabilire ciò che è normale per l'account e i carichi di lavoro. Ciò consente ad AMS di identificare un'anomalia più rapidamente e di accelerare la risposta agli incidenti.

Gestisci le comunicazioni di AMS relative agli eventi di sicurezza

AMS ti tiene informato durante le indagini contattando i tuoi contatti di sicurezza tramite una segnalazione in caso di incidente. Il vostro AMS cloud service delivery manager (CSDM) e l'architetto cloud AMS (CA) sono i punti di contatto a cui rivolgervi per qualsiasi comunicazione durante un'indagine di sicurezza attiva.

La comunicazione include la notifica automatica quando viene generato un avviso di sicurezza, l'analisi della comunicazione dopo l'evento, la creazione di call bridge e la consegna continua di elementi quali file di registro, istantanee delle risorse infette e la trasmissione dei risultati delle indagini all'utente durante l'evento di sicurezza.

I campi standard inclusi nelle notifiche di avviso di sicurezza AMS sono elencati di seguito. Questi campi forniscono informazioni che consentono di indirizzare gli eventi ai team appropriati all'interno dell'organizzazione per la correzione.

- Tipo di ricerca
- Identificatore del ritrovamento (se pertinente)
- Individuazione della gravità
- Descrizione del ritrovamento
- Individuazione della data e dell'ora di creazione
- AWS ID dell'account
- Regione (se pertinente)
- AWS Risorse (IAM user/role/policy EC2, S3, EKS)

Vengono forniti campi aggiuntivi a seconda del tipo di risultato, ad esempio EKS Findings include i dettagli di Pod, Container e Cluster.

Contenere

L'approccio di AMS al contenimento si basa sulla collaborazione con te. Conosci la tua attività e gli impatti sul carico di lavoro che potrebbero derivare dalle attività di contenimento, come l'isolamento della rete, il de-provisioning di utenti o ruoli IAM, la ricostruzione delle istanze e così via.

Una parte essenziale del contenimento è il processo decisionale. Ad esempio, spegnere un sistema, isolare una risorsa dalla rete o disattivare l'accesso o terminare le sessioni. Queste decisioni sono più facili da prendere se esistono strategie e procedure predeterminate per contenere l'incidente. AMS fornisce la strategia di contenimento e quindi implementa la soluzione dopo aver considerato il rischio associato all'implementazione delle azioni di contenimento.

Esistono diverse opzioni di contenimento a seconda delle risorse oggetto di analisi. AMS prevede che durante un'indagine su un incidente vengano implementati contemporaneamente più tipi di contenimento. Alcuni di questi esempi includono:

- Applica regole di protezione per bloccare il traffico non autorizzato (gruppo di sicurezza, NACL, regole WAF, regole SCP, Deny listing, impostazione dell'azione di firma in quarantena o blocco)
- Isolamento delle risorse
- Isolamento di rete
- Disabilitazione degli utenti, dei ruoli e delle politiche IAM
- Modifica/riduzione dei privilegi di utente e ruolo IAM
- Interruzione, sospensione, eliminazione delle risorse di calcolo
- Limitazione dell'accesso pubblico alla risorsa interessata
- Chiavi di accesso, chiavi API e password a rotazione
- Eliminazione delle credenziali divulgate e delle informazioni sensibili

AMS vi incoraggia a prendere in considerazione il tipo di strategie di contenimento per ogni tipo di incidente grave che rientra nella vostra propensione al rischio, con criteri chiaramente documentati per facilitare il processo decisionale in caso di incidente. I criteri per determinare la strategia appropriata includono:

- Potenziali danni alle risorse
- Conservazione delle prove
- Indisponibilità del servizio (ad esempio, connettività di rete, servizi forniti a parti esterne)
- Tempo e risorse necessari per implementare la strategia

- Efficacia della strategia (ad esempio, contenimento parziale, contenimento totale)
- Permanenza della soluzione (ad esempio, decisioni relative a porte unidirezionali o porte bidirezionali)
- Durata della soluzione (ad esempio, soluzione alternativa di emergenza da rimuovere in quattro ore, soluzione temporanea da rimuovere in due settimane, soluzione permanente).
- Applica controlli di sicurezza attivabili per ridurre il rischio e concedi il tempo necessario per definire e implementare un contenimento più efficace.

La velocità di contenimento è fondamentale, AMS consiglia un approccio graduale per ottenere un contenimento efficiente ed efficace attraverso strategie a breve e lungo termine.

Utilizzate questa guida per prendere in considerazione la vostra strategia di contenimento che prevede diverse tecniche in base al tipo di risorsa.

- Strategia di contenimento
  - AMS può identificare la portata dell'incidente di sicurezza?
    - In caso affermativo, identifica tutte le risorse (utenti, sistemi, risorse).
    - In caso negativo, esaminate parallelamente all'esecuzione del passaggio successivo sulle risorse identificate.
  - La risorsa può essere isolata?
    - In caso affermativo, procedi a isolare le risorse interessate.
    - In caso negativo, collabora con i proprietari e i gestori del sistema per determinare le ulteriori azioni necessarie per contenere il problema.
  - Tutte le risorse interessate sono isolate dalle risorse non interessate?
    - In caso affermativo, procedi con il passaggio successivo.
    - In caso negativo, continuate a isolare le risorse interessate fino a raggiungere un contenimento a breve termine per evitare che l'incidente si aggravi ulteriormente.
- Backup del sistema
  - Sono state create copie di backup dei sistemi interessati per ulteriori analisi?
  - Le copie forensi sono crittografate e archiviate in un luogo sicuro?
    - In caso affermativo, procedi con il passaggio successivo.
    - In caso negativo, crittografa le immagini forensi, quindi conservale in un luogo sicuro per evitare utilizzi accidentali, danni e manomissioni.

Sradicare

Dopo aver contenuto un incidente, potrebbe essere necessario eliminarlo per eliminare del tutto le fonti di minaccia e proteggere il sistema prima di procedere alla fase di ripristino successiva. Le misure di eradicazione potrebbero includere l'eliminazione del malware e la rimozione degli account utente compromessi, nonché l'identificazione e la mitigazione di tutte le vulnerabilità sfruttate. Durante l'eliminazione, è importante identificare tutti gli account, le risorse e le istanze interessati all'interno dell'ambiente in modo che possano essere corretti.

È buona norma che l'eradicazione e il ripristino avvengano secondo un approccio graduale, in modo da dare priorità alle fasi di riparazione. Per gli incidenti su larga scala, il ripristino potrebbe richiedere mesi. L'intento delle fasi iniziali deve essere quello di aumentare la sicurezza complessiva con modifiche di valore relativamente rapide (da giorni a settimane) per prevenire incidenti futuri. Le fasi successive devono concentrarsi sui cambiamenti a lungo termine (ad esempio, modifiche all'infrastruttura) e sul lavoro continuo per mantenere l'azienda il più sicura possibile.

Per alcuni incidenti, l'eradicazione non è necessaria o viene eseguita durante il recupero.

Considera i seguenti aspetti:

- È possibile modificare l'immagine del sistema e quindi rafforzarlo con patch o altre contromisure per prevenire o ridurre il rischio di attacchi?
- Tutti i malware e gli altri artefatti lasciati dagli aggressori sono stati rimossi e i sistemi interessati sono protetti da ulteriori attacchi?

Ripristino

AMS collabora con te per ripristinare il normale funzionamento dei sistemi, confermare che funzionino normalmente e (se applicabile) correggere le vulnerabilità per prevenire incidenti simili.

Considera i seguenti aspetti:

- I sistemi interessati sono aggiornati e rafforzati contro l'attacco recente e i possibili attacchi futuri?
- In che giorno e a che ora è possibile ripristinare la produzione dei sistemi interessati?
- Quali strumenti utilizzerete per testare, monitorare e verificare che i sistemi ripristinati in produzione non siano vulnerabili alle tecniche di attacco iniziali?

Segnalazione post incidente

Dopo l'evento, AMS esegue un processo di revisione delle indagini per tutti gli incidenti di sicurezza. Inoltre, AMS avvia un processo di correzione dell'errore (COE) per risolvere gli incidenti di sicurezza causati da un errore di sistema o procedurale che plausibilmente ha margini di miglioramento. AMS collabora con te per migliorare continuamente l'esperienza delle indagini sulla sicurezza. Il processo COE aiuta AMS a identificare i fattori che contribuiscono agli eventi che influiscono sui clienti e collega tali cause alle azioni successive, elementi che possono impedire il ripetersi di eventi simili o contribuire a mitigare la durata o il livello di impatto.

Il processo di revisione delle indagini sugli incidenti di sicurezza affronta i seguenti elementi per identificare le opportunità di miglioramento:

- Qual è stato il tempo trascorso dall'inizio dell'incidente alla scoperta dell'incidente, alla valutazione iniziale dell'impatto e a ciascuna fase del processo di gestione dell'incidente (ad esempio, contenimento, ripristino)?
- Quanto tempo ha impiegato il team di risposta all'incidente per rispondere alla segnalazione iniziale dell'incidente?
- Quanto tempo è stato necessario per eseguire un'analisi d'impatto iniziale?
- Era evitabile e in che modo? Esiste uno strumento o un processo che avrebbe potuto impedirlo?
- Avremmo potuto rilevarlo prima e in che modo?
- Cosa avrebbe potuto velocizzare le indagini?
- Sono state seguite le procedure documentate di risposta agli incidenti? Erano adeguate?
- La condivisione delle informazioni con altre parti interessate è stata effettuata in modo tempestivo? Come potrebbe essere migliorata?
- La collaborazione con altri team (addetti AWS alla sicurezza, agli account, al team di AWS sviluppo e al team di sicurezza dei clienti) è stata efficace? In caso contrario, cosa potrebbe essere migliorato?
- Quali fasi preparatorie mancavano che avrebbero potuto essere utili, le matrici di escalation, i RACI, i modelli di responsabilità condivisa e così via? È necessario aggiornare qualche Runbook?
- Qual era la differenza tra la valutazione d'impatto iniziale e la valutazione d'impatto finale? Cosa possiamo fare per migliorare l'accuratezza delle valutazioni nelle fasi iniziali della risposta all'incidente?
- Quali sono gli elementi d'azione tratti dalle lezioni apprese?

Runbook di risposta agli incidenti di sicurezza in AMS

Questa sezione contiene due runbook:

- Risposta all'attività dell'utente root
- Risposta agli eventi di malware

Risposta all'attività dell'utente root

L'utente root è il superutente del tuo AWS account. Tieni presente che AMS monitora l'utilizzo dei root. È consigliabile utilizzare l'utente root solo per le poche attività che lo richiedono, ad esempio modificare le impostazioni dell'account, attivare l'accesso AWS Identity and Access Management (IAM) alla fatturazione e alla gestione dei costi, modificare la password root e attivare l'autenticazione a più fattori (MFA). Per ulteriori informazioni, consulta Attività che richiedono credenziali utente root.

Per ulteriori informazioni su come informare AMS dell'utilizzo root pianificato, consulta Quando e come utilizzare l'account root in AMS.

Quando viene rilevata un'attività dell'utente root, sia che si tratti di tentativi falliti di accesso, che potrebbero indicare un attacco di forza bruta, sia di attività nell'account dopo un accesso riuscito, viene generato un evento e viene inviato un incidente ai contatti di sicurezza definiti.

AWS Managed Services Operations analizza le attività non pianificate degli utenti root, esegue la raccolta, il triage e l'analisi dei dati ed esegue attività di contenimento secondo le tue indicazioni, seguite dall'analisi post-evento.

Se utilizzi il modello operativo AMS Advanced, ricevi comunicazioni aggiuntive dagli ingegneri di AMS CSDM e AMS Ops che confermano l'attività non pianificata dell'utente root, dovuta alla responsabilità di AMS di proteggere le credenziali degli utenti root. AMS analizza l'attività dell'utente root fino a quando non viene confermato un percorso da seguire.

Preparazione

Informate AMS di qualsiasi utilizzo pianificato dell'utente root inviando una richiesta di servizio AMS con i dati e gli orari dell'evento pianificato per evitare attività di risposta agli incidenti non necessarie.

Rivolgiti periodicamente GameDays ad AMS per verificare che i processi di risposta agli incidenti dei clienti di AMS siano aggiornati, le persone e i sistemi e costruisci una memoria muscolare con le persone responsabili per ottenere una risposta più rapida agli incidenti.

Fase A: rilevamento

AMS monitora l'attività principale negli account attraverso fonti di rilevamento, tra cui GuardDuty il monitoraggio AMS.

Se disponi di AMS Accelerate, il modello operativo risponde all'incidente richiedendo un'indagine per eventuali attività impreviste dell'utente root. Quando ciò si verifica, AMS Operations avvia il Compromised Account runbook.

Se disponi di AMS Advanced, il modello operativo risponde all'incidente o informa il CSDM di qualsiasi attività pianificata dell'utente root per chiudere un'indagine attiva sulla compromissione dell'account.

Fase B: analisi

AMS esegue un'indagine approfondita sugli eventi degli utenti root quando determina che l'attività non è autorizzata. Utilizzando sia le automazioni che il team di risposta alla sicurezza AMS, i log e gli eventi vengono analizzati alla ricerca di anomalie e comportamenti imprevisti per gli utenti root. I log vengono forniti per aiutare a determinare se l'attività è sconosciuta, se si tratta di un evento utente root autorizzato o se richiede ulteriori indagini.

Alcuni esempi delle informazioni fornite durante l'indagine a supporto dei controlli interni includono:

- Informazioni sull'account: su quale account è stato utilizzato l'account root?
- Indirizzo e-mail per l'utente root: ogni utente root è associato a un indirizzo e-mail dell'organizzazione
- Dettagli di autenticazione: da dove e quando l'utente root ha avuto accesso al vostro ambiente?
- Record di attività: cosa ha fatto l'utente dopo aver effettuato l'accesso come root? Questi record sono sotto forma di CloudWatch eventi. Capire come leggere questi registri aiuta nelle indagini.

È consigliabile essere pronti a ricevere le informazioni di analisi e disporre di un piano per contattare i punti di contatto autorizzati per gli account all'interno dell'organizzazione. Poiché gli utenti root non vengono nominati come individui, determinare chi ha accesso all'indirizzo di posta elettronica principale utilizzato per l'account all'interno dell'organizzazione aiuta a indirizzare rapidamente le domande all'interno dell'organizzazione.

Fase C: contenimento ed eliminazione

AMS collabora con i tuoi team di sicurezza per eseguire il contenimento seguendo le indicazioni dei tuoi contatti autorizzati per la Customer Security. Le opzioni di contenimento includono:

- Rotazione delle credenziali e delle chiavi appropriate.
- Interruzione delle sessioni attive su account e risorse.
- Eliminazione delle risorse create.

Durante le attività di contenimento, AMS collabora a stretto contatto con il vostro team di sicurezza per garantire che eventuali interruzioni dei carichi di lavoro siano ridotte al minimo e che le credenziali root siano protette in modo adeguato.

Una volta completato il piano di contenimento, collaborerai con il team operativo di AMS per tutte le azioni di ripristino necessarie.

Rapporto successivo all'incidente

Se necessario, AMS avvia il processo di revisione delle indagini per identificare le lezioni apprese. Come parte del completamento di un COE, AMS comunica tutti i risultati pertinenti ai clienti interessati per aiutarli a migliorare il processo di risposta agli incidenti.

AMS documenta tutti i dettagli finali dell'indagine, raccoglie le metriche appropriate e quindi segnala l'incidente a tutti i team interni di AMS che richiedono informazioni, compresi il CSDM e la CA assegnati.

Risposta agli eventi di malware

Le EC2 istanze Amazon vengono utilizzate per ospitare una varietà di carichi di lavoro, tra cui software di terze parti e software sviluppato su misura distribuito dai team applicativi all'interno delle organizzazioni. AMS fornisce e ti incoraggia a distribuire i tuoi carichi di lavoro su immagini che vengono patchate e gestite su base continuativa da AMS.

Durante il funzionamento delle istanze, AMS monitora le anomalie nel comportamento o nell'attività attraverso una serie di controlli di rilevamento della sicurezza, tra cui Amazon, Endpoint Protection GuardDuty, Network Traffic e feed interni di Amazon sulle minacce.

I clienti AMS con il modello operativo AMS Advanced installano automaticamente il client di monitoraggio della sicurezza degli endpoint (EPS) sulle risorse assegnate. Ciò garantisce che le risorse siano monitorate e supportate 24 ore su 24, 7 giorni su 7, inclusa la creazione di un incidente di sicurezza quando viene rilevato un evento.

AMS monitora anche Malware GuardDuty Findings. Questi sono disponibili sia su AMS Advanced che su AMS Accelerate, se abilitati. Per ulteriori informazioni, consulta GuardDuty la sezione Protezione da malware in Amazon.

> **Note**
>
> Se hai optato per Bring Your Own EPS, la procedura di risposta agli incidenti è diversa da quella descritta in questa pagina. Per ulteriori informazioni, consulta la documentazione di riferimento.

Quando viene rilevato un malware, viene creato un incidente e l'utente riceve una notifica dell'evento. Questa notifica è seguita da tutte le attività di riparazione che si sono verificate. AMS Operations indaga, esegue la raccolta, il triage e l'analisi dei dati, quindi esegue attività di contenimento secondo le indicazioni del cliente, seguite dall'analisi post-evento.

Fase A: Rilevamento

AMS monitora gli eventi sulle istanze con il monitoraggio di una soluzione GuardDuty di sicurezza degli endpoint. AMS determina le attività di arricchimento e valutazione appropriate per aiutarvi a prendere decisioni di contenimento o di accettazione del rischio in base al tipo di scoperta o di avviso.

La raccolta dei dati viene eseguita in base al tipo di risultato. La raccolta dei dati prevede l'interrogazione di più fonti di dati sia all'interno che all'esterno dell'account interessato per creare un quadro dell'attività osservata o delle configurazioni che destano preoccupazione.

AMS esegue la correlazione dei risultati con altri allarmi e avvisi o telemetria provenienti da qualsiasi account interessato o piattaforma AMS di intelligence sulle minacce.

Fase B: analisi

Una volta raccolti, i dati vengono analizzati per identificare eventuali attività o indicatori di preoccupazione. Durante questa fase dell'indagine, AMS collabora con voi per integrare le conoscenze aziendali e di settore relative alle istanze e ai carichi di lavoro, al fine di aiutarvi a capire cosa ci si aspetta da ciò che è fuori dall'ordinario.

Alcuni esempi delle informazioni fornite durante l'indagine a supporto dei controlli interni includono:

- Informazioni sull'account: su quale account è stata osservata l'attività del malware?
- Dettagli sull'istanza: Quali istanze sono implicate negli eventi relativi al malware?
- Timestamp dell'evento: quando è scattato l'avviso?
- Informazioni sul carico di lavoro: cosa è in esecuzione sull'istanza?

- Dettagli sul malware, se pertinenti: famiglie di malware e informazioni open source sul malware.
- Dettagli sugli utenti o sui ruoli: quali utenti o ruoli sono interessati e coinvolti nell'attività?
- Record delle attività: quali attività vengono registrate sull'istanza? Questi sono sotto forma di CloudWatch eventi ed eventi di sistema generati dall'istanza. Capire come leggere questi registri ti aiuterà nelle indagini
- Attività di rete: quali endpoint si connettono all'istanza, a cosa si connette l'istanza e cos'è l'analisi del traffico?

È consigliabile essere pronti a ricevere informazioni sulle indagini e predisporre un piano su come contattare i punti di contatto appropriati per account, istanze e carichi di lavoro all'interno dell'organizzazione. Comprendere la topologia di rete e la connessione prevista può aiutare ad accelerare l'analisi dell'impatto. Anche la conoscenza dei test di penetrazione pianificati nell'ambiente e delle recenti implementazioni eseguite dai proprietari delle applicazioni può accelerare le indagini.

Se si determina che l'attività è pianificata e autorizzata, l'incidente viene aggiornato e l'indagine termina. Se il compromesso viene confermato, tu e AMS stabilite il piano di contenimento appropriato.

Fase C: Contenere ed eliminare

AMS collabora con te per determinare le attività di contenimento appropriate sulla base dei dati raccolti e delle informazioni note. Le opzioni di contenimento includono, a titolo esemplificativo ma non esaustivo:

- Conservazione dei dati tramite istantanee
- Modifica delle regole di rete per limitare il traffico in entrata o in uscita dalle istanze
- Modifica delle policy relative agli utenti e ai ruoli di SCP, IAM per limitare l'accesso
- Chiusura, sospensione o disattivazione delle istanze
- Interruzione di qualsiasi connessione persistente
- Rotazione delle credenziali/chiavi appropriate

Se scegli di eseguire l'attività di eradicazione sull'istanza, AMS ti aiuta a raggiungere tale obiettivo. Le opzioni includono, a titolo esemplificativo ma non esaustivo:

- Rimozione di qualsiasi software indesiderato

- Ricostruzione dell'istanza da un'immagine pulita e completamente patchata e ridistribuzione delle applicazioni e della configurazione
- Ripristino dell'istanza da un backup precedente
- Distribuzione di applicazioni e servizi su un'altra istanza all'interno dell'account che potrebbe essere adatta a ospitare i carichi di lavoro.

È importante determinare in che modo il malware è stato distribuito ed eseguito sull'istanza prima del ripristino del servizio per assicurarsi che vengano applicati eventuali controlli aggiuntivi per prevenire la ricomparsa del malware sull'istanza. AMS fornisce approfondimenti o informazioni aggiuntivi ai tuoi partner o team forensi, se necessario per supportare l'analisi forense.

A questo punto, collabori con AMS Operations per le attività di ripristino. AMS collabora a stretto contatto con te per ridurre al minimo le interruzioni dei carichi di lavoro e proteggere le istanze.

Rapporto successivo all'incidente

Se necessario, AMS avvia il processo di revisione delle indagini per identificare le lezioni apprese. Nell'ambito del completamento di un COE, AMS vi comunica i risultati pertinenti per aiutarvi a migliorare il processo di risposta agli incidenti.

AMS documenta i dettagli finali dell'indagine, raccoglie i parametri appropriati e segnala l'incidente ai team interni di AMS che richiedono informazioni, compresi il CSDM e la CA assegnati.

Verifica della sicurezza delle richieste di modifica in AMS Advanced

Il processo di revisione delle richieste di modifica di AWS Managed Services garantisce che AMS esegua una revisione di sicurezza delle modifiche richieste man mano che vengono implementate per tuo conto nel tuo account.

Standard tecnici avanzati AMSdefinisci i criteri di sicurezza minimi, le configurazioni e i processi per stabilire la sicurezza di base dei tuoi account. Quando AMS implementa le modifiche richieste, seguiamo questi standard.

AMS valuta tutte le richieste di modifica rispetto agli standard tecnici AMS. Qualsiasi modifica che possa ridurre il livello di sicurezza del tuo account deviando dagli standard tecnici viene sottoposta a un processo di revisione della sicurezza. Durante questo processo, i rischi rilevanti vengono evidenziati da AMS e analizzati e approvati dal vostro responsabile dell'approvazione del rischio autorizzato per bilanciare le esigenze di sicurezza e quelle aziendali.

Processo di gestione dei rischi per la sicurezza dei clienti

Il processo AMS Advanced Customer Security Risk Management (CSRM) aiuta a identificare e comunicare chiaramente i rischi ai proprietari giusti. Questo processo riduce al minimo i rischi di sicurezza nell'ambiente e riduce il sovraccarico operativo continuo per i rischi identificati.

Per impostazione predefinita, quando un membro dell'organizzazione richiede ad AMS di implementare una modifica all'ambiente gestito, AMS esamina la modifica per determinare se la richiesta non rientra negli standard tecnici, il che potrebbe alterare il livello di sicurezza dell'account. Se esiste un rischio di sicurezza elevato o molto elevato, la revisione della modifica viene accettata o rifiutata dal personale di sicurezza autorizzato. Le modifiche richieste vengono inoltre valutate per rilevare eventuali effetti negativi sulla capacità di AMS di gestire l'account. Se la revisione rileva possibili impatti negativi, sono necessarie ulteriori revisioni e approvazioni all'interno di AMS.

È possibile disattivare il flusso di lavoro basato sull'approvazione nel processo CSRM per rischi elevati o molto elevati. Per modificare l'opzione CSRM per account specifici da CSRM standard a Solo notifica, collabora con i tuoi Cloud Service Delivery Manager per creare un'accettazione del rischio una tantum. Se scegli di procedere con l'opzione Solo notifica, AMS implementa le modifiche richieste indipendentemente dalla categoria di rischio. Inoltre, AMS invia una notifica di rischio ai responsabili autorizzati dell'approvazione del rischio anziché richiedere l'approvazione prima dell'implementazione della modifica. Rivolgiti ai tuoi Cloud Architect o Cloud Service Delivery Manager per ulteriori informazioni sul processo AMS CSRM, su come modificare l'opzione CSRM predefinita durante l'onboarding di nuovi account AMS o su come aggiornare gli account esistenti.

> **Note**
>
> AMS consiglia vivamente di utilizzare l'opzione predefinita di Standard CSRM in tutti gli account.

Standard tecnici avanzati AMS

Le seguenti sono le categorie degli standard tecnici AMS Advanced:

ID	Categoria
AMS-STD-001	Configurazione dei tag

ID	Categoria
AMS-STD-002	AWS Identity and Access Management
AMS-STD-003	Sicurezza di rete
AMS-STD-004	Test di penetrazione
AMS-STD-005	Amazon GuardDuty
AMS-STD-006	Sicurezza dell'host
AMS-STD-007	Registrazione di log
AMS-STD-008	SONO PAZZO
AMS-STD-009	Varie

Controlli standard in AMS Advanced

I seguenti sono i controlli standard di AMS:

AMS-STD-001 - Configurazione dei tag

Di seguito è riportato il controllo standard per 001 - Tagging Configuration.

1. Tutte le AWS risorse richieste dal team AMS per scopi operativi e gestionali devono avere la seguente coppia chiave-valore.
   - AppId= AMSInfrastructure
   - Ambiente= AMSInfrastructure
   - AppName = AMSInfrastructure
   - AMSResource=Vero
2. Tutti i tag richiesti dal team AMS diversi da quelli elencati in precedenza devono avere i prefissi indicati nell'elenco dei prefissi AMS (vedi Nota).
3. I valori dei tag richiesti dal team AMS (AppId, Environment and AppName) possono essere modificati su qualsiasi risorsa creata dall'utente in base alle richieste di modifica.
4. Qualsiasi tag sugli stack richiesto da AMS non deve essere eliminato in base alle richieste di modifica.

5. Non è possibile utilizzare la convenzione di denominazione dei tag AMS per la propria infrastruttura, come indicato al punto 2.
6. È possibile creare tag personalizzati nelle risorse richieste da AMS (in genere per casi di utilizzo relativi alla fatturazione e alla rendicontazione dei costi). I tag personalizzati vengono mantenuti se le risorse vengono aggiornate tramite l'aggiornamento dello stack e non mediante l'aggiornamento del modello.

Note

Elenco dei prefissi AMS

1. ams-*
2. AWSManagedServizi*
3. /ams/ *
4. ams*
5. MASSA*
6. Nome*
7. cm*
8. MC*
9. Mc*
10. sentinella*
11. Sentinella*
12. Servizi gestiti*
13. Nuovo AMS*
14. AWS_*
15. aws*
16. VPC_*
17. CloudTrail*
18. Sentiero nuvoloso*
19. /aws_riservato/
20. INGERI*
21. EPSDB*

22. MMS*
23. TemplateId*
24. StackSet-ams*
25. StackSet-AWS - Zona di atterraggio
26. IAMPolicy*
27. cliente-mc-*
28. Radice*
29. LandingZone*
30. StateMachine*
31. codedeploy_service_role
32. host di gestione
33. sentinel.int.
34. EPS
35. UnhealthyInServiceBastion
36. ms-

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

ID	Standard tecnico
1.0	Durata del timeout
1.1	Una sessione di timeout predefinita per utenti federati è di un'ora e può essere aumentata fino a quattro ore.
1.2	Il tempo di accesso allo stack predefinito è di 12 ore.
2.0	AWS Utilizzo dell'account root
2.1	Se viene utilizzato un account root per qualsiasi motivo, Amazon GuardDuty deve essere configurato per generare risultati pertinenti.

ID	Standard tecnico
2.2	Per gli account single-account landing zone (SALZ) e gli account di gestione multi-account landing zone (MALZ) (precedentemente noto come account), l' Master/Billing account utente Root deve avere l'MFA virtuale abilitata e il soft token MFA viene scartato durante l'onboarding dell'account, in modo che né AMS né i clienti possano accedere come root. La procedura standard di perdita della password AWS root deve essere seguita insieme a AMS Cloud Service Delivery Manager (CSDM). Questa configurazione deve rimanere valida durante il ciclo di vita degli account gestiti da AMS.
2.3	Non è necessario creare chiavi di accesso per l'account root.
3.0	Creazione e modifica degli utenti
3.1	È possibile creare IAM users/roles con accesso programmatico e con autorizzazioni di sola lettura senza alcuna politica limitata nel tempo. Tuttavia, l'autorizzazione a consentire la lettura di oggetti (ad esempio, S3:GetObject) in tutti i bucket Amazon Simple Storage Service dell'account non è consentita.

ID	Standard tecnico
3.1.1	Gli utenti umani IAM per l'accesso alla console e con autorizzazioni di sola lettura possono essere creati con la politica limitata nel tempo (fino a 180 giorni), mentre la removal/renewal/ extension politica limitata nel tempo comporterà la notifica del rischio. Tuttavia, l'autorizzazione a consentire la lettura di oggetti (ad esempio, S3:GetObject) in tutti i bucket S3 dell'account non è consentita.
3.2	Gli utenti e i ruoli IAM per l'accesso da console e programmatico con autorizzazioni che modificano l'infrastruttura (scrittura e gestione delle autorizzazioni) nell'account del cliente non devono essere creati senza l'accettazione del rischio. Esistono eccezioni per le autorizzazioni di scrittura a livello di oggetto S3, consentite senza l'accettazione del rischio, purché i bucket specifici rientrino nell'ambito di applicazione e per le operazioni di etichettatura su tag non correlati ad AMS.
3.3	Gli utenti IAM con accesso programmatico, denominati `customer_servicenow_user` e `customer_servicenow_logging _user` necessari per ServiceNow l'integra zione nell'account dell'applicazione SALZ o MALZ e negli *account principali* possono essere creati senza alcuna politica limitata nel tempo.

ID	Standard tecnico
3.4	È possibile creare utenti IAM con accesso programmatico, utilizzo `customer_cloud_endure_policy` e `customer_cloud_endure_deny_policy` (con accesso in sola lettura) necessari per l' CloudEndure integrazione negli account SALZ e MALZ, ma necessitano di una policy limitata nel tempo per il periodo della migrazione pianificata. Il limite di tempo può essere di un periodo massimo di 180 giorni senza RA. L'SCP è inoltre autorizzato a modificare gli account MALZ per consentire a queste politiche di funzionare per il periodo richiesto. È possibile definire le finestre di migrazione appropriate per le proprie esigenze e modificarle in base alle esigenze.
4.0	Politiche, azioni e APIs
4.1	Tutti gli utenti e i ruoli IAM negli account SALZ devono avere la Customer Deny Policy (CDP) predefinita allegata per proteggere l'infrast ruttura AMS da danni accidentali o intenzionali.
4.2	AMS SCPs deve essere abilitato in tutti gli account gestiti da AMS in MALZ.
4.3	Le identità in grado di eseguire azioni amministrative sulle chiavi KMS, ad esempio, e `PutKeyPolicy ScheduleKeyDeletion` , devono essere limitate solo agli operatori AMS e ai responsabili di automazione.

ID	Standard tecnico
4.4	Una policy non deve fornire all'amministratore un'istruzione equivalente a «Effect»: «Allow» con «Action»: «*» su «Resource»: «*» senza l'accettazione del rischio.
4.5	La policy IAM non deve includere alcuna azione che includa l'azione Allow S3: *** su qualsiasi bucket senza accettazione del rischio.
4.6	Le chiamate API contro le politiche chiave KMS per le chiavi dell'infrastruttura AMS nelle politiche IAM del cliente non devono essere consentite.
4.7	Le azioni che aggirano il processo di gestione delle modifiche (RFC) non devono essere consentite, come l'avvio o l'arresto dell'istanza, la creazione di un bucket S3 o di un'istanza RDS e così via.
4.8	Le azioni che apportano modifiche ai record DNS dell'infrastruttura AMS in Amazon Route 53 non devono essere consentite.
4.9	Gli utenti umani IAM con accesso alla console, creati dopo aver seguito il giusto processo, non devono avere alcuna policy collegata direttame nte, ad eccezione della policy trust, assume role e time limited policy.
4.10	È possibile creare profili di EC2 istanze Amazon con accesso in lettura a un segreto o uno spazio dei nomi specifico Gestione dei segreti AWS all'interno dello stesso account.

ID	Standard tecnico
4.11	Le autorizzazioni di AWS Managed Services Change Management (AMSCM) o AWS Managed Services Service Knowledge Management System (AMSSKMS) possono essere aggiunte a qualsiasi ruolo (possibilità di aprire). SR/Incident/RFC
4.12	La politica IAM non deve includere alcuna azione che includa l'azione Allow logs: DeleteLogGroup e logs: DeleteLogStream su qualsiasi gruppo di CloudWatch log AMS Amazon.
4.13	Le autorizzazioni per creare chiavi multiregi onali non devono essere consentite.
4.14	Per fornire l'accesso ai bucket S3 ARNs che non sono ancora stati creati nei tuoi account, utilizza la chiave `s3:ResourceAccount` di condizione S3 specifica del servizio per specificare il numero di account.
4.15	Puoi visualizzare, creare, elencare ed eliminare l'accesso alla tua dashboard personalizzata, ma solo l'accesso alla visualizzazione e all'elenco sulle CloudWatch dashboard di Amazon.
4.15.1	Puoi visualizzare, creare, elencare ed eliminare l'accesso alla dashboard personalizzata di S3 Storage Lens.
4.16	È possibile concedere autorizzazioni complete relative a SQL Workbench per roles/users lavorare sui database Amazon Redshift.

ID	Standard tecnico
4.17	Qualsiasi AWS CloudShell autorizzazione può essere concessa ai ruoli del cliente in alternati va alla CLI.
4.18	Un ruolo IAM con un Servizio AWS responsab ile affidabile deve inoltre essere conforme agli standard tecnici IAM.
4.19	I Service Linked Roles (SLRs) non sono soggetti agli standard tecnici AMS IAM, in quanto sono creati e gestiti da IAM Service Team.
4.20	Le policy IAM non devono consentire l'accesso illimitato in lettura agli oggetti bucket Amazon S3 (ad esempio, Amazon S3GetObject:) su tutti i bucket di un account: • Negli account in modalità sviluppatore: le violazioni generano una notifica di rischio • Negli account in modalità non sviluppatore: le violazioni richiedono l'accettazione del rischio
4.21	Tutte le autorizzazioni IAM per il tipo di risorsa «savingsplan» possono essere concesse ai clienti.
4.22	I tecnici AMS non sono autorizzati a copiare o spostare manualmente i dati dei clienti (file, oggetti S3, database) in nessuno dei servizi di storage dei dati, come Amazon S3, Amazon Relational Database Service, Amazon DynamoDB e così via, o nel file system del sistema operativo.

ID	Standard tecnico
4.23	La politica SCP non deve essere modificata per consentire accessi aggiuntivi in nessuno degli account gestiti da AMS.
4.24	Non devono essere consentite modifiche alla politica SCP che potrebbero compromettere l'infrastruttura o le capacità di gestione di AMS. (Nota: le risorse AMS hanno il tag `AppId= AMSInfrastructure` e seguono l'AMS Protected Namespace).
4.25	La funzionalità AMS Automated IAM Provision ing deve essere abilitata nei tuoi account come funzionalità opzionale.
4.26	I ruoli o gli utenti di AMS assunti da persone non devono avere accesso ai contenuti dei clienti in S3, RDS, DynamoDB, Redshift, Elasticache, EFS e. FSx Inoltre, qualsiasi accesso a contenuti nuovi e noti APIs rilasciati da altri Servizi AWS che garantiscono l'accesso ai contenuti dei clienti deve essere esplicita mente negato nei ruoli di operatore.
5.0	Federazione
5.1	L'autenticazione deve essere configurata utilizzando la federazione nell'account gestito da AMS.
5.2	Deve esserci un solo trust in uscita unidirezi onale da AMS AD all'Active Directory (AMS AD si affida ad on-premise).

ID	Standard tecnico
5.3	Gli archivi di identità utilizzati per l'autenti cazione su AMS non devono esistere negli account delle applicazioni gestite da AMS.
6.0	Politiche trasversali agli account
6.1	È possibile configurare le politiche di fiducia dei ruoli IAM tra account AMS che appartengono allo stesso cliente in base ai record dei clienti.
6.2	Le politiche di fiducia dei ruoli IAM tra account AMS e non AMS devono essere configura te solo se l'account non AMS è di proprietà dello stesso cliente AMS (confermando che si trovano sotto lo stesso AWS Organizations account o abbinando il dominio e-mail al nome dell'azienda del cliente).
6.3	Le politiche di fiducia dei ruoli IAM tra account AMS e account di terze parti non devono essere configurate senza l'accettazione del rischio.
6.4	È possibile configurare politiche su più account per accedere a qualsiasi account AMS gestito dal cliente CMKs tra account AMS dello stesso cliente.
6,5	È possibile configurare politiche tra account per accedere a qualsiasi chiave KMS all'interno di un account non AMS tramite un account AMS.

ID	Standard tecnico
6.6	Le politiche relative all'accesso a qualsiasi chiave KMS all'interno di un account AMS da parte di un account di terze parti non devono essere consentite senza l'accettazione del rischio.
6.6.1	Le politiche tra account per l'accesso a qualsiasi chiave KMS all'interno di un account AMS tramite un account diverso da AMS possono essere configurate solo se l'account non AMS è di proprietà dello stesso cliente AMS.
6.7	È possibile configurare policy tra più account per accedere a qualsiasi dato o risorsa del bucket S3 in cui i dati possono essere archiviat i (come Amazon RDS, Amazon DynamoDB o Amazon Redshift) tra account AMS dello stesso cliente.
6.8	È possibile configurare policy tra account per accedere a tutti i dati o le risorse del bucket S3 in cui i dati possono essere archiviati (come Amazon RDS, Amazon DynamoDB o Amazon Redshift) in un account non AMS da un account AMS con accesso in sola lettura.

ID	Standard tecnico
6.9	Le policy tra account per accedere a tutti i dati o le risorse del bucket S3 in cui i dati possono essere archiviati (come Amazon RDS, Amazon DynamoDB o Amazon Redshift) con autorizza zioni di scrittura da AMS a un account non AMS (o da un account non AMS a AMS) devono essere configurate solo se l'account non AMS è di proprietà dello stesso cliente AMS (conferma ndo che si trovano sullo stesso account o abbinando dominio email con il nome dell' AWS Organizations azienda del cliente).
6,10	È possibile configurare policy tra account per accedere a tutti i dati o le risorse del bucket S3 in cui i dati possono essere archiviati (come Amazon RDS, Amazon DynamoDB o Amazon Redshift) in un account di terze parti da un account AMS con accesso in sola lettura.
6.11	Le policy tra account per accedere a qualsiasi dato o risorsa del bucket S3 in cui i dati possono essere archiviati (come Amazon RDS, Amazon DynamoDB o Amazon Redshift) in un account di terze parti da un account AMS con accesso in scrittura non devono essere configurate.
6.12	Le politiche interaccount di account di terze parti per accedere a un bucket S3 o alle risorse in cui è possibile archiviare i dati (come Amazon RDS, Amazon DynamoDB o Amazon Redshift) non devono essere configurate senza l'accettazione del rischio.
7.0	Gruppi di utenti

ID	Standard tecnico
7.1	I gruppi IAM con autorizzazioni di sola lettura e non mutative sono consentiti.
8.0	Policy basate su risorse
8.1	Le risorse dell'infrastruttura AMS devono essere protette dalla gestione da parte di identità non autorizzate mediante l'aggiunta di politiche basate sulle risorse.
8.2	Le tue risorse devono essere configurate con politiche basate sulle risorse con privilegi minimi, a meno che tu non specifichi esplicita mente una politica diversa.
9.0	Servizi forniti in modalità self-service (SSPS)
9.1	Il ruolo o la policy IAM predefiniti di AMS (inclusi profilo di istanza, SSPS, pattern) non devono essere modificati con o senza alcuna accettazione del rischio. Sono consentite eccezioni (senza accettazione del rischio) per le politiche di fiducia. L'etichettatura del ruolo, della politica o delle modifiche dell'utente è consentita anche nei ruoli SSP predefiniti.
9.3	La policy SSPS per il ruolo della console Systems Manager Automation non può essere associata a nessun ruolo personalizzato oltre al ruolo predefinito. Le altre policy SSPS devono essere associate ai ruoli IAM personalizzati solo dopo aver verificato che l'associazione della policy a un ruolo personalizzato non fornisca autorizzazioni aggiuntive al di fuori della progettazione prevista per il servizio SSPS predefinito.

AMS-STD-003 - Sicurezza di rete

Di seguito è riportato il controllo standard per 003 - Network Security:

ID	Standard tecnico
	Reti
1.0	È necessario accedere a tutte EC2 le istanze tramite SSH o RDP solo tramite gli host Bastion, l'intervallo CIDR VPC VPC dell'host bastion o dall'intervallo CIDR VPC della stessa istanza.
2.0	L'IP elastico sulle istanze è consentito EC2
3.0	È necessario utilizzare il piano di controllo AMS e, per estensione, nel piano dati TLS 1.2+.
4.0	Tutto il traffico in uscita deve passare utilizzan do l'account IGW o TGW.
5.0	Un gruppo di sicurezza non deve avere l'origine 0.0.0.0/0 nella regola in entrata se non è collegato a un sistema di bilanciamento del carico come previsto dalla versione 9.0
6.0	Il bucket o gli oggetti S3 non devono essere resi pubblici senza l'accettazione del rischio.
7.0	L'accesso alla gestione dei server sulle porte SSH/22 o SSH/2222 (non SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 o 1604, LDAP/389 o 636 e RPC/135, NETBIOS/1 37-139 non deve essere consentito dall'esterno del VPC tramite gruppi di sicurezza.
8.0	L'accesso alla gestione del database sulle porte (MySQL/3306, PostgreSQL/5432, Oracle/15

ID	Standard tecnico
	21, MSSQL/1433) o sulla porta personalizzata non deve essere consentito dal pubblico non indirizzato a VPC su DX, VPC-Peer o VPN tramite un gruppo di sicurezza. IPs
8.1	Qualsiasi risorsa in cui è possibile archiviar e i dati dei clienti non deve essere esposta direttamente alla rete Internet pubblica.
9.0	L'accesso diretto alle applicazioni tramite le porte HTTP/80, HTTPS/8443 e HTTPS/443 da Internet è consentito solo ai sistemi di bilanciamento del carico, ma non direttame nte alle risorse di calcolo, ad esempio istanze, contenitori, ecc. EC2 ECS/EKS/Fargate
10.0	È possibile consentire l'accesso alle applicazi oni tramite le porte HTTP/80 e HTTPS/443 dall'intervallo IP privato del cliente.
11.0	Qualsiasi modifica ai gruppi di sicurezza che controllano l'accesso all'infrastruttura AMS non deve essere consentita senza l'accettazione del rischio.
12.0	AMS Security fa riferimento agli standard ogni volta che viene richiesto di collegare un gruppo di sicurezza a un'istanza.
13.0	L'accesso al bastione dei clienti sulle porte 3389 e 22 deve essere consentito solo da intervalli di IP privati instradati nel VPC tramite DX, VPC-Peer o VPN.

ID	Standard tecnico
14.0	L'associazione tra account di zone private ospitate VPCs da un account AMS a un altro account AMS (o da un account non AMS a AMS) deve essere configurata solo se l'account non AMS è di proprietà dello stesso cliente AMS (confermando che si trovano sullo stesso account AWS Organization o abbinando il dominio e-mail al nome dell'azienda del cliente) utilizzando strumenti interni.
15.0	È possibile consentire connessioni peering VPC tra account che appartengono allo stesso cliente.
16.0	La base AMS AMIs può essere condivisa con account non AMS a condizione che entrambi gli account siano di proprietà dello stesso cliente (confermando che appartengono allo stesso AWS Organizations account o abbinando il dominio e-mail al nome dell'azienda del cliente) utilizzando strumenti interni.
17.0	La porta FTP 21 non deve essere configurata in nessuno dei gruppi di sicurezza senza un'accett azione del rischio.
18.0	La connettività di rete tra account tramite gateway di transito è consentita a condizion e che tutti gli account siano di proprietà del cliente.
19.0	Non è consentito rendere pubblica una sottorete privata

ID	Standard tecnico
20.0	Le connessioni peering VPC con account di terze parti (non di proprietà del cliente) non devono essere consentite.
21.0	L'allegato Transit Gateway con un account di terze parti (non di proprietà del cliente) non deve essere consentito.
22.0	Qualsiasi traffico di rete necessario ad AMS per fornire i servizi ai clienti non deve essere bloccato al punto di uscita della rete del cliente.
23.0	La condivisione delle regole del resolver con quelle Account AWS di proprietà dello stesso cliente è consentita con una notifica del rischio
19.0	ICMP
19,1	La richiesta ICMP in entrata ad Amazon EC2 dall'infra del cliente richiederà una notifica del rischio.
19.2	È consentita la richiesta in entrata provenien te da un IPs instradamento pubblico verso Amazon VPC tramite DX, VPC-Peer o VPN tramite un gruppo di sicurezza.
19.3	Le richieste in entrata provenienti da un pubblico IPs non indirizzato ad Amazon VPC tramite DX, VPC-Peer o VPN tramite un gruppo di sicurezza richiederebbero l'accettazione del rischio.
19.4	È consentita la richiesta ICMP in uscita EC2 da Amazon verso qualsiasi destinazione.
20.0	Condivisione di gruppi di sicurezza

ID	Standard tecnico
20.1	Se un gruppo di sicurezza soddisfa questo standard di sicurezza, può essere condiviso tra VPCs lo stesso account e tra account della stessa organizzazione.
20.2	Se un gruppo di sicurezza non soddisfa questo standard e in precedenza era richiesta l'accetta zione del rischio per tale gruppo di sicurezza , l'uso della funzionalità di condivisione dei gruppi di sicurezza tra VPCs lo stesso account o tra account della stessa organizzazione non è consentito senza l'accettazione del rischio per quel nuovo VPC o account.

AMS-STD-004 - Test di penetrazione

Di seguito è riportato il controllo standard per 004 - Penetration Testing

1. AMS non supporta l'infrastruttura pentest. È responsabilità del cliente. Ad esempio, Kali non è una distribuzione Linux supportata da AMS.
2. I clienti devono attenersi ai test di penetrazione.
3. AMS deve ricevere una notifica preventiva con 24 ore di anticipo nel caso in cui il cliente desideri eseguire test di penetrazione dell'infrastruttura all'interno degli account.
4. AMS fornirà al cliente l'infrastruttura di pentesting in base ai requisiti del cliente esplicitamente indicati nella richiesta di modifica o nella richiesta di assistenza da parte del cliente.
5. La gestione delle identità per l'infrastruttura di pentesting del cliente è responsabilità del cliente.

AMS-STD-005 - GuardDuty

Di seguito è riportato il controllo standard per 005 - GuardDuty

1. GuardDuty deve essere abilitato in tutti gli account dei clienti in ogni momento.
2. GuardDuty I risultati del Customer Managed Application Account (CMA) in MALZ non genereranno allarmi per il team operativo.

3. GuardDuty gli avvisi devono essere archiviati nello stesso account o in qualsiasi altro account gestito dalla stessa organizzazione.
4. La funzionalità di elenco IP affidabile di non GuardDuty deve essere utilizzata. In alternativa, è possibile utilizzare l'archiviazione automatica, utile per scopi di controllo.
5. GuardDuty la delega dell'amministratore non deve essere abilitata in MALZ poiché l'amministratore delegato sarebbe in grado di eseguire azioni con privilegi elevati come disabilitarle GuardDuty negli altri account senza accettare il rischio.
6. GuardDuty I filtri di archiviazione automatica devono utilizzare l'ambito minimo per il rendimento massimo. Ad esempio, se AMS rileva più dati imprevedibili IPs in diversi blocchi CIDR e se esiste un ASN aziendale appropriato da utilizzare, utilizza l'ASN. Tuttavia, se puoi limitarti a intervalli o indirizzi /32 specifici, allora limitati a quelli.

AMS-STD-006 - Sicurezza dell'host

Di seguito è riportato il controllo standard per 006 - Host Security

- Un agente antivirus deve essere sempre in esecuzione su tutte le EC2 istanze. (ad esempio, Trend Micro DSM).
- Il modulo antimalware deve essere abilitato.
- L'agente EPS deve includere tutte le directory e i file per la scansione.
- I file messi in quarantena dalla soluzione antivirus possono essere condivisi con l'utente su richiesta.
- Non è necessario installare una soluzione di sicurezza degli endpoint di terze parti.
- La frequenza di aggiornamento delle firme antivirus deve essere impostata su almeno una volta al giorno.
- La frequenza di scansione pianificata deve essere impostata su almeno una volta al mese.
- La scansione in tempo reale (in accesso) deve essere abilitata e in esecuzione in qualsiasi momento.
- AMS non deve eseguire sulle tue istanze alcuno script personalizzato che non sia di proprietà o creato da AMS. (Nota: è possibile farlo utilizzando l'accesso Stack Admin tramite Stack Admin access CT o utilizzando AWS Systems Manager Automation (AMS SSPS).
- L'autenticazione a livello di rete (NLA) non deve essere disabilitata sull'host Windows.
- Il sistema operativo host deve essere aggiornato con le ultime patch di sicurezza in base al ciclo di patch configurato.

- Un account gestito AMS non deve contenere un'istanza non gestita nell'account.
- La creazione di account di amministratore locale sull'istanza da parte di AMS non deve essere consentita.
- La coppia di chiavi non EC2 deve essere creata.
- Non è necessario utilizzare sistemi operativi dichiarati come End of Life (EOL) e non è previsto alcun ulteriore supporto di sicurezza fornito dal fornitore o da terze parti.

AMS-STD-007 - Registrazione

Quello che segue è il controllo standard per 007 - Logging

ID	Standard tecnico
1.0	Tipi di registro
1.1	Registri del sistema operativo: tutti gli host devono registrarsi in base al numero minimo di eventi di autenticazione dell'host, eventi di accesso per tutti gli utilizzi di privilegi elevati ed eventi di accesso per tutte le modifiche alla configurazione degli accessi e dei privilegi, comprese quelle relative all'esito positivo e negativo.
1.2	AWS CloudTrail: CloudTrail la registrazione degli eventi di gestione deve essere abilitata e configurata per inviare i log a un bucket S3.
1.3	Registri di flusso VPC: tutti i registri del traffico di rete devono essere registrati tramite VPC Flow Logs.
1.4	Amazon S3 Server Access Logging: i bucket S3 obbligatori di AMS che archiviano i log devono avere la registrazione degli accessi al server abilitata.

ID	Standard tecnico
1.5	AWS Config Istantanee: AWS Config devono registrare le modifiche alla configurazione per tutte le risorse supportate in tutte le regioni e consegnare i file degli snapshot di configura zione ai bucket S3 almeno una volta al giorno.
1.6	Registri dell'Endpoint Protection System (EPS): la registrazione della soluzione EPS deve essere abilitata e configurata per inviare i log a un gruppo di log Logs. CloudWatch
1,7	Registri delle applicazioni: i clienti possono abilitare la registrazione nelle proprie applicazi oni e archiviarli nel gruppo di log Logs o in un bucket S3. CloudWatch
1.8	Registrazione a livello di oggetto S3: i clienti hanno la possibilità di abilitare la registrazione a livello di oggetto nei propri bucket S3.
1.9	Registrazione dei servizi: i clienti hanno la possibilità di abilitare e inoltrare i log per i servizi SSPS come qualsiasi altro servizio di base.
1.10	Log Elastic Load Balancing (Load Classic/A pplication Load Balancer/Network Balancer): le voci dei log di accesso e degli errori devono essere archiviate nei bucket S3 gestiti da AMS 2.0.
2.0	Controllo degli accessi

ID	Standard tecnico
2.1	Non è necessario disporre dell'accesso in scrittura o eliminazione nei bucket S3 richiesti da AMS che memorizzano log e CloudWatch Logs; gruppi di log.
2.2	È necessario disporre dell'accesso in sola lettura a tutti i log dei propri account.
2.3	I bucket S3 obbligatori di AMS che archiviano i log non devono consentire l'utilizzo di account di terze parti, come previsto dalle politiche relative ai bucket.
2.4	I log dei gruppi di CloudWatch log Logs non devono essere eliminati senza l'approvazione esplicita del contatto di sicurezza autorizzato.
3.0	Conservazione dei log
3.1	I gruppi di log CloudWatch Logs obbligatori da AMS devono avere un periodo minimo di conservazione dei log di 90 giorni.
3.2	I bucket S3 obbligatori da AMS che archiviano i log devono avere un periodo di conservazione minimo di 18 mesi sui log.
3.3	AWS Backup le istantanee dovrebbero essere disponibili con una conservazione minima di 31 giorni sulle risorse supportate.
4.0	Encryption (Crittografia)
4.1	La crittografia deve essere abilitata in tutti i bucket S3 richiesti da AMS Teams che archivia i log.

ID	Standard tecnico
4.2	Qualsiasi inoltro dei log dagli account dei clienti a qualsiasi altro account deve essere crittogra fato.
5.0	Integrità
5.1	Il meccanismo di integrità dei file di registro deve essere abilitato. La «convalida dei file di registro» deve essere configurata nei AWS CloudTrail percorsi richiesti dai team AMS.
6.0	Inoltro dei log
6.1	Qualsiasi registro può essere inoltrato da un account AMS a un altro account AMS dello stesso cliente.
6.2	Qualsiasi registro può essere inoltrato da AMS a un account diverso da AMS solo se l'account non AMS è di proprietà dello stesso cliente AMS.
6.3	I registri di un account cliente non devono essere inoltrati a un account di terzi (che non è di proprietà del cliente).

AMS-STD-008 - AMS-MAD

Di seguito è riportato il controllo standard per 008 - AMS-MAD

ID	Standard tecnico
1.0	Gestione degli accessi
1.1	Solo gli utenti con privilegi AMS con accessi interattivi e attività di automazione devono essere autorizzati ad accedere all'host di

ID	Standard tecnico
	gestione per l'amministrazione dell'AD gestito negli account dei clienti.
1.2	Gli amministratori AD devono avere solo privilegi di amministratore delegato (gruppo di amministratori delegati AMS).
1.3	I tecnici che accedono agli ambienti AD del cliente (host o istanze di gestione) devono disporre di un accesso limitato nel tempo.
1.4	I clienti hanno accesso in sola lettura agli oggetti AD utilizzando Remote Server Administrator Tools in un'istanza. EC2
1.5	I diritti amministrativi per l'utente o il gruppo di Active Directory non devono essere consentiti.
1.6	AWS La condivisione della directory con il Account AWS proprietario dello stesso cliente è consentita con una notifica del rischio.
2.0	Account di servizio
2.1	Gli account di servizio gestiti di gruppo (gMSA) devono essere utilizzati ovunque siano supportati dalle applicazioni anziché gli account di servizio standard.
2.2	Tutti gli altri account di servizio devono essere creati dopo il processo di accettazione del rischio.

ID	Standard tecnico
2.3	I gruppi di sicurezza AD non devono essere riutilizzati a meno che non sia esplicitamente richiesto dal cliente. È necessario creare nuovi gruppi AD. Gli oggetti del computer che richiedono l'accesso all'account del servizio devono essere aggiunti al nuovo gruppo di sicurezza.
2.4	Qualsiasi account di servizio gMSA deve essere aggiunto all'unità organizzativa (OU) «Account di servizio gestito».
2.5	Tutti gli account di servizio non GMSA devono essere aggiunti nell'unità organizzativa «Users→Account di servizio».
3.0	Oggetti di policy di gruppo (GPO)
3.1	Le impostazioni del GPO «Impostazioni di Windows > Impostazioni di sicurezza» non devono essere modificate se riducono in qualche modo il livello di sicurezza dell'account rispetto allo stato corrente.
3.2	In MALZ, RFCs inviato da un account dell'appl icazione che richiede la creazione di un GPO, il GPO deve essere collegato all'unità organizza tiva corrispondente all'account dell'app. Qualsiasi elemento GPOs che influisca su tutti gli account deve provenire dall'account Shared Service.
3.3	Il timeout predefinito della sessione di inattivit à RDP deve essere impostato su 15 minuti per tutti i server del dominio Active Directory.

ID	Standard tecnico
4.0	Active Directory Trust
4.1	La fiducia in uscita unidirezionale (da directory ospitata da AMS a Customer Directory) è consentita se i server IPs di inoltro condizion ali vengono indirizzati a VPC tramite DX, VPC-Peer o VPN.
5.0	Altri
5.1	Il meccanismo di integrità dei file di registro deve essere abilitato. La «convalida dei file di registro» deve essere configurata nei AWS CloudTrail percorsi richiesti dai team AMS.
6.0	Inoltro dei log
6.1	Gli utenti, i gruppi, gli oggetti informatici, le unità organizzative o altre entità del cliente non devono utilizzare la convenzione di denominazione AMS secondo la convenzione di denominazione AMS.
6.2	Tutto OUs deve essere gestito da AMS.

AMS-STD-009 - Varie

Di seguito è riportato il controllo standard per 009 - Varie

- Se la crittografia è abilitata in una risorsa, oggetto, database o file system, non deve essere disabilitata.

Modifiche che introducono rischi di sicurezza elevati o molto elevati nell'ambiente

Le seguenti modifiche introducono un rischio di sicurezza elevato o molto elevato nell'ambiente in uso:

AWS Identity and Access Management

- High_risk-IAM-001: crea chiavi di accesso per l'account root
- high_risk-IAM-002: modifica della politica SCP per consentire accessi aggiuntivi
- high_risk-IAM-003: modifica della politica SCP che potrebbe compromettere l'infrastruttura AMS
- high_risk-IAM-004: creazione di un file role/user con infrastruttura che modifica le autorizzazioni (scrittura, gestione delle autorizzazioni o etichettatura) nell'account del cliente
- high_risk-IAM-005: IAM gestisce le politiche di trust tra account AMS e account di terze parti (non di proprietà del cliente)
- high_risk-IAM-006: politiche interaccount per accedere a qualsiasi chiave KMS da un account AMS tramite un account di terze parti)
- high_risk-IAM-007: politiche tra account di terze parti per accedere al bucket S3 di un cliente AMS o a risorse in cui è possibile archiviare i dati (come Amazon RDS, Amazon DynamoDB o Amazon Redshift)
- high_risk-IAM-008: assegna le autorizzazioni IAM a qualsiasi autorizzazione che modifichi l'infrastruttura nell'account del cliente
- high_risk-IAM-009: consenti l'elenco e la lettura su tutti i bucket S3 dell'account
- high_risk-IAM-010: read/write provisioning IAM automatizzato con autorizzazioni

Sicurezza della rete

- High_risk-NET-001: porte di gestione del sistema operativo aperte SSH/22 o SSH/2222 (non SFTP/2222), TELNET/23, RDP/3389, WinRM/5985-5986, VNC/ 5900-5901 TS/CITRIX/1494 o 1604, LDAP/389 o 636 e NETBIOS/137-139 da Internet
- High_risk-NET-002: porte di gestione del database aperte MySQL/3306, PostgreSQL/5432, Oracle/1521, MSSQL/1433 o qualsiasi porta cliente di gestione da Internet
- High_risk-net-003: apri le porte applicative HTTP/80, HTTPS/8443 e HTTPS/443 direttamente su qualsiasi risorsa di calcolo. Ad esempio, EC2 ECS/EKS/Fargate istanze, contenitori e così via da Internet

- High_risk-net-004: qualsiasi modifica ai gruppi di sicurezza che controllano l'accesso all'infrastruttura AMS
- High_risk-net-006: peering VPC con l'account di terze parti (non di proprietà del cliente)
- High_risk-net-007: aggiunta del firewall del cliente come punto di uscita per tutto il traffico AMS
- High_risk-NET-008: l'allegato Transit Gateway con l'account di terze parti non è consentito
- High_Risk-S3-001: fornisce o abilita l'accesso pubblico nel bucket S3

Registrazione di log

- CloudTrailHigh_risk-log-001: disabilita. (È richiesta l'approvazione di Ops Site Manager)
- High_risk-log-002: disabilita i registri di flusso VPC. (È richiesta l'approvazione di Ops Site Manager)
- High_risk-log-003: inoltro dei log tramite qualsiasi metodo (notifica di eventi S3, pull dell'agente SIEM, push dell'agente SIEM, ecc.) da un account gestito da AMS a un account di terze parti (non di proprietà del cliente)
- High_risk-log-004: utilizza percorsi non AMS per CloudTrail

Sicurezza dell'host

- High_risk-host-001: disabilita End Point Security nell'account per qualsiasi motivo. (È richiesta l'approvazione di Ops Site Manager)
- High_risk-host-002: disabilita l'applicazione di patch in una risorsa o a livello di account.
- High_risk-host-003: distribuzione di un'istanza non gestita nell'account. EC2
- High_risk-host-004: esecuzione di uno script personalizzato fornito dal cliente.
- High_risk-host-005: creazione di account di amministratore locale sulle istanze.
- High_risk-host-006: tipo/estensione di file Trend Micro EPS, esclusioni dalla scansione o disattivazione della protezione da malware sugli endpoint.

> **Note**
>
> L'accettazione del rischio non è richiesta per le esclusioni anti-malware EPS o le regole di GuardDuty soppressione relative ai test di penetrazione o alle scansioni di vulnerabilità o ai problemi di servizio che influiscono sulle prestazioni, che giustificano azioni proattive. events/known Una notifica di rischio è sufficiente in queste situazioni.

- High_risk-host-007: Crea per KeyPair EC2
- High_risk-host-008: disabilita la sicurezza degli endpoint nel EC2
- High_risk-host-009: account che utilizzano il sistema operativo End of Life (EOL)

Miscellaneous (Varie)

- High_risk-ENC-001: disabilita la crittografia in qualsiasi risorsa se è abilitata

Active Directory gestita

- High_risk-AD-001: Fornisci i diritti di amministratore all'utente o al gruppo Active Director
- High_risk-AD-002: politiche GPO in grado di ridurre il livello di sicurezza dell'account

Gestione della continuità in AMS Advanced

Nell'ambito della gestione della continuità, AWS Managed Services (AMS) fornisce l'accesso automatizzato a AWS Backup un servizio nativo con AWS. Ciò facilita l'accesso a un servizio che supporta Amazon EBS, Amazon, EC2 Amazon RDS, Amazon EFS e altro ancora.

Per saperne di più, consulta AWS Backup: Come funziona.

Argomenti

Cos'è la gestione della continuità?

La gestione della continuità è il processo utilizzato da AMS per fornire backup e istantanee per l'account.

AMS fornisce l'accesso AWS Backup tramite i tipi di modifica utilizzati per creare e gestire processi e piani di backup.

Come funziona la gestione della continuità

AMS utilizza AWS Backupper la gestione della continuità.

Quando si inizia a lavorare con AWS Backup AMS:

1. Esegui un backup su richiesta
2. Crea un piano di backup (opzionale, AMS fornisce piani di backup predefiniti)
3. Usa l'AMS predefinito come archivio di backup (opzionale)
4. Gestisci (esegui, perfeziona, elimina e così via) i tuoi piani di backup e i punti di ripristino

Piani di backup AMS

Un piano di backup è un'espressione di policy che definisce quando e come eseguire il backup delle risorse AWS supportate, come database RDS, volumi EBS, tabelle DynamoDB e file system EFS. Le politiche di pianificazione e conservazione sono gestite tramite piani di backup personalizzati, che è possibile creare utilizzando un tipo di modifica (CT) con AMS Advanced o utilizzando AMS Accelerate. AWS Backup Assegna risorse ai tuoi piani di backup utilizzando tag ed esegue AWS Backup automaticamente il backup e conserva i backup per le risorse assegnate in base al piano di backup definito. Puoi creare più piani di backup se disponi di carichi di lavoro con requisiti di backup differenti.

Un piano di backup può avere fino a sei regole di backup che definiscono, tra gli altri dettagli, una pianificazione e un periodo di conservazione. La pianificazione del backup determina quando viene AWS Backup avviato un processo di backup e con che frequenza viene creato un backup. È possibile scegliere una frequenza oraria, giornaliera, settimanale o mensile. L'impostazione dei giorni di eliminazione determina per quanti giorni l'istantanea viene archiviata prima di essere eliminata automaticamente.

> **Note**
>
> AMS Advanced: in caso di migrazione dal sistema di backup AMS legacy, AMS crea un piano di backup predefinito per la compatibilità con le versioni precedenti. La coppia chiave:valore in questo scenario è Backup:True. Per supportare la compatibilità con le versioni precedenti, il valore qui non fa distinzione tra maiuscole e minuscole, quindi Backup:True o Backup:true sono tutti tag validi. Tutte le altre coppie chiave:valore fanno distinzione tra maiuscole e minuscole.
>
> AWS Backup può operare a livello di volume EBS o a livello di EC2 istanza Amazon, ma non entrambe le operazioni contemporaneamente, poiché ciò può portare a una situazione di gara in cui i backup potrebbero entrare in conflitto.

Piani di backup predefiniti, landing zone multi-account

Durante la nuova RFC per la creazione dell'account, AMS garantisce l'esistenza di un piano di backup predefinito generale a livello di account per salvaguardare i carichi di lavoro. I valori per i campi obbligatori sono impostati di default, come illustrato nella sezione seguente:

Piano di backup AMS predefinito

default-backup-plan

Chiave TAG: `Backup`

Valore TAG: `True`

```
RuleForDailyBackups schedule expression: cron(30 23 ? * *) (a daily backup for 23:30
 UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(30 23 ? * 7 *) (a weekly backup for
 23:30 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(30 23 * ? *) (a monthly backup for
 23:30 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(30 23 1 1 ? *) (a yearly backup for
 23:30 UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Piano di backup AMS predefinito	Start Time	Retention
backup orario	N/D	N/D
backup giornaliero	ogni giorno alle 23:30 UTC	7 giorni
backup settimanale	settimanale alle 23:30 UTC, solo il sabato	4 settimane
backup mensile	mensilmente alle 23:30 UTC, il giorno 1 del mese	26 settimane
backup annuale	23:30 UTC, il giorno 1 del mese	2 anni

Piano di backup AMS predefinito avanzato

Questo piano è un modello di AWS Backup best practice per la protezione dagli attacchi ransomware. Implementa una strategia di backup giornaliera, settimanale, mensile e annuale. AWS Backup il backup continuo è abilitato con la massima conservazione (31 giorni) sulle risorse supportate.

ams-enhanced-default-backup-piano

Chiave TAG: `backup-orchestrator-enhanced`

Valore TAG: `true`

```
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
 UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForDailyBackups continuous backup: true
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
 02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
 UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Piano di backup AMS avanzato	Start Time	Retention
backup orario	N/D	N/D
backup giornaliero	ogni giorno 4:00 UTC	31 giorni
backup settimanale	sabato, 2:00 UTC	6 settimane
backup mensile	1° del mese, 2:00 UTC	26 settimane
backup annuale	1 gennaio, 2:00 UTC	2 anni

Piano di backup AMS sensibile ai dati

Questo piano è un modello per le migliori pratiche di AWS Backup per la protezione dagli attacchi ransomware per applicazioni sensibili ai dati. Implementa una strategia di backup oraria, giornaliera, settimanale, mensile e annuale. Il backup continuo di AWS Backup è abilitato con la conservazione massima (31 giorni) sulle risorse supportate.

ams-data-sensitive-backup-piano

Chiave TAG: `backup-orchestrator-data-sensitive`

Valore TAG: `true`

```
RuleForHourlyBackups schedule expression: cron(0 * ? * * *) (an hourly backup at the
 hour mark)
RuleForHourlyBackups delete after days: 7 days
RuleForDailyBackups schedule expression: cron(0 0 4 ? * * ) (a daily backup for 04:00
 UTC time)
RuleForDailyBackups delete after days: 31 days
RuleForWeeklyBackups schedule expression: cron(0 0 2 ? * 7) (a weekly backup for 02:00
 UTC time only on Saturday)
RuleForWeeklyBackups delete after weeks: 6 weeks
RuleForMonthlyBackups schedule expression: cron(0 2 1 * ? *) (a monthly backup for
 02:00 UTC time on day 1 of the month)
RuleForMonthlyBackups delete after weeks: 26 weeks
RuleForYearlyBackups schedule expression: cron(0 2 1 1 ? *) (a yearly backup for 02:00
 UTC time on day 1 of the month, only in January)
RuleForYearlyBackups delete after years: 2 years
```

Piano di backup AMS per dati sensibili ai dati	Start Time	Retention
backup orario	all'ora	7 giorni
backup giornaliero	ogni giorno 4:00 UTC	31 giorni
backup settimanale	sabato, 2:00 UTC	6 settimane
backup mensile	1° del mese, 2:00 UTC	26 settimane
backup annuale	1 gennaio, 2:00 UTC	2 anni

casseforti di backup AMS

AWS Backup organizza le istantanee in unità di archiviazione logiche chiamate casseforti.

È possibile controllare le notifiche di backup vault a livello di singolo vault utilizzando i tag. È possibile disattivare le notifiche per un vault specifico aggiungendo il tag `AMSNotificationOptOut` e impostando il valore su un vault specifico. `True` Per riprendere a ricevere le notifiche dal vault, rimuovi il tag.

Per visualizzare un elenco dei tuoi backup AMS, apri la console.AWS Backup Nel riquadro di navigazione, scegli Backup vault e seleziona uno degli archivi di backup AMS dalle seguenti tabelle. Nella sezione Backup, visualizza l'elenco di tutti i backup nel backup vault. Seleziona un backup da modificare, eliminare o ripristinare.

Vault per piani di backup AMS

Nome AMS Vault	Descrizione
ams-automated-backups	Questo vault riceve tutti i punti di ripristino utilizzati dal piano predefinito AWS Backup AMS Advanced. default-backup-plan
ams-automated-enhanced-backups	Questo vault riceve tutti i punti di ripristino utilizzati dal AWS Backup piano ams-enhan ced-default-backup di default avanzato di AMS Advanced.
ams-automated-data-sensitive-backup	Questo vault riceve tutti i punti di ripristino utilizzati dal piano -plan di AMS Advanced AWS Backup . ams-data-sensitive-backup
ams-manual-backups	Questa è la posizione predefinita per tutti i backup dei piani di backup di Start Backup Job RFC (ct-2hhud2lx01tq7), se non è definito alcun nome di vault.
ams-custom-backups	Questa è la posizione predefinita per le istantanee che AMS scatta prima di applicare le patch a un'istanza utilizzando Patch Orchestra

Nome AMS Vault	Descrizione
	tor o le attività di patch mensili. Queste vengono rimosse automaticamente in base alla politica predefinita di 60 giorni relativa al ciclo di vita delle patch di AMS.

Tipi di modifiche al backup AMS

AMS ne offre diversi CTs per creare e utilizzare piani di backup.

> **Important**
>
> Non modificate i piani di backup predefiniti di AMS poiché le modifiche potrebbero andare perse. Crea invece nuovi piani per le tue configurazioni personalizzate.

- Piano di backup: Crea
- Backup Job: Avvio
- Backup Job: Stop
- Punto di ripristino: Elimina
- DynamoDB | Creazione da Backup
- Volume EBS: creazione da backup
- Amazon Elastic File System (EFS): creazione da backup

Monitoraggio e reportistica dei backup con AMS

> **Important**
>
> Il monitoraggio e il reporting dei backup AMS sono disponibili solo nelle regioni supportate da AMS. Questi sono Stati Uniti orientali (Virginia), Stati Uniti occidentali (California settentrionale), Stati Uniti occidentali (Oregon), Stati Uniti orientali (Ohio), Canada (Centrale), Sud America (San Paolo), UE (Irlanda), UE (Francoforte), UE (Londra), UE (Parigi), Asia Pacifico (Mumbai), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Asia Pacifico (Asia Pacifico), Asia Pacifico (Sydney), Asia Pacifico (Mumbai), Asia Pacifico

(Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Asia Pacifico (Mumbai), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney), Asia Pacifico (Mumbai), Asia Pacifico (Seoul), Asia Pacifico (Singapore), Asia Pacifico (Sydney) Tokyo).

AMS genera report self-service giornalieri e report mensili sulla copertura delle risorse e sullo stato dei processi di backup. I report mensili sono condivisi in Monthly Business Reviews (MBRs). Per ulteriori informazioni sui report di backup giornalieri, consulta di backup giornaliero.

Gli esperti AMS monitorano tutte le attività di backup configurate utilizzando AWS Backup. In caso di errori di backup, AMS indaga sull'errore e comunica all'utente la causa principale e le opzioni di riparazione, se disponibili. Per evitare rumori di allarme, durante gli eventi che causano un numero elevato di errori di backup negli account, AMS formula una raccomandazione collettiva, tramite il CSDM, anziché notificarvi ogni singolo errore.

Tieni presente che AMS non monitora alcun backup configurato utilizzando la funzionalità di backup autonoma di un AWS servizio.

Risposta al disaster recovery

Oltre alle opzioni descritte nelle sezioni seguenti, è utile che tu sappia quali passaggi adottare per avviare un disaster recovery (DR) con AMS.

In caso di emergenza e devi avviare un ripristino, segui queste linee guida generali:

1. Apri un incidente ad alta priorità con la categoria Disponibilità. AMS aprirà un ponte per conferenze e inviterà il tuo team a partecipare.
2. Conosci l'elenco delle risorse che devi recuperare.
3. Conosci la landing zone (LZ) di destinazione in cui devi riprenderti (ad esempio, lo stesso account, una AZ diversa o un account diverso e una regione diversa).
4. Invia richieste di recupero per ogni risorsa nella landing zone di destinazione. Segui il piano di ripristino di emergenza esistente o consulta le opzioni nella sezione seguente (ad esempioProtezione da disastri per EC2 le istantanee EBS su AMS, oProtezione in caso di emergenza EC2 con Elastic Disaster Recovery su AMS).
5. Ripristina la funzionalità dell'applicazione e utilizza l'assistenza AMS per risolvere i problemi relativi all'infrastruttura.

AMS può aiutarvi a prepararvi per questo evento e a creare un piano di disaster recovery per la vostra organizzazione che risponda a queste domande. Per ulteriori dettagli, contattate il vostro cloud service delivery manager (CSDM) o il cloud architect (CA).

Pianificazione del disaster recovery

Il disaster recovery (DR) è un servizio fondamentale per la continuità e la conformità aziendale. AMS collabora con te per aiutarti a pianificare, implementare e mantenere la tua strategia di DR su AMS.

AMS landing zone (LZ), multi-account e single-account, fornisce componenti nativi, Multi-AZ e ad alta disponibilità per i componenti dell'infrastruttura AMS che soddisfano la maggior parte degli scenari di protezione dai disastri. Tuttavia, a seconda della copertura geografica della tua azienda, potresti aver bisogno di una protezione regionale. Per la disponibilità interregionale e il DR, è necessario un altro account AMS in una regione diversa (questo vale sia per la landing zone con più account che per la landing zone con account singolo).

AMS si allinea alle linee guida di AWS DR descritte in questo blog, Rapidly recovery mission-critical systems in a disaster, e supporta le seguenti quattro opzioni:

- Multisito (o ad alta disponibilità)
- Standby a caldo
- Luce pilota
- Backup e ripristino

Queste opzioni e il relativo supporto AMS sono descritti nelle seguenti sezioni.

Multisito o ad alta disponibilità (HA)

La soluzione HA è in genere fornita dalle funzionalità integrate dell'applicazione, come il clustering o la replica sincrona. Gli utenti vengono indirizzati sia a Prod che ai nodi. HA/DR Il DNS punta ai nodi direttamente o tramite un sistema di bilanciamento del carico elastico (ELB).

Il vostro architetto cloud AMS (CA) collaborerà con voi nell'ambito della vostra pianificazione Well-Architected-Review e del DR.

HA DR utilizza servizi e funzionalità applicativi e AWS nativi, come illustrato nel seguente grafico:

Il sito DR può essere uguale o diverso. Regione AWS

> **Note**
>
> Una regione diversa (interregionale) avrà un ambiente Active Directory diverso.

Fasi DR (failover): failover automatico, non sono necessarie operazioni manuali. In caso di guasto nella LZ principale, gli utenti verranno automaticamente reindirizzati al nodo. DR/HA Ciò è possibile grazie alla configurazione del DNS e dell'applicazione.

Metriche HA DR:

- Obiettivo del punto di ripristino (RPO): <5 min
- Obiettivo del tempo di ripristino e (RTO): <5 min
- Manutenzione: elevata (sono necessarie modifiche sincrone in entrambi gli ambienti, ad esempio configurazione dell'applicazione, applicazione di patch, SG o ALB, certificati e così via).
- Costo: alto

Warm standby

Il termine «warm standby» viene utilizzato per descrivere uno scenario di disaster recovery (DR) in cui una versione ridotta dell'ambiente è in esecuzione nel cloud.

La replica dei dati viene gestita dal livello dell'applicazione, in genere in modo asincrono, su un'istanza online, mentre le altre istanze (ad esempio, il livello Applicazione e Web) potrebbero essere disattivate per ridurre i costi. Gli utenti vengono indirizzati solo al sito di produzione. È possibile che anche altre AWS risorse, come Elastic Load Balancer (ELB), siano preinstallate nel sito DR.

Il vostro AMS Cloud Architect (CA) collaborerà con voi nell'ambito della vostra Well-Architected-Review pianificazione e del DR.

Warm Standby DR utilizza servizi e funzionalità applicativi e AWS nativi, come illustrato nel seguente grafico:

Il sito DR può essere uguale o diverso. Regione AWS

> **Note**
>
> Una regione diversa (interregionale) avrà un ambiente Active Directory diverso.

Fasi di DR (failover):

1. Blocca la replica dei dati e rendi principale l'istanza di dati nel sito DR
2. Aggiorna la configurazione dell'applicazione come richiesto (nuovo IP, nome del server e così via)
3. Reindirizza il DNS al sito DR (ELB)
4. Dipendenze AD, se necessario (account di servizio, SPNs GPOs, e così via)

Metriche HA DR:

- Recovery Point Objective (RPO): < 1 ora
- Recovery Time Objective e (RTO): <1 ora (dipende dal numero di istanze e dall'orchestrazione)
- Manutenzione: elevata (sono necessarie modifiche sincrone in entrambi gli ambienti, ad esempio configurazione delle applicazioni, applicazione di patch, gruppi di sicurezza (SG) o Application Load Balancer (ALB), certificati e così via).
- Costo: medio

Pilot light

In questo approccio di disaster recovery (DR), replicate parte del vostro ambiente Prod per un set limitato di servizi di base. Una piccola parte dell'infrastruttura è sempre in funzione e sincronizza contemporaneamente dati mutabili (come database o documenti), mentre altre parti dell'infrastruttura vengono disattivate e utilizzate solo durante i test. A differenza di un approccio di backup e ripristino, è necessario assicurarsi che gli elementi principali più importanti siano già configurati e funzionanti nella landing zone del DR (la luce pilota).

Il vostro AMS Cloud Architect collaborerà con voi nell'ambito della vostra pianificazione Well-Architected-Review e del DR.

Pilot Light DR utilizza servizi e funzionalità applicativi e AWS nativi, come illustrato nel seguente grafico:

Il sito DR può essere uguale o diverso. Regione AWS

> **Note**
>
> Una regione diversa (interregionale) avrà un ambiente Active Directory diverso.

Fasi di DR (failover):

1. Blocca la replica dei dati e rendi principale l'istanza di dati nel sito DR
2. Avvia le istanze e l'infrastruttura disattivate
3. Aggiorna la configurazione dell'applicazione come richiesto (nuovo IP, nome del server e così via)
4. Aggiungete le istanze all'ELB come richiesto
5. Reindirizza il DNS al sito DR (ELB)
6. Dipendenze AD, se necessario (account di servizio, SPNs GPOs, e così via)

Metriche Pilot Light DR:

- Recovery Point Objective (RPO): < 1 ora
- Obiettivo del tempo di ripristino e (RTO): ~1 ora (dipende dal numero di istanze e dall'orchestrazione)
- Manutenzione: media
- Costo: medio

Backup e ripristino

Questo approccio di disaster recovery (DR) semplice e a basso costo esegue il backup dei dati e delle applicazioni ovunque si trovino nella landing zone del DR per utilizzarli durante il ripristino da un disastro.

Il tuo AMS Cloud Architect collabora con te nell'ambito della pianificazione di Backup e DR.

Backup and Restore DR utilizza strumenti e processi automatizzati AMS, come illustrato nel seguente grafico:

È possibile utilizzare due metodi di backup e replica:

- Snapshot EBS (Recovery Point Objective (RPO) > 1 ora), nota come «EBS»
- AWS Elastic Disaster Recovery (Recovery Point Objective (RPO) ~ 0,25 ore), noto come «DRS»

Il sito DR può trovarsi nello stesso sito o in un altro. Regione AWS

> **Note**
>
> Una regione diversa (interregionale) ha un ambiente Active Directory diverso.

Fasi di DR (failover):

1. Ripristina le istanze dalle istantanee (processo in due fasi con prima istanza placeholder)
2. Aggiorna la configurazione dell'applicazione (nuovo IP, nome del server e così via)
3. Configura altre infrastrutture come richiesto (SG, ELB e così via)
4. Reindirizza il DNS al sito DR (ELB)
5. Se necessario, aggiorna o ripristina le dipendenze AD (account di servizio, nomi principali di servizio (SPNs), oggetti delle policy di gruppo (GPOs) e così via)

Metriche di backup e ripristino del disaster recovery:

- Recovery Point Objective (RPO): >1 ora o ~0,25 ore (dipende dalla soluzione selezionata: EBS o DRE)
- Recovery Time Objective e (RTO): ~1 ora (dipende dal numero di istanze e dall'orchestrazione)
- Manutenzione: elevata (sono necessarie modifiche sincrone in entrambi gli ambienti, come la configurazione delle applicazioni, l'applicazione di patch, i gruppi di sicurezza o i sistemi di bilanciamento del carico delle applicazioni, i certificati e così via.
- Costo: medio

Protezione da disastri per EC2 le istantanee EBS su AMS

Prerequisiti:

- AMS Prod Landing Zone (fonte)
- Zona di atterraggio AMS DR (destinazione DR)

- Le istantanee EBS sono abilitate per le EC2 istanze ()AWS Backup

Soluzione di replica delle istantanee:

- Cross AZ: non applicabile: le istantanee EBS sono progettate per essere altamente disponibili nella regione
- Interregione: AWS Backup

Il diagramma seguente rappresenta il processo di EC2 ripristino dalle istantanee EBS su AMS:

EC2 Fasi di DR su AMS:

1. Crea una RFC per condividere le istantanee EBS con l'account di destinazione (necessario per il DR interregionale).

   : Gestione, Advanced Stack Components, EBS Snapshot, Share
2. Crea uno stack AMS segnaposto nella EC2 sottorete di destinazione (sottorete del sito DR). Si consiglia di utilizzare CFN ingestion per creare lo stack in modo che il cliente possa combinare i passaggi di assegnazione dei gruppi di sicurezza e altri (come l'aggiunta dell'istanza a un ELB) nello stesso stack.

   Tipo di modifica: Deployment, Ingestion, Stack from Template, Create CloudFormation
3. Genera un RFC per eseguire EC2 il ripristino del volume dello stack.

   Tipo di modifica: gestione, componenti dello stack avanzato, stack di EC2 istanze, volumi di ripristino.

   Il CT ripristina i volumi dalle istantanee condivise nel passaggio 1 e si collega all'istanza placeholder creata nel passaggio 2.

Funzionalità Volume Restore CT:

- Chiudi l'istanza placeholder
- Ripristina i volumi dalle istantanee
- Sostituisci i volumi
- Avvia l'istanza

- Abbandona il vecchio dominio
- Modifica del nome host
- Riavviare. Gli script di bootstrap AMS aggiungono l'istanza al dominio di destinazione (DR) all'avvio

Ingresso CT per il ripristino del volume:

- InstanceId (ID dell'istanza segnaposto)
- RootDeviceSnapshotId, lo snapshot EBS per il volume root ripristinato
- KMSKeyId, l'identificatore di chiave KMS, o ARN, per crittografare tutti i volumi ripristinati sull'istanza EC2
- DeviceNames, fino a 25 (opzionale)
- SnapshotIds, fino a 25 (opzionale). Elenco di istantanee dei volumi da ripristinare

Protezione in caso di emergenza EC2 con Elastic Disaster Recovery su AMS

Prerequisiti:

- AMS Prod Landing Zone (fonte)
- Zona di atterraggio AMS DR (destinazione DR)
- Devi prima inizializzare il servizio Elastic Disaster Recovery per tutto Regioni AWS ciò in cui intendi utilizzarlo.

Crea un ruolo IAM nella tua landing zone (LZ) DR per l'accesso alla console Elastic Disaster Recovery.

- Importante: un documento SSM viene creato come azione post-lancio all'interno di DRS. Questa azione deve essere abilitata su tutti i server nelle PostLaunch impostazioni.
- l'istanza di destinazione (placeholder) deve avere una chiave tag: "AWSDRS«, value:"»AllowLaunchingIntoThisInstance. L'istanza placeholder deve essere interrotta. Altrimenti, AMS non può selezionare l'istanza placeholder nelle impostazioni di avvio e Elastic Disaster Recovery non può eseguire il ripristino sull'istanza placeholder.

Per un diagramma del processo di configurazione e ripristino di Elastic Disaster Recovery EC2 su AMS, consulta l'architettura generale AWS Elastic Disaster Recovery (AWSDRS).

EC2 Fasi di DR con Elastic Disaster Recovery su AMS:

1. Crea uno stack EC2 AMS segnaposto nella sottorete di destinazione (sottorete del sito DR) con i tag appropriati. Per ulteriori informazioni, consulta la sezione precedente. Ti consigliamo di utilizzare CFN ingestion per creare lo stack in quanto puoi combinare i passaggi di assegnazione dei gruppi di sicurezza e di etichettare l'istanza, il volume EBS e altro (ad esempio aggiungere l'istanza a un ELB) nello stesso stack.

   Tipo di modifica: Deployment, Ingestion, Stack from Template, Create CloudFormation

2. Arresta l'istanza placeholder.

   Tipo di modifica: gestione, componenti dello stack avanzati, istanza, EC2 Stop

3. Se non l'hai fatto nel passaggio 1, contrassegna l'istanza placeholder e il relativo volume EBS con la chiave: "AWSDRS«, value:"». AllowLaunchingIntoThisInstance

   Tipo di modifica: gestione, componenti dello stack avanzati, tag, aggiornamento.

4. Utilizza l'istanza placeholder del passaggio 1 come destinazione in Launch into instance ID, DRS Launch Settings per il server di origine. Avvia l'esercitazione di ripristino dell'istanza dalla console Elastic Disaster Recovery per il server di origine.

   > **Note**
   >
   > I volumi delle istanze segnaposto vengono conservati nell'account. Per eliminare questi volumi, invia un Management | Advanced stack components | EBS Volume | Delete change type (ct-3e3h8u0sp5z80) al termine dell'operazione di disaster recovery.

Flusso di lavoro di ripristino Elastic Disaster Recovery:

- L'istanza di destinazione (segnaposto) deve trovarsi nello stato interrotto
- Scambia i volumi ed elimina il volume radice di origine (segnaposto)
- Avviate l'istanza
- Esegui le azioni successive al lancio per completare i seguenti elementi:
  - Attiva l'agente SSM.
  - Scambia i volumi ed elimina il volume radice di origine (segnaposto).
  - Avviate l'istanza

- Esegui il documento PostLaunchScript SSM. Questo documento fa quanto segue:
  1. Lascia il vecchio dominio.
  2. Cambia il nome host.
  3. Riavviare. Gli script di bootstrap AMS uniscono l'istanza al dominio di destinazione (DR) durante l'avvio.

Gestione delle patch in AMS

Argomenti

In AMS, la gestione delle patch è un servizio che ti aiuta a mantenere gli aggiornamenti dei fornitori del sistema operativo sulle tue istanze Amazon Elastic Compute Cloud EC2 (Amazon). Hai la libertà di personalizzare la frequenza e il processo di applicazione delle patch alle tue EC2 istanze Amazon.

Puoi configurare la gestione delle patch durante l'onboarding e aggiornarla utilizzando il processo RFC. Gli stack creati utilizzando il sistema di gestione delle modifiche e un modello compatibile con le patch (per Amazon, gruppo Auto EC2 Scaling, stack HA a uno o due livelli) vengono sottoscritti automaticamente alla gestione delle patch.

AMS fornisce una funzionalità, Patch Orchestrator: patching basato su tag, per la configurazione delle patch.

Per le definizioni dei termini relativi all'applicazione delle patch, vedere. Termini chiave AMS

Important

- Gli stack o le istanze che lo costituiscono non possono disattivare la gestione delle patch, se il modello AMS da cui viene creato lo stack è compatibile con la gestione delle patch. Attualmente, l'applicazione delle patch è compatibile con i seguenti modelli di stack:
  - Amazon EC2 stack | Create e Amazon EC2 stack | Create (con volumi aggiuntivi)
  - EC2 Istanza Amazon lanciata con CloudFormation ingest
  - Gruppo Auto Scaling | Crea (EC2 le istanze Amazon del gruppo sono dotate di patch)
  - Stack a un livello ad alta disponibilità | Crea e stack a due livelli ad alta disponibilità | Crea
- Se è in corso un incidente che interessa uno stack, gli operatori AMS possono riprogrammare o annullare l'applicazione delle patch programmate.

- Per impostazione predefinita, tutte le istanze all'interno di un particolare stack compatibile con le patch vengono applicate le patch sul posto. Per applicare una patch ai gruppi di Auto Scaling con un sostituto di Amazon Machine Image (AMI) utilizzando l' latest/patched AMI AMS, invia una richiesta di servizio. AMIs Gli aggiornamenti vengono condivisi con gli account ogni mese.

Important

È possibile specificare repository di patch alternativi per i nodi gestiti. Sebbene AMS implementi le configurazioni di patch richieste, l'utente è responsabile della selezione e della convalida della sicurezza dei repository scelti. È inoltre necessario accettare tutti i rischi derivanti dall'utilizzo di questi archivi, come i rischi della catena di approvvigionamento.
Di seguito sono riportate le migliori pratiche per la sicurezza del processo di gestione delle patch:

- Utilizzate solo fonti di repository affidabili e verificate
- L'impostazione predefinita è costituita dagli archivi standard dei fornitori di sistemi operativi, quando possibile
- Controlla regolarmente le configurazioni dei repository personalizzati

Tip

AMS consiglia di abilitare i backup per le istanze che dispongono di applicazioni o servizi preziosi. Per informazioni sull'abilitazione dei backup, consulta. Gestione della continuità in AMS Advanced

AMS Patch Orchestrator: un modello di patching basato su tag

Se hai effettuato l'onboarding del nuovo modello di patching basato su tag AMS Patch Orchestrator, puoi utilizzare i tag per applicare la configurazione della patch a un set preciso di risorse, chiamato gruppo di patch, che vanno da un'istanza a tutte le tue istanze. Per informazioni sui tag AMS, consulta Uso dei tag. Le istruzioni sulla configurazione dei tag Patch Orchestrator sono fornite nella sezione seguente.

Le patch vengono installate durante le finestre di patch definite con SSM Patch Window | Create. Ogni finestra di patch è una finestra di manutenzione di AWS Systems Manager che viene eseguita secondo una pianificazione a scelta, ha una durata configurata e si applica a un gruppo di patch. Le istanze che non fanno parte di una finestra di patch esplicita vengono applicate le patch durante la finestra di manutenzione predefinita che definisci quando effettui l'onboarding su Patch Orchestrator.

> **Important**
>
> Se è pianificata l'esecuzione di più finestre di manutenzione delle patch contemporaneamente, è necessario che vengano elaborate meno di 1001 istanze alla volta. Si tratta di una limitazione di AWS Systems Manager. AMS consiglia almeno un'ora ogni cinquanta istanze.

Per impostazione predefinita, tutte le patch del sistema operativo (OS) fornite dal fornitore vengono installate durante una finestra di manutenzione o una patch su richiesta. Questa è chiamata la linea di base delle patch predefinita. Se desideri limitare le patch installate, puoi definire una linea di base di patch personalizzata usando una delle patch baseline create CTs (per OSes), vedi la sottocategoria Patching. Ad esempio, è possibile utilizzare una linea di base di patch personalizzata in modo che vengano installati solo gli aggiornamenti di sicurezza critici e importanti per uno o più gruppi di patch.

Dopo l'installazione delle patch su un'istanza, l'istanza viene riavviata. Le notifiche di patch vengono inviate prima e dopo l'applicazione delle patch e un promemoria aggiuntivo viene inviato entro 96 ore prima dell'avvio pianificato. Inoltre, AMS applica gli aggiornamenti agli strumenti di gestione dell'infrastruttura (come l'agente AWS SSM) durante la finestra di manutenzione selezionata.

> **Important**
>
> AMS sta rendendo obsoleta la segnalazione mensile di conformità delle patch delle istanze con patch mancanti e non invierà report mensili. Questa modifica è stata apportata alla luce dei report operativi self-service rilasciati di recente, che si aggiornano ogni 24 ore e sono disponibili su richiesta e forniscono i dati più recenti e granulari. Per ulteriori informazioni sui report, consulta Reporting self-service. Per ulteriori informazioni sui report, consultaReport self-service.

Per ulteriori informazioni sulle notifiche, vedereNotifiche sulle patch.

Utilizzo di Patch Orchestrator

Abilita AMS Patch Orchestrator per il tuo account inviando una richiesta di servizio che include i seguenti dettagli:

- Categoria: Altro
- Oggetto: Onboard to Patch Orchestrator
- E-mail CC: gli indirizzi e-mail CC ricevono notifiche quando lo stato di questa RFC di onboarding cambia
- Dettagli: incolla le seguenti informazioni nell'e-mail e fornisci i tuoi valori. Tieni presente che ThirdTagKey è facoltativo. Per consigli ed esempi, consulta la tabella seguente.

```
Default maintenance window Schedule:
Default Maintenance Window Schedule TimeZone:
Default Maintenance Window Duration:
Default Maintenance Window Cutoff:
Default Patch Backup Retention In Days:
Default Maintenance Window Notification Emails:
First Tag Key:
Second Tag Key:
Third Tag Key:
```

La tabella seguente descrive il formato e i consigli per i valori forniti.

Configurazioni di patching basate su tag di Patch Orchestrator

Nome del parametro	Informazioni	Raccomandazione o esempio
Pianificazione predefinita della finestra di manutenzione	La pianificazione della finestra di manutenzione predefinita sotto forma di espressione cron o rate. Ad esempio: • `cron(0 3 ? * 6L *)`: 03:00 l'ultimo venerdì di ogni mese • `rate(7 days)`: Ogni sette giorni	Ti consigliamo di far funzionar e la finestra almeno una volta al mese in un giorno feriale costante.

Nome del parametro	Informazioni	Raccomandazione o esempio
	Per ulteriori informazioni sulla creazione di espressioni cron e collegamenti alle risorse relative alle espressioni cron e rate, consulta Cron and rate expression for maintenance windows.	
Fuso orario di pianificazione della finestra di manutenzione predefinita	Il fuso orario su cui viene eseguita la finestra di manutenzione predefinita si basa sul formato Internet Assigned Numbers Authority (IANA).	Ad esempio: • America/Los_Angeles • etc/UTC
Durata predefinita della finestra di manutenzione	La durata della finestra di manutenzione predefinita, in ore.	Almeno 1 ora ogni 50 istanze, più 2 ore per l'interruzione.
Interruzione predefinita della finestra di manutenzione	Il numero di ore prima della fine della finestra di manutenzione predefinita in cui non viene avviato alcun nuovo comando di applicazione delle patch. Questo intervallo serve per consentire il completamento dell'applicazione delle patch prima della fine della finestra.	Almeno 2 ore.
Conservazione predefinita del backup delle patch in giorni (opzionale)	L'intervallo di tempo predefinito, espresso in giorni, per conservare i punti di ripristino EBS creati prima dell'applicazione delle patch alle istanze.	Ti consigliamo di mantenere il valore predefinito, che è 60.

Nome del parametro	Informazioni	Raccomandazione o esempio
Email di notifica della finestra di manutenzione predefinita	Da uno a cinque indirizzi e-mail o liste di distribuzione per ricevere notifiche sullo stato di applicazione delle patch nella finestra di manutenzione predefinita.	Si consiglia di utilizzare le liste di distribuzione di gruppo anziché le singole e-mail.
First Tag Key	La prima chiave di tag da utilizzare per creare i valori dei tag del Patch Group.	Ad esempio,. AppId Specifica te null se avete già definito i vostri gruppi di patch con un tag Patch Group.
Seconda chiave del tag	La seconda chiave di tag da utilizzare per creare i valori dei tag del Patch Group.	Ad esempio, Environment. Specificate null se avete già definito i vostri gruppi di patch con un tag Patch Group.
Terza chiave del tag (opzionale)	La terza chiave di tag opzionale da utilizzare per creare i valori dei tag del Patch Group.	Ad esempio, Group.

Dopo aver effettuato l'onboarding al nuovo modello di servizio di patching Patch Orchestrator, tutte le istanze con tag appropriati presenti nel tuo account appartengono a un gruppo di patch con un tag Patch Group. Patch Orchestrator utilizza il tag Patch Group esistente o un tag creato da AMS composto dai due o tre valori di tag concatenati specificati durante l'onboarding di Patch Orchestrator. Ad *`Tag Value 1`* esempio*`Tag Value 2`*, *`Tag Value 3`* {} - {} - {}. AMS aggiorna questi tag AMS-Applied Patch Group ogni 12 ore. Se necessario, puoi aggiornare i valori dei tag del Patch Group con i tipi di modifica Tag | Update (Review Required) o Tag | Update (Review Required).

Ad esempio, se la tua EC2 istanza Amazon ha le seguenti coppie di tag chiave:valore:

- `AppId:MyApplication`
- `Environment:Production`
- `Group:1`

Durante l'onboarding hai specificato le seguenti chiavi di tag:

- `First Tag Key = AppId`
- `Second Tag Key = Environment`
- `Third Tag Key = Group`

AMS crea il seguente tag Patch Group e lo applica alle tue istanze:. `Patch Group:MyApplication-Production-1`

> **Note**
>
> Gli avvisi di errore delle patch non vengono creati per le istanze con sistemi operativi non supportati o che vengono interrotte durante la finestra di manutenzione.

Prerequisiti di Patch Orchestrator

Il flusso di lavoro di Patch Orchestrator si rivolge EC2 alle istanze Amazon a cui è stata applicata la patch dall'ultima versione di System Manager Automation Document:. AWSManagedServices-PatchInstanceFromMaintenanceWindow

Come parte del flusso di lavoro documentale, il documento di comando run «AWS-RunPatchBaseline" viene eseguito su ciascuna delle EC2 istanze Amazon dei membri del gruppo di patch. Per ulteriori informazioni, consulta Informazioni sul documento SSM AWS- RunPatchBaseline.

Requisiti:

- EC2 Istanza Amazon distribuita da Amazon Machine Image (AMI) fornita da AMS o su un'AMI tramite il CT «Stack from migration partner migrated instance» (ct-257p9zjk14ija).
- Connessione Internet in uscita abilitata. Per firewall/proxy le soluzioni, il requisito è consentire gli endpoint di mirroring del repository and/or Linux di Windows Update, le impostazioni proxy di AWS System Manager e la configurazione del proxy di metadati. Per ulteriori informazioni, consulta Configurazione dell'agente SSM per l'utilizzo di un proxy e Utilizzo di un proxy HTTP
- Ruolo IAM corrispondente all'accesso minimo permissivo per il servizio SSM del ruolo IAM. `customer-mc-ec2-instance-profile`
- Consigliamo 10 GB di spazio disponibile nella partizione root. Per il sistema operativo Linux, almeno 2 GB disponibili nella `/var` partizione.

- Autorità di certificazione funzionante e valida per il download degli aggiornamenti.
- Windows Server Update Services (WSUS) - Registro che include, a titolo esemplificativo ma non esaustivo: DisableWindowsUpdateAccess, NoWindowsUpdate; Gli aggiornamenti automatici non devono compromettere il funzionamento del processo di Windows Update.

Convalida:

- Per le istanze del sistema operativo Linux che utilizzano yum package manager, è possibile convalidare la disponibilità degli aggiornamenti eseguendo `#yum check-update`
- Per Linux OS RedHat 5.7 e versioni successive, 6.1 e versioni successive e 7.0 e versioni successive; EC2 istanze Amazon migrate al tuo account AMS tramite il CT «Stack from migration partner migrated instance» (ct-257p9zjk14ija), devi convalidare lo stato del gestore delle sottoscrizioni per aggiornare le prestazioni.
- Sul sistema operativo Windows, abilita Windows Server Update Services (WSUS). Nessuna politica locale dovrebbe bloccare la capacità di WSUS di scansionare o installare gli aggiornamenti. Una volta effettuato l'accesso come amministratore, è possibile convalidarlo eseguendo una scansione degli aggiornamenti disponibili dalla console del servizio Windows Update. Le versioni del sistema operativo Windows Server, tra cui 2012R2, 2016 e 2019, dispongono di impostazioni Windows Update predefinite per il download e l'installazione. È possibile configurare le impostazioni desiderate prima della scansione. Nelle versioni successive del sistema operativo, questa operazione può innescare l'installazione; configurate prima il comportamento desiderato.
- Richiedi la convalida al team AMS Operations inviando una richiesta di servizio: "Documento di AWSManagedServices-CheckPatchingPrerequisites automazione da eseguire su un' EC2 istanza Amazon per la valutazione della preparazione delle patch».

> **Note**
>
> Gli avvisi di errore delle patch non vengono creati per le istanze con sistemi operativi non supportati o che vengono interrotte durante la finestra di manutenzione.

Finestre di patch

Le istanze di uno specifico gruppo di patch vengono corrette durante una o più finestre di patch. Le finestre di patch vengono eseguite secondo una pianificazione definita come espressione cron o rate e hanno una durata configurabile in modo da mantenere le interruzioni legate all'applicazione

delle patch entro un intervallo di tempo prescelto. AMS consiglia di creare più finestre di patch che coprano collettivamente tutte le istanze, in modo che corrispondano alle routine di patching specifiche dell'organizzazione e di utilizzare la finestra di manutenzione predefinita come riserva. Le finestre di patch vengono create con il tipo di modifica RFC Deployment | Patching | SSM patch window | Create (ct-0el2j07llrxs7). Tutte le istanze che non fanno parte di una finestra di patch vengono applicate le patch durante la finestra di manutenzione predefinita creata durante l'onboarding.

Normalmente, non è necessario aggiornare una finestra di patch per includere nuove istanze. In genere, ciò viene fatto modificando i tag delle istanze. Ad esempio, considerate la seguente sequenza di eventi:

1. Due istanze sono contrassegnate con `AppId:MyApplicationEnvironment:Production`,`Group:1`.

   Ciò produce un tag su queste istanze, supponendo che First Tag Key = AppId, Second Tag Key = Environment, Third Tag Key = Group e venga creata una finestra di patch per il gruppo di patch MyApplication -Production-1.
2. Vengono create altre tre istanze e contrassegnate con,. `AppId:MyApplication Environment:Production Group:1`

   Questo produce un tag per Patch Group: MyApplication -Production-1.

Non è necessaria alcuna modifica alla finestra della patch perché raccoglie tutte e cinque le istanze al momento della successiva esecuzione pianificata.

Per una discussione più dettagliata e una procedura dettagliata sull'utilizzo di questo tipo di modifica, vedi SSM Patch Window | Create.

Notifiche sulle patch

> **Important**
>
> A partire dal 1° febbraio 2025, i clienti AMS non riceveranno più notifiche per le finestre vuote di manutenzione delle patch nei loro account gestiti.

Gli indirizzi e-mail sottoscritti (fino a cinque) ricevono un'e-mail simile alla seguente appena prima dell'inizio della finestra di manutenzione della patch:

```
Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME was started at:
 2020-02-21T12:02:18.196Z.
Details:
    Maintenance Window AccountId:   YOUR_ACCOUNT_ID
    Maintenance Window Region:      YOUR_ACCOUNT_REGION
    Maintenance Window Id:          THE_MAINTENANCE_WINDOW_ID
    Maintenance Window Name:        THE_MAINTENANCE_WINDOW_NAME
    Maintenance Window Description: MaintenanceWindow for patching patch
 Group PATCH_GROUP_NAME
    Maintenance Window Patch Group: PATCH_GROUP_NAME
    Maintenance Window ExecutionId: THE_EXECUTION_ID
Targets:
    InstanceId           InstanceName        StackId
    -------------------  --------------      ----------------------
    THE_INSTANCE_ID      THE_INSTANCE_NAME   THE_STACK_NAME

A follow-up message with a detailed report is sent as soon as the maintenance window is
 over.

Please raise a service request if you have any inquires about AMS Patch Orchestrator by
 following this URL:
https://console.aws.amazon.com/managedservices/servicerequest/new

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team
```

Al termine dell'attività della patch, gli indirizzi e-mail sottoscritti ricevono un'e-mail simile alla seguente:

```
Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME ended at:
 2020-02-21T12:03:20.058Z, with status: SUCCESS.
Details:
    Maintenance Window AccountId:   YOUR_ACCOUNT_ID
    Maintenance Window Region:      YOUR_ACCOUNT_REGION
    Maintenance Window Id:          THE_MAINTENANCE_WINDOW_ID
    Maintenance Window Name:        THE_MAINTENANCE_WINDOW_NAME
    Maintenance Window Description: MaintenanceWindow for patching patch
 Group PATCH_GROUP_NAME
```

```
    Maintenance Window Patch Group: PATCH_GROUP_NAME
    Maintenance Window ExecutionId: THE_EXECUTION_ID
Targets:
    RfcId                        InstanceId        InstanceName          StackId
       Status
    -----------------------  -------------------  --------------
 -----------------------  --------
    THE_RFC_ID        THE_INSTANCE_ID     THE_INSTANCE_NAME THE_STACK_NAME
  STATUS

You can view the current Patch Compliance of your Amazon EC2 Instances by following
 this URL:
https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

Please raise an Incident if an issue is impacting one of your production applications
 by following this URL:
https://console.aws.amazon.com/managedservices/incident/new

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team
```

Ogni 96 ore il sistema di patching AMS identifica tutte le prossime finestre di manutenzione gestita dalle patch entro tali 96 ore e invia una notifica di promemoria a tutti gli indirizzi e-mail sottoscritti che rientrano in tale periodo di 96 ore. Questo potrebbe avvenire solo un'ora prima della finestra o le 96 ore complete. Ad esempio:

```
Dear Customer,
The AMS Patch Maintenance Window THE_MAINTENANCE_WINDOW_NAME will start at:
 2020-05-06T16:35:36.523Z.
Details:
    Maintenance Window AccountId:   YOUR_ACCOUNT_ID
    Maintenance Window Region:      YOUR_ACCOUNT_REGION
    Maintenance Window Id:          THE_MAINTENANCE_WINDOW_ID
    Maintenance Window Name:        THE_MAINTENANCE_WINDOW_NAME
    Maintenance Window Description: MaintenanceWindow for patching patch
 Group PATCH_GROUP_NAME
    Maintenance Window Patch Group: PATCH_GROUP_NAME
    Maintenance Window Next Start Time: 2020-05-06T16:35:36.523Z
    Maintenance Window Schedule:        rate(24 hours)
    Maintenance Window Timezone:        THE_TIMEZONE
```

```
At this time, these are the instances in the "PATCH_GROUP_NAME" Patch Group:
    InstanceId           InstanceName    StackId                 InstanceState

-------------------------------------------------------------------------------------------

    THE_INSTANCE_ID      THE_INSTANCE_NAME   THE_STACK_NAME  running/stopped
    THE_INSTANCE_ID      THE_INSTANCE_NAME   THE_STACK_NAME  running/stopped
    THE_INSTANCE_ID      THE_INSTANCE_NAME   THE_STACK_NAME  running/stopped

A notification message is sent as soon as the maintenance window starts.

You can view the current Patch Compliance of your Amazon EC2 Instances by following
 this URL:
https://console.aws.amazon.com/systems-manager/compliance?region=YOUR_ACCOUNT_REGION

If you would like to disable this maintenance window or you have inquires about the AMS
 Patch Orchestrator click on the following URL:
https://console.aws.amazon.com/managedservices/servicerequest/new

If you would like to delete this maintenance window, you can run the CT with id
 "ct-0q0bic0ywqk6c" against the stack id "stack-rctyznutkyj4tkkzq".

Kind Regards,

Amazon Web Services
Amazon Managed Services
Patch Team
```

Patch di base

Per impostazione predefinita, tutte le patch fornite dal fornitore del sistema operativo (OS) vengono installate utilizzando la patch di base di default di AMS. Se desideri limitare le patch installate, puoi facoltativamente creare una patch di base utilizzando il tipo di modifica RFC Deployment | Patching | SSM Patch baseline | Create (l'ID CT varia in base al sistema operativo). *OS*

Per informazioni sull'utilizzo di questi tipi di modifiche, consulta la sottocategoria Patching.

Tag riservati di Patch Orchestrator

Patch Orchestrator genera anche i seguenti tag che non possono essere modificati:

- AMSPatchGruppo: questo tag viene utilizzato per la generazione del valore dei tag Patch Group. Non dovresti modificare il AMSPatch gruppo. È possibile modificare il tag «Patch Group» se

si desidera utilizzare un valore «Patch Group» personalizzato. Patch Orchestrator continua a generare un valore per AMSPatch Group in base alle chiavi di tag fornite durante l'onboarding, ma non modificherà il valore del tag «Patch Group» se è stato impostato su un valore personalizzato dall'utente. Per smettere di usare un valore personalizzato «Patch Group», puoi impostare il valore di «Patch Group» in modo che corrisponda al valore del tag Group. AMSPatch

- AMSDefaultPatchGroup— Questo tag indica se un'istanza fa parte della finestra di manutenzione predefinita, con un valore di True o False. Se il Patch Group di un'istanza non è assegnato a una finestra di manutenzione, questo valore è impostato su True.

Patch su richiesta

AMS ha un tipo di modifica che si adatta alla linea di base della patch utilizzata, per consentirvi di eseguire una patch su istanze su richiesta. Questa può essere la linea di base predefinita impostata all'atto dell'imbarco o la linea di base della patch Patch Orchestrator Systems Manager impostata con il tipo di modifica Patch Baseline (l'ID CT varia in base al sistema operativo).

È possibile utilizzare il tipo di modifica delle patch su richiesta con o senza Patch Orchestrator.

Per informazioni sull'utilizzo di questo tipo di modifica, vedere On Demand Patching | Run.

> **Note**
>
> Non è possibile utilizzare istanze che fanno parte di un gruppo Auto Scaling in un tipo di modifica con patch su richiesta.

Patch standard AMS

AMS supporta i clienti esistenti utilizzando il modello di patching standard AMS, ma questo modello non è disponibile per i nuovi clienti e verrà ritirato a favore di AMS Patch Orchestrator.

I contenuti tipici delle patch per l'applicazione delle patch standard di AMS includono gli aggiornamenti dei fornitori per i sistemi operativi supportati e il software preinstallato con i sistemi operativi supportati (ad esempio, IIS e Apache Server).

Durante l'onboarding di AMS, si specificano i requisiti di applicazione delle patch, le policy, la frequenza e le finestre di patch preferite. Queste configurazioni consentono di evitare di mettere tutte

le applicazioni offline contemporaneamente per applicare le patch all'infrastruttura, in modo da poter controllare a quale infrastruttura viene applicata la patch e quando.

> **Note**
>
> Il processo di applicazione delle patch descritto in questo argomento si applica solo agli stack. L'infrastruttura AMS viene patchata durante un processo separato. La AWS Managed Services Maintenance Window (o Maintenance Window) esegue attività di manutenzione per AWS Managed Services (AMS) e si svolge 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. È possibile configurare la finestra delle patch AMS al momento dell'onboarding oppure approvare o rifiutare la notifica mensile del servizio di patch.

AMS analizza regolarmente EC2 le istanze Amazon gestite alla ricerca di aggiornamenti disponibili tramite la funzionalità di aggiornamento del sistema operativo. Forniamo inoltre aggiornamenti regolari alla base AMS Amazon Machine Images (AMIs) supportata nel nostro ambiente.

Dopo la convalida, le versioni AMS AMI vengono condivise con tutti gli account AMS. Puoi visualizzare le versioni AWS AMI disponibili utilizzando la chiamata EC2 API DescribeImagesAmazon o la EC2 console Amazon. Per trovare gli AMS disponibili AMIs, consultaTrova AMI IDs, AMS.

AMS esegue pianificazioni di patch ad hoc solo quando richiesto dall'utente. In precedenza AMS inviava una notifica; attualmente non viene inviata alcuna notifica.

> **Note**
>
> Per impostazione predefinita, AMS utilizza Systems Manager per applicare le patch facendo in modo che il gestore pacchetti (Linux) o il servizio System Update (Windows) interroghino il proprio repository predefinito per vedere quali nuovi pacchetti sono disponibili. Se, nel corso delle day-to-day operazioni, avete installato un pacchetto su un host Linux utilizzando il gestore di pacchetti predefinito, tale gestore di pacchetti preleva anche i nuovi pacchetti per quel software quando sono disponibili. In tal caso, potresti voler eseguire un'azione di patch (descritta in questa sezione) per disattivare tale istanza.

Sistemi operativi supportati

Sistemi operativi supportati (x86-64)

- Amazon Linux 2023
- Amazon Linux 2 (data di fine del supporto AMS prevista per il 30 giugno 2026)
- Oracle Linux 9.x, 8.x
- Red Hat Enterprise Linux (RHEL) 9.x, 8.x
- SUSE Linux Enterprise Server 15 SP6
- SUSE Linux Enterprise Server per SAP 15 e versioni successive SP3
- Microsoft Windows Server 2022, 2019, 2016
- Ubuntu 20.04, 22.04, 24.04

Sistemi operativi supportati () ARM64

- Amazon Linux 2023
- Amazon Linux 2 (data di fine del supporto AMS prevista per il 30 giugno 2026)

Patch supportate

AWS Managed Services supporta l'applicazione di patch principalmente a livello di sistema operativo. Le patch installate possono differire in base al sistema operativo.

Important

Tutti gli aggiornamenti vengono scaricati dagli archivi remoti del servizio patch di base di Systems Manager configurati sull'istanza e descritti più avanti in questo argomento. L'istanza deve essere in grado di connettersi ai repository in modo da poter eseguire l'applicazione delle patch.
Per disattivare il servizio di base delle patch per i repository che forniscono pacchetti che desideri gestire autonomamente, esegui il seguente comando per disabilitare il repository:

```
yum-config-manager DASHDASHdisable REPOSITORY_NAME
```

Recupera l'elenco dei repository attualmente configurati con il seguente comando:

```
yum repolist
```

- Repository preconfigurati Amazon Linux (in genere quattro):

ID del repository	Nome del repository
amzn-main/latest	amzn-base principale
amzn-updates/più recenti	amzn-updates-base
epel/x86_64	Pacchetti aggiuntivi per Enterprise Linux 6 - x86_64
pbis	Aggiornamenti dei pacchetti PBIS

- Archivi preconfigurati Red Hat Enterprise Linux (cinque per Red Hat Enterprise Linux 7 e cinque per Red Hat Enterprise Linux 6):

ID del repository	Nome del repository
Regione RHUI- -7/x86_64 client-config-server	Server di configurazione del client Red Hat Update Infrastructure 2.0
Regione RHUI- /7Server/x86_64 rhel-server-releases	Red Hat Enterprise Linux Server 7
Regione RHUI- /7Server/x86_64 rhel-server-releases	Red Hat Enterprise Linux Server 7 RH Common () RPMs
epel/x86_64	Pacchetti aggiuntivi per Enterprise Linux 7 - x86_64
pbis	Aggiornamenti dei pacchetti PBIS

ID del repository	Nome del repository
Regione RHUI- -6 client-config-server	Red Hat Update Infrastructure 2.0
Regione RHUI- rhel-server-releases	Red Hat Enterprise Linux Server 6 () RPMs

ID del repository	Nome del repository
Regione RHUI- rhel-server-rh-common	Red Hat Enterprise Linux Server 6 RH Common () RPMs
respingere	Pacchetti aggiuntivi per Enterprise Linux 6 - x86_64
pbis	Aggiornamenti dei pacchetti PBIS

- Archivi preconfigurati CentOS 7 (in genere cinque):

ID del repository	Nome del repository
base/7/x86_64	CentOS-7 - Base
aggiornamenti/7/x86_64	CentOS-7 - Aggiornamenti
extras/7/x86_64	CentOS-7 - Extra
epel/x86_64	Pacchetti aggiuntivi per Enterprise Linux 7 - x86_64
pbis	Aggiornamenti dei pacchetti PBIS

- Per Microsoft Windows Server, tutti gli aggiornamenti vengono rilevati e installati utilizzando l'agente di Windows Update, configurato per utilizzare il catalogo di Windows Update (questo non include gli aggiornamenti di Microsoft Update).

  Nei sistemi operativi Microsoft Windows, Patch Manager utilizza il file cab wsusscn2.cab di Microsoft come fonte degli aggiornamenti di sicurezza del sistema operativo disponibili. Questo file contiene informazioni sugli aggiornamenti relativi alla sicurezza pubblicati da Microsoft. Patch Manager scarica regolarmente questo file da Microsoft e lo utilizza per aggiornare il set di patch disponibili per le istanze di Windows. Il file contiene solo gli aggiornamenti identificati da Microsoft come correlati alla sicurezza. Man mano che vengono elaborate le informazioni del file, Gestione patch rimuove anche gli aggiornamenti sostituiti da quelli successivi. Pertanto, viene visualizzato e può essere installato solo l'aggiornamento più recente. Ad esempio, se KB4 012214 sostituisce KB3135456, solo KB4 012214 viene reso disponibile come aggiornamento in Patch Manager.

Per ulteriori informazioni sul file wsusscn2.cab, vedere l'articolo di Microsoft Using WUA to Scan for Updates Offline.

Applicazione di patch e progettazione dell'infrastruttura

AMS utilizza diversi metodi di applicazione delle patch a seconda della progettazione dell'infrastruttura: mutabili o immutabili (per le definizioni dettagliate, vedere). Termini chiave AMS

Con le infrastrutture mutabili, l'applicazione delle patch viene eseguita utilizzando una tradizionale metodologia locale di installazione degli aggiornamenti direttamente EC2 sulle istanze Amazon, individualmente, dai tecnici operativi AMS. Questo metodo di patching viene utilizzato per gli stack che non sono gruppi di Auto Scaling e contengono una singola istanza EC2 Amazon o poche istanze. In questo scenario, la sostituzione dell'AMI su cui si basava l'istanza o lo stack distruggerebbe tutte le modifiche apportate a quel sistema dalla prima implementazione, quindi ciò non avviene. Gli aggiornamenti vengono applicati al sistema in esecuzione e potrebbero verificarsi tempi di inattività del sistema (a seconda della configurazione dello stack) a causa del riavvio dell'applicazione o del sistema. Questo problema può essere mitigato con una strategia di aggiornamento. Blue/Green Per ulteriori informazioni, consulta AWS CodeDeploy Introduces Blue/Green Deployments.

Con infrastrutture immutabili, il metodo di patching sostituisce l'AMI. Le istanze immutabili vengono aggiornate in modo uniforme utilizzando un'AMI aggiornata che sostituisce l'AMI specificata nella configurazione del gruppo Auto Scaling. I rilasci di AMS aggiornati (ovvero con patch) AMIs ogni mese, di solito la settimana del Patch Tuesday. La sezione seguente descrive come funziona.

Come funziona l'applicazione di patch standard AMS

AMS utilizza il servizio Systems Manager Run Command per le patch critiche pianificate regolarmente, mensili e in base alle necessità, con due metodi di patching principali, sul posto e la sostituzione dell'AMI, a seconda della strategia di implementazione dell'infrastruttura (mutabile o immutabile). Questa sezione descrive il servizio, i tipi, i metodi e i processi di applicazione delle patch di AMS.

AMS definisce due tipi di patch, che sono programmati in modo diverso:

- Patch critiche: gli aggiornamenti vengono applicati il più rapidamente possibile, dopo l'accettazione della notifica.
- Patch standard: aggiornamenti regolari dei fornitori del sistema operativo e applicati mensilmente.

Le patch vengono applicate tramite patch sul posto o sostituendo l'AMI (su richiesta).

Aggiorna la scansione

AMS utilizza Amazon EC2 Run Command Service per contattare i tuoi EC2 stack Amazon e distribuire gli script di scansione e patching richiesti. AMS utilizza il componente nativo di gestione dei pacchetti già installato sul sistema operativo supportato per eseguire tutti i comportamenti di scansione e patch richiesti sullo EC2 stack Amazon. Per Red Hat e Amazon Linux, il servizio utilizza yum. Per Windows, il servizio utilizza Windows Update Agent.

Le scansioni vengono eseguite quotidianamente utilizzando SSM Maintenance Windows e il documento AWS di default di AMS. RunPatchBaseline Ogni EC2 stack Amazon raggiungibile viene scansionato utilizzando gli archivi di aggiornamento per Linux e Windows. Il processo di patching AMS rileva tutti gli stack EC2 Amazon raggiungibili e quindi esegue le scansioni in un processo in batch in modo che lo stack rimanga sempre integro, anche se si verifica un errore durante l'esecuzione della scansione. I risultati della scansione vengono quindi salvati per ogni EC2 stack Amazon.

Per visualizzare i risultati della scansione per uno stack o un'istanza, invia una richiesta di servizio con l'ID dello stack o l'ID dell'istanza.

Il processo di applicazione delle patch predefinito di AMS consiste nell'installare tutte le patch disponibili indipendentemente dalla classificazione o dalla gravità delle patch (ad esempio, critiche o standard). L'eccezione sono le patch che sono state esplicitamente escluse dallo stack (le patch definite obbligatorie da AMS non devono essere escluse).

Ti viene inviata una notifica del servizio di patch 14 giorni prima della finestra di manutenzione proposta. In questo modo avrai il tempo di testare le patch proposte e accettarle o rifiutarle. Se non rispondi alla notifica del servizio di patch, alle tue istanze non viene applicata la patch. Quando arriva il momento di installare le patch, AMS crea una Request for Change (RFC) per ogni stack e tale RFC appare nell'elenco RFC del tuo account.

Finestra e avviso di manutenzione configurati da AMS

Con l'applicazione di patch configurata da AMS, ogni account ha una finestra di manutenzione mensile, che viene definita al momento dell'onboarding dell'account. La AWS Managed Services Maintenance Window (o Maintenance Window) esegue attività di manutenzione per AWS Managed Services (AMS) e si svolge 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.

La finestra di applicazione delle patch è diversa. La richiesta di servizio in uscita per l'applicazione delle patch (nota anche come notifica di servizio) include una finestra di patch consigliata.

> **Note**
>
> Per informazioni sulla risposta alla notifica del servizio di applicazione delle patch, vedere. Azioni che puoi intraprendere con l'applicazione di patch standard AMS

La notifica del servizio di applicazione delle patch viene inviata via e-mail all'indirizzo e-mail di contatto registrato per l'account. La notifica include un collegamento alla console AWS Support in cui è possibile rispondere. Puoi anche rispondere alla notifica utilizzando la pagina AMS Service Request. La notifica del servizio include:

- Un elenco di aggiornamenti IDs (CSUs IUs, e OUs) che si applicano allo stack e gli aggiornamenti che hai richiesto di escludere dall'applicazione delle patch (se presenti).
- IDs delle istanze che saranno interessate.
- Una finestra di applicazione delle patch proposta quando verranno applicati gli aggiornamenti. È possibile richiedere una finestra di patching diversa.
- Una richiesta di accettazione dell'applicazione di patch proposta o la richiesta di ulteriori informazioni. AMS ti dà il tempo di testare l'impatto degli aggiornamenti e approvare o rifiutare l'applicazione delle patch o chiedere l'esclusione di aggiornamenti specifici. Se hai bisogno di più tempo per i test e desideri che gli aggiornamenti vengano applicati dopo il test, rispondi alla notifica del servizio e descrivi ciò che desideri, oppure invia una richiesta di servizio per una nuova patch RFC in base ai dettagli della RFC precedente. Se non rispondi affatto alla notifica del servizio, non viene intrapresa alcuna azione di patch e la RFC viene annullata.

Se approvi la notifica del servizio, AMS esegue la patch RFC e applica gli aggiornamenti entro la finestra di patch concordata, in base all'impegno di servizio.

Al termine dell'applicazione delle patch, AMS invia all'utente una corrispondenza nella Service Request, con un riepilogo dell'esito dell'attività di patch (esito positivo o negativo).

Patch sul posto

L'applicazione di patch sul posto si riferisce a un metodo in cui AMS accede a ciascuna istanza dello stack e applica le patch.

L'applicazione di patch sul posto avviene su infrastrutture mutabili utilizzando istanze EC2 Amazon che eseguono un sistema operativo supportato. L'applicazione delle patch applica tutti gli aggiornamenti non esclusi disponibili fino a quel momento. Quando vengono rilasciate patch critiche, esiste un ulteriore processo di applicazione delle patch critiche.

Patch standard: sul posto

L'applicazione delle patch standard avviene secondo la pianificazione delle patch concordata suggerita nella notifica del servizio patch e include aggiornamenti periodici delle patch che non sono considerati critici.

Prima della finestra di applicazione delle patch proposta e con la risposta affermativa dell'utente alla notifica, viene creata una patch RFC che viene visualizzata nella dashboard RFC.

Patch critiche: sul posto

Quando un fornitore di sistema operativo rilascia un aggiornamento di sicurezza fondamentale, AMS notifica all'utente la presenza della patch RFC inviando una notifica di servizio (all'indirizzo e-mail di contatto del proprio account) per ogni stack, in base all'impegno di servizio AMS. La notifica del servizio include quanto segue per ogni aggiornamento:

- Data di rilascio dell'aggiornamento
- Criticità dell'aggiornamento
- Dettagli dell'aggiornamento (riferimento KB, ecc.)
- IDs degli stack interessati

È possibile testare gli aggiornamenti elencati nella notifica e approvare o rifiutare le patch rispondendo alla notifica del servizio. Se approvi la notifica, devi fornire una finestra di patch specifica per stack per l'installazione degli aggiornamenti.

> **Note**
>
> Le finestre di patch che scadono entro 24 ore dalla risposta alla notifica del servizio possono essere riprogrammate in base alla capacità disponibile.

Se non rispondi entro 10 giorni o se rifiuti la patch proposta, l'applicazione viene annullata.

Se desideri applicare gli aggiornamenti dopo il periodo consentito (fornito nella notifica), invia una richiesta di assistenza per una nuova pianificazione delle patch in base ai dettagli della notifica precedente.

Se approvi la notifica del servizio, AMS applica gli aggiornamenti entro la finestra di patch specificata, in base all'impegno del servizio.

In caso di aggiornamenti multipli, è possibile escludere aggiornamenti specifici dall'applicazione delle patch specificando gli aggiornamenti da escludere nella risposta alla notifica del servizio.

AMS ti invia una notifica di servizio per ogni stack, indicante l'esito di ogni aggiornamento (esito positivo o negativo).

Applicazione di patch agli aggiornamenti AMI (utilizzo delle patch AMIs per i gruppi di Auto Scaling)

L'applicazione di patch sostitutive alle AMI viene eseguita su infrastrutture immutabili aggiornando l'ID AMI configurato per distribuire nuove istanze EC2 Amazon in un gruppo di Auto Scaling.

Amazon Machine Images (AMIs) viene rilasciato regolarmente per i sistemi operativi supportati. I fornitori di sistemi operativi rilasciano nuove patch su base periodica. AMS prende l'AMI fornita da Amazon, la aggiorna con le patch più recenti e quindi aggiunge i componenti appropriati per consentirle di funzionare nell'ambiente AMS. Quindi, rende disponibile la nuova AMI AMS a tutti i clienti AMS condividendo l'AMI con gli account. I tuoi stack di gruppi Auto Scaling possono essere aggiornati su base mensile con questi AMS appena rilasciati. AMIs L'immagine seguente illustra come AMIs vengono utilizzati in AMS i vostri ambienti.

I gruppi Auto Scaling creano le proprie istanze in base all'AMI configurata per il gruppo Auto Scaling. Quando le condivisioni AMS vengono aggiornate AMIs, sono disponibili le seguenti opzioni a seconda di come gestisci gli aggiornamenti AMI:

- Se si utilizza uno strumento di distribuzione delle applicazioni (ad esempio UserData CodeDeploy, e così via) che personalizza automaticamente le istanze dopo la creazione, è possibile effettuare le seguenti operazioni:
  - Rispondi alla notifica del servizio di patching o invia una richiesta di assistenza per l'AMI AMS più recente che sostituisca l'AMI di configurazione del gruppo Auto Scaling corrente. Dopo la sostituzione dell'ID AMI nella configurazione dei gruppi di Auto Scaling, AMS avvia gli aggiornamenti periodici delle istanze e le configurazioni delle istanze del gruppo Auto Scaling (ad

esempio, installazione di applicazioni, script di avvio, ecc.) vengono applicate automaticamente alle nuove istanze create con la nuova AMI AMS.

- Se utilizzi un' custom/golden AMI nella configurazione dei tuoi gruppi di Auto Scaling, puoi:
  - Crea un'istanza con la nuova AMI AMS, personalizza l'istanza e crea una nuova AMI dorata. Condividi la nuova Golden AMI con AMS utilizzando la EC2 console Amazon e invia una richiesta di servizio ad AMS per aggiornare la configurazione dei tuoi gruppi di Auto Scaling per utilizzare la tua nuova AMI personalizzata.
  - Condividi la tua Golden AMI esistente con AMS utilizzando la EC2 console Amazon e invia una richiesta di assistenza affinché AMS aggiorni la tua Golden AMI. Per fare ciò, AMS crea un'istanza dalla tua AMI dorata, applica le patch a quell'istanza, crea una nuova AMI dorata per te e quindi aggiorna la configurazione dei tuoi gruppi di Auto Scaling per utilizzare la nuova AMI. Lo svantaggio è che AMS non può verificare che la tua nuova AMI personalizzata funzioni nel modo desiderato. Invece, dovresti testare l'istanza creata con la nuova AMI e verificare che tutto funzioni correttamente prima di creare una nuova AMI dorata, condividerla e richiedere che AMS aggiorni i tuoi gruppi di Auto Scaling. AMS non consiglia questa opzione.

Patching standard: aggiornamenti AMI

Ogni mese AMS rilascia nuove Amazon Machine Images (AMIs) con miglioramenti del servizio e nuove patch che si applicano a. AMIs

> **Note**
>
> I nuovi AMS AMIs vengono generati dopo Patch Tuesday da AWS aggiornato AMIs. Quindi, AMS li testa prima di renderli disponibili. Dopo il nuovo AMIs test, le azioni AMS sono state aggiornate AMIs agli account gestiti.

Patch critiche: aggiornamenti AMI

Quando necessario, AMS fornisce AMIs aggiornamenti con patch di sicurezza critiche rilasciate dall'ultima versione mensile dell'AMI.

Il processo per gli aggiornamenti critici di sicurezza delle infrastrutture immutabili è identico al processo AMI mensile per le infrastrutture immutabili, tranne per il fatto che viene creata una nuova AMI AMS al di fuori della normale pianificazione (Patch Tuesday), basata sul rilascio di nuovi aggiornamenti critici. AMS rende disponibile una nuova AMI con le patch di sicurezza critiche in base

agli accordi sul livello di servizio (SLAs) definiti per il tuo account. Aggiornamenti AMS dei gruppi Auto Scaling solo su richiesta. Utilizza una richiesta di assistenza per inviare richieste di sostituzione dell'AMI.

Errori di applicazione delle patch standard AMS

In caso di aggiornamenti non riusciti, AMS esegue un'analisi per comprendere la causa dell'errore e comunica all'utente l'esito dell'analisi. Se l'errore è attribuibile ad AMS, riproviamo a eseguire gli aggiornamenti se rientrano nella finestra di manutenzione. Altrimenti, AMS crea notifiche di servizio per l'aggiornamento non riuscito dell'istanza e attende le tue istruzioni.

In caso di guasti attribuibili al sistema, è possibile inviare una richiesta di assistenza con una nuova patch RFC per aggiornare le istanze.

Azioni che puoi intraprendere con l'applicazione di patch standard AMS

Oltre a testarne di nuovi AMIs, è possibile intraprendere diverse azioni per gestire l'applicazione di patch all'infrastruttura:

- Se il test degli aggiornamenti ha richiesto più tempo di quanto consentito dalla finestra di patch, puoi richiedere ad AMS di applicare gli aggiornamenti che sono stati annullati quando sei pronto inviando una richiesta di servizio (utilizza i dettagli nella notifica di servizio originale come base).
- È possibile richiedere l'applicazione di un aggiornamento importante (UI) o altro aggiornamento (OU) prima della successiva finestra di aggiornamento automatico inviando una richiesta di servizio contenente un elenco degli aggiornamenti, delle istanze applicabili e altri dettagli, a seconda dei casi. Poiché questo CT non è automatizzato, la pianificazione e l'esecuzione richiedono più tempo. Verificate gli obiettivi del livello di servizio (SLOs) per il momento opportuno. Per ulteriori informazioni, consulta Obiettivi del livello di servizio AMS (SLOs).

Inoltre, è possibile utilizzare AMS esistenti, con patch, AMIs per crearne di personalizzati AMIs. Per informazioni, consulta AMI | Create.

> **Note**
>
> Non puoi richiedere una nuova AMI AMS basata su un aggiornamento importante o altro aggiornamento prima della prossima finestra di manutenzione, perché il processo di rilascio dell'AMI AMS segue una cadenza uniforme a vantaggio di tutti i clienti AMS.

Cambiare ciò che esce patched/opting

Con l'applicazione di patch configurata da AMS, nella risposta alla notifica del servizio di applicazione delle patch o in una richiesta di assistenza, puoi modificare le risorse a cui applicare le patch. Puoi eseguire le operazioni indicate di seguito:

- Definite un elenco di patch da escludere dalla riparazione, per stack e per sistema operativo.
- Definite un elenco di risorse che devono essere escluse da determinate patch o da tutte le patch.
- Definite un elenco di risorse che devono essere sempre escluse da tutte le patch.
- Definite un elenco di risorse a cui applicare le patch in un determinato giorno e in una certa ora (utile se non avete definito una finestra di manutenzione).

Per escludere una o più patch, invia una richiesta di servizio o rispondi alla notifica del servizio di patch utilizzando il modello fornito di seguito. Non inviate una RFC. Includi nella richiesta il nome o i nomi della patch che desideri escludere e il motivo. Includi queste informazioni in una richiesta di assistenza come segue:

- Nome: il nome della patch. Per le patch di Windows, questo è il nome KB, ad esempio`KB3145384`. Per le patch Linux, questo è il nome del pacchetto, ad esempio. `openssh-6.6.1p1-25.61.amzn1.x86_64`
- Motivo: un commento che indica il motivo per cui la patch viene esclusa.
- Ora di scadenza: il momento in date/time cui scade l'esclusione.

Se una patch esclusa è già installata, viene rimossa.

La richiesta viene esaminata da un operatore che ne discuterà con l'utente se l'esclusione di tali patch rappresenti un rischio significativo per la sicurezza. Viene inoltre negoziata la data di scadenza per le patch escluse. Dopo la data di scadenza concordata, l'esclusione scade e la patch viene installata su qualsiasi patch successiva.

Le patch presenti nell'elenco di esclusione vengono comunque restituite nei risultati della scansione, se applicabile.

> **Note**
>
> A differenza di Windows, le patch Linux sono specifiche della versione. Questa distinzione è importante perché le nuove versioni di una patch esclusa non vengono escluse

automaticamente. È tua responsabilità notificare ad AMS di escludere nuove versioni di una patch Linux se è quello che vuoi fare.

Modelli di risposta alle notifiche del servizio di patch

È necessario rispondere alle notifiche del servizio di applicazione delle patch, utilizzando il formato specificato, per eseguire l'applicazione delle patch sulle istanze. Dovresti farlo se non hai già impostato una finestra di manutenzione con AMS.

Quando rispondi a una notifica di servizio, utilizza il formato fornito.

Se non è impostata alcuna finestra di manutenzione, facci sapere quando correggere quanto mostrato di seguito:

```
UTC                 StartTime       StackId                     InstanceId (Optional)
2019-04-01          15:00           stack-123456789012          i-1234566789
2019-04-01          15:00           stack-123456789013          i-1234566784
2019-04-01          15:00           stack-123456789014          i-1234566783
2019-04-01          15:00           stack-123456789015          i-1234566782
```

Se hai una finestra di manutenzione impostata e desideri che determinate risorse vengano escluse da determinate patch, usa il seguente formato:

```
StackId                     InstanceId (Optional)       Exclude Patches
stack-123456789012          i-1234566789                PATCH
stack-123456789013          i-1234566784                PATCH
stack-123456789014          i-1234566783                PATCH
stack-123456789015          i-1234566782                PATCH
```

Se avete una finestra di manutenzione impostata e desiderate che determinate risorse siano sempre escluse da tutte le patch, utilizzate il seguente formato:

```
StackId                     InstanceId (Optional)       Exclude Patches
stack-123456789012          i-1234566789                ALL
stack-123456789015          i-1234566782                ALL
```

Preparazione per l'applicazione delle patch

Per preparare l'ambiente all'applicazione automatica delle patch, consigliamo quanto segue:

- Assicurati di disporre di un inventario completo di tutte le istanze da correggere.
- Assicuratevi che il backup delle vostre risorse sia effettuato regolarmente nell'ambito della vostra strategia di continuità aziendale. I backup aggiuntivi vengono creati come parte della sequenza di patch e questi vengono eliminati automaticamente in base alla politica di conservazione di Patch Orchestrator configurata (l'impostazione predefinita è 60 giorni).
- Assicurati che tutte le licenze pertinenti siano aggiornate.
- Modifica le finestre di manutenzione dello stack per applicare le patch in modo da applicare le patch agli stack di test prima degli stack di produzione. In questo modo, eventuali errori relativi all'applicazione delle patch vengono rilevati negli stack di test e possono essere identificati prima che gli stack di produzione vengano corretti.

Visualizzazione delle impostazioni delle patch

Per scoprire qual è la tua attuale configurazione di applicazione delle patch, puoi fare quanto segue:

- Inviate una richiesta di servizio ad AMS con la richiesta.
- Attendi una notifica del servizio di patch. L'avviso di patch indica tutte le patch da applicare e le istanze da applicare e suggerisce anche una finestra di aggiornamento.

È possibile inviare una richiesta di assistenza per modificare quanto segue:

- Intervallo di scansione: la quantità di tempo, in minuti, tra le scansioni di conformità eseguite sulle istanze di questo stack.

  L'impostazione predefinita è `240` (4 ore).
- NotificationWindow: con quanto anticipo (in minuti) rispetto a una modifica pianificata (patch) deve esserti inviata la notifica. L'impostazione predefinita è `10080` (7 giorni).

Patch standard AMS FAQs

Questa sezione fornisce le risposte ad alcune domande frequenti.

- D: Come posso disattivare l'applicazione di patch a livello globale?

  R: Per disattivare globalmente l'applicazione delle patch, invia una richiesta di assistenza. Tieni presente che non puoi disattivare le patch obbligatorie di AMS. Tutti gli stack continueranno a essere scansionati in modo da poter segnalare eventuali vulnerabilità.

- D: Come posso escludere stack specifici dall'applicazione delle patch?

  R: Per escludere definitivamente stack specifici dall'applicazione delle patch, invia una richiesta di assistenza. Per escludere determinati stack da un particolare ciclo di patch, rispondi all'imminente avviso di patch con l'elenco degli stack da escludere. Per informazioni, consulta Cambiare ciò che esce patched/opting. Tieni presente che non puoi disattivare le patch obbligatorie.

- D: Cosa succede se non approvo una notifica del servizio di patch?

  R: Hai 14 giorni per approvare una richiesta di servizio di patching standard e 10 giorni per approvare un avviso di patch importante. Se non approvi la richiesta di assistenza entro il periodo di tempo, l'impegno di assistenza viene annullato e non viene eseguita alcuna patch. In caso di patch obbligatorie, le patch vengono applicate indipendentemente dalla risposta alla richiesta di servizio.

- D: Come si esclude l'installazione di patch e pacchetti specifici?

  R: Per escludere definitivamente patch o pacchetti specifici, invia una richiesta di servizio. Per escludere determinate patch o pacchetti da un particolare ciclo di patch, rispondi all'imminente avviso di patch con l'elenco delle patch o dei pacchetti da escludere. Per informazioni dettagliate, vedi Cambiare ciò che esce patched/opting. Tieni presente che non puoi disattivare le patch obbligatorie.

- D: Cosa succede se un sistema si guasta a causa dell'applicazione di patch?

  R: AMS monitora ogni sistema. AMS invia all'utente una notifica di servizio sull'esito di ogni aggiornamento (ovvero, esito positivo o negativo) per stack e istanza. Se viene rilevato un errore, AMS indaga, ripristina l'istanza e quindi un tecnico operativo AMS tenta di applicare manualmente la patch. Per informazioni, consulta Errori di applicazione delle patch standard AMS.

- D: Quali aggiornamenti sono gestiti da AMS?

R: AMS gestisce gli aggiornamenti a livello di sistema operativo notificati ad AMS dal fornitore. Per ulteriori informazioni, consulta Patch supportate.

- D: Quali aggiornamenti non sono gestiti da AMS?

  R: Gli aggiornamenti a livello di applicazione non sono gestiti da AMS.

- D: Come vengono aggiornati i gruppi di Auto Scaling?

  R: I gruppi Auto Scaling vengono aggiornati con un'AMI sostitutiva nella configurazione del gruppo Auto Scaling ed eseguono un aggiornamento progressivo. Un aggiornamento progressivo osserva l' HealthyHostThreshold impostazione della configurazione di patch, che determina quante EC2 istanze Amazon in uno stack devono essere mantenute attive durante l'applicazione delle patch. Per ulteriori informazioni, consulta Applicazione di patch agli aggiornamenti AMI (utilizzo delle patch AMIs per i gruppi di Auto Scaling).

- D: Come faccio a installare gli aggiornamenti al di fuori del ciclo normale?

  R: Per gli aggiornamenti a livello di sistema operativo che desideri installare al di fuori della normale pianificazione delle patch, invia una richiesta di assistenza utilizzando la notifica di installazione delle patch che hai ricevuto. Ciò può accadere se il test di una patch proposta ha richiesto più di 21 giorni (per una patch standard) o 14 giorni (per una patch critica). Out-of-bandl'applicazione delle patch può essere eseguita sul posto per le istanze Amazon EC2 autonome.

- D: Come vengono applicate le patch agli stack o alle istanze appena distribuiti?

  R: Quando crei una nuova istanza Amazon EC2 Stack o un gruppo Auto Scaling, devi sempre specificare l'AMI AMS più recente, che conterrà già le patch più recenti. Per le infrastrutture mutabili, l'applicazione di patch in linea deve essere eseguita non appena lo stack viene distribuito.

Impegni relativi al servizio di patching

In base al tipo di implementazione dell'infrastruttura e alla criticità dell'aggiornamento, forniamo impegni di servizio per aggiornamenti di sicurezza critici per infrastrutture mutabili e immutabili e aggiornamenti importanti per infrastrutture mutabili e immutabili.

Applicazione di patch standard

Questi sono gli impegni di servizio AMS per l'applicazione di patch standard.

Applicazione di patch standard, infrastruttura mutabile (applicazione di patch in loco)

Evento/azione	Misurazione dell'impegno nel servizio
Gli aggiornamenti importanti vengono rilasciati tra un mese.	L'orologio inizia
A quattordici giorni dalla creazione della notifica di patch standard, AMS comunica all'utente l'imminente installazione di patch pianificate tramite una notifica di servizio e via e-mail per ogni stack. La notifica del servizio include: • Un elenco di aggiornamenti IDs (CSUs e IUs) applicabili (necessari e non applicati) per lo stack e gli aggiornamenti esclusi dall'appl icazione delle patch • IDs degli stack interessati • La finestra di manutenzione in cui verranno applicati gli aggiornamenti	L'orologio si interrompe dopo l'invio della notifica di servizio.
Verificate l'impatto degli aggiornamenti e approvate o rifiutate la RFC. Se non rispondi entro 14 giorni o rifiuti l'applicazione della patch nella risposta alla notifica del servizio, non viene intrapresa alcuna azione. Se impieghi più di 14 giorni per eseguire il test e desideri che gli aggiornamenti vengano	Se non approvi o non rispondi entro 14 giorni, la modifica in sospeso viene annullata e l'impegno di servizio per gli aggiornamenti non è applicabile.

Evento/azione	Misurazione dell'impegno nel servizio
applicati dopo il periodo di 14 giorni, invia una richiesta di servizio per una nuova patch RFC in base ai dettagli della RFC precedente.	
Se approvi la notifica del servizio entro 14 giorni, AMS applica gli aggiornamenti. Puoi scegliere di escludere aggiornam enti specifici da una RFC specificando gli aggiornamenti da escludere nella risposta alla notifica del servizio.	L'orologio inizia se approvi la notifica del servizio entro 14 giorni dalla ricezione. L'orologi o si interrompe dopo il tentativo di installazione dell'aggiornamento.
AMS invia una notifica di servizio sull'esito di ogni tentativo di aggiornamento. La notifica di servizio include i seguenti dettagli: • ID EC2 istanza Amazon • Aggiornamento 1 Riuscito o non riuscito: ARN a1, ARN a2... • Aggiornamento 2 riuscito o non riuscito: ARN b1, ARN b2... • Aggiornamento N riuscito o non riuscito: ARN c1, ARN c2...	Non applicabile.
In caso di aggiornamenti non riusciti, AMS esegue un'analisi per comprendere la causa dell'errore e comunica all'utente l'esito dell'anal isi. Se l'errore è attribuibile ad AMS, AMS riprova gli aggiornamenti se rientra nella finestra di manutenzione, altrimenti AMS crea notifiche di servizio per la combinazione istanza-aggiornamento fallita e attende le istruzioni in una finestra di manutenzione.	Non applicabile.

Evento/azione	Misurazione dell'impegno nel servizio
In caso di guasti imputabili a te, invia una richiesta di assistenza per una nuova patch RFC per aggiornare le istanze.	Non applicabile.

Patch critiche

Questi sono gli impegni di servizio di AMS per gli aggiornamenti di sicurezza critici.

Aggiornamenti critici di sicurezza, infrastruttura mutevole

Evento/azione	Misurazione dell'impegno nel servizio
La CSU viene rilasciata.	L'orologio inizia
AMS notifica la patch RFC tramite una notifica di servizio (che invia anche un'e-mail) per ogni stack. La notifica del servizio include: • Data di rilascio degli aggiornamenti • Criticità degli aggiornamenti • Dettagli dell'aggiornamento: riferimento KB e così via • IDs degli stack interessati	L'orologio si interrompe dopo l'invio della notifica del servizio.
Si testano gli aggiornamenti elencati nella RFC e si approva o si rifiuta la RFC entro 10 giorni rispondendo alla notifica del servizio. Fornisci una finestra di manutenzione specifica (per stack) per l'installazione degli aggiornam enti. Le finestre di manutenzione specifica te entro 24 ore dalla risposta alla notifica del servizio possono essere riprogrammate in base alla capacità disponibile.	Se non approvi o non rispondi entro 14 giorni, la modifica in sospeso viene annullata e l'impegno di servizio per l'aggiornamento non è applicabile.

Evento/azione	Misurazione dell'impegno nel servizio
Se non rispondi entro 10 giorni o se rifiuti la patch RFC, l'azione in sospeso viene annullata. Se desideri applicare gli aggiornamenti dopo il periodo di 14 giorni, invia una richiesta di servizio per una nuova patch RFC in base ai dettagli della RFC precedente.	
Se approvi la notifica del servizio, AMS applica gli aggiornamenti. Per più aggiornamenti, puoi scegliere di escludere aggiornamenti specifici dalla modifica specificando gli aggiornamenti da escludere nella risposta alla notifica del servizio.	Se la finestra di manutenzione desiderata non rientra nell'intervallo di tempo dell'impegno di servizio, l'impegno di servizio per l'aggiorn amento viene perso solo se la RFC non viene eseguita entro la finestra di manutenzione desiderata.
AMS invia all'utente una notifica di servizio sull'esito di ogni aggiornamento applicato. La notifica di servizio include i seguenti dettagli: • ID EC2 istanza Amazon • Aggiornamento riuscito: ARN a1, ARN a2... • Aggiornamento non riuscito: ARN c1, ARN c2...	Non applicabile.
In caso di aggiornamenti non riusciti, AMS esegue un'analisi per comprenderne la causa e comunica all'utente l'esito dell'analisi. Se l'errore è attribuibile ad AMS, AMS riprova gli aggiornamenti se rientra nella finestra di manutenzione, altrimenti AMS crea notifiche di servizio per la combinazione istanza-a ggiornamento fallita e attende le istruzioni in una nuova finestra di manutenzione.	Non applicabile.

Evento/azione	Misurazione dell'impegno nel servizio
In caso di guasti imputabili a te, invia una richiesta di assistenza per una nuova patch RFC per aggiornare le istanze.	Non applicabile.

Aggiornamenti di sicurezza critici, infrastruttura immutabile

Evento/azione	Misurazione dell'impegno nel servizio
La CSU viene rilasciata.	L'orologio inizia
AMS comunica all'utente quanto segue tramite una notifica di servizio: • Data di rilascio dell'aggiornamento • Criticità dell'aggiornamento • Dettagli dell'aggiornamento (riferimento KB e così via) • L'impatto di AMS Amazon Machine Images (AMI) • Data e ora di rilascio previste per il nuovo aggiornamento AMIs	L'orologio continua a funzionare.
Versioni di AMS aggiornate AMIs nell'account gestito.	L'orologio si ferma.
Se approvi la notifica del servizio, AMS applica gli aggiornamenti. AMS ti comunica i dati AMIs condivisi nel tuo account, tramite una notifica di servizio e via e-mail.	Non applicabile.
Se il test del nuovo AMIs richiede più tempo del tempo assegnato (una settimana), puoi inviare una richiesta di assistenza ad AMS per aggiornare i tuoi gruppi di Auto Scaling con	Non applicabile.

Evento/azione	Misurazione dell'impegno nel servizio
la nuova AMI AMS (così com'è). Se desideri modificare la nuova AMI AMS con le tue configurazioni, usa una RFC con Management | Other | Other | Update CT (ct-0xdawir96cy7k) per richiedere l'aggiornamento dei tuoi gruppi di Auto Scaling.	

Rapporti e opzioni

AWS Managed Services (AMS) raccoglie dati da vari servizi AWS nativi per fornire report a valore aggiunto sulle principali offerte AMS.

AMS offre due tipi di report dettagliati:

- Report su richiesta: puoi richiedere determinati report ad hoc tramite il tuo Cloud Service Delivery Manager (CSDM). Questi report non hanno limiti perché potrebbe essere necessario richiederli più volte durante l'onboarding o gli eventi critici. Tuttavia, tieni presente che questi report non sono progettati per essere forniti secondo una pianificazione come i report settimanali. Per comprendere meglio le tue esigenze o per ulteriori informazioni sull'utilizzo dei report self-service, contatta il tuo CSDM.
- Report self-service: i report self-service AMS ti consentono di interrogare e analizzare direttamente i dati tutte le volte che ne hai bisogno. Utilizza i report self-service per accedere ai report dalla console AMS e ai set di dati di report tramite bucket S3 (un bucket per account). Ciò ti consente di integrare i dati nel tuo strumento di Business Intelligence (BI) preferito in modo da poter personalizzare i report in base alle tue esigenze.

Argomenti

Report su richiesta

Argomenti

AMS raccoglie dati da vari servizi AWS nativi per fornire report a valore aggiunto sulle principali offerte AMS. Per una copia di questi report, invia una richiesta al tuo Cloud Service Delivery Manager (CSDM).

Rapporti AMS Patch

Rapporti disponibili

- Rapporto riassuntivo sui dettagli dell'istanza di
- Rapporto sui dettagli della patch
- Rapporto Istanze a cui sono state perse le patch
- Rapporto sulla copertura SSM sull'applicazione delle patch

Rapporto riassuntivo sui dettagli dell'istanza di

Il rapporto di riepilogo dei dettagli dell'istanza di patch fornisce i dettagli delle istanze raccolti per le istanze inserite nella reportistica. Si tratta di un rapporto informativo che aiuta a identificare tutte le istanze registrate, lo stato dell'account, i dettagli dell'istanza, la copertura della finestra di manutenzione, il tempo di esecuzione della finestra di manutenzione, i dettagli dello stack e il tipo di piattaforma. Questo rapporto fornisce quanto segue:

1. Dati sulle istanze di produzione e non di produzione di un account. Nota: le fasi di produzione e non produzione derivano dal nome dell'account e non dai tag dell'istanza.
2. Dati sulla distribuzione delle istanze per tipo di piattaforma. Nota: il tipo di piattaforma «N/A» si intende quando non è AWS Systems Manager possibile recuperare le informazioni sulla piattaforma.
3. Dati sulla distribuzione dello stato delle istanze e sul numero di istanze in esecuzione, interrotte o terminate.

Nome del campo	Definizione
Data/ora del rapporto	La data e l'ora di generazione del rapporto.
ID dell'account	ID account AWS a cui appartiene l'ID dell'istanza
Nome dell'account	Nome dell'account AWS

Nome del campo	Definizione
Account di produzione	Identificatore degli account AMS prod e non prod, a seconda che il nome dell'acco unt includa o meno il valore «PROD», «NONPROD». Esempio: PROD, NONPROD, Non disponibile
Stato dell'account	Stato dell'account AMS. Ad esempio: ACTIVE, INACTIVE
Impegno al servizio dell'account AMS	PREMIO, IN PIÙ
Zona di atterraggio	Contrassegno per il tipo di landing zone dell'account. Ad esempio: MALZ, NON-MALZ
Restrizioni di accesso	Regioni a cui l'accesso è limitato. Ad esempio: US SOIL
ID dell'istanza	ID dell' EC2 istanza
Nome dell'istanza	Nome dell' EC2 istanza
Tipo di piattaforma dell'istanza	Tipo di sistema operativo (OS). Ad esempio: Windows, Linux e così via
Nome della piattaforma dell'istanza	Nome del sistema operativo (OS). Ad esempio: MicrosoftWindowsServer 2012R2Standard, RedHatEnterpriseLinuxServer
Nome stack	Nome dello stack che contiene l'istanza
Tipo di pila	Stack AMS (infrastruttura AMS all'interno dell'account del cliente) o stack del cliente (infrastruttura gestita da AMS che supporta le applicazioni dei clienti). Esempi: AMS, CUSTOMER

Nome del campo	Definizione
Nome del gruppo con scalabilità automatica	Nome dell'Auto Scaling Group (ASG) che contiene l'istanza
Instance Patch Group	Nome del gruppo di patch utilizzato per raggruppare le istanze e applicare la stessa finestra di manutenzione. Se il gruppo di patch non è assegnato, il valore sarà «Non assegnato »
Tipo di gruppo di patch di istanze	Tipo di gruppo di patch. PREDEFINITO: gruppo di patch predefinito con la finestra di manutenzione predefinita, determinata dal `AMSDefaultPatchGroup:True` tag sull'istanza. CLIENTE: gruppo di patch creato dal cliente. NOT_ASSIGNED: nessun gruppo di patch assegnato
Stato dell'istanza	Stato all'interno del ciclo di vita dell' EC2 istanza. Esempi: TERMINATED, RUNNING, STOPPING, STOPED, SHUTTING-DOWN, PENDING. Per ulteriori informazioni, consulta Ciclo di vita dell'istanza.
Copertura della finestra di manutenzione	Se in questa istanza sono presenti future finestre di manutenzione. Esempi: COVERED o NOT_COVERED
Data e ora di esecuzione della finestra di manutenzione	La prossima volta è prevista l'esecuzione della finestra di manutenzione. Se NULL, esecuzione a finestra singola, cioè non ricorrente

Rapporto sui dettagli della patch

Il rapporto AWS Managed Services (AMS) Patch Details fornisce dettagli sulle patch e copre la finestra di manutenzione di varie istanze, tra cui:

1. Dati sui gruppi di patch e sui relativi tipi.
2. Dati sulle finestre di manutenzione, durata, termine ultimo, date future di esecuzione della finestra di manutenzione (pianificazione) e istanze interessate da ciascuna finestra.
3. Dati su tutti i sistemi operativi inclusi nell'account e numero di istanze in cui il sistema operativo è installato.

Nome del campo	Definizione
Data/ora del rapporto	La data e l'ora di generazione del rapporto.
ID account	ID account AWS a cui appartiene l'ID dell'istanza
Nome dell'account	Nome dell'account AWS
ID dell'istanza	ID dell' EC2 istanza
Account di produzione	Identificatore degli account AMS prod e non prod, a seconda che il nome dell'account includa o meno il valore «PROD», «NONPROD». Se i dati non sono disponibili, il valore sarà «Non disponibile»
Stato dell'account	Stato dell'account AMS. Ad esempio: ACTIVE, INACTIVE
Tipo di piattaforma di istanza	Tipo di sistema operativo (OS). Ad esempio: Windows, Linux
Nome della piattaforma dell'istanza	Nome del sistema operativo (OS). Ad esempio: MicrosoftWindowsServer 2012R2Standard, RedHatEnterpriseLinuxServer

Nome del campo	Definizione
Tipo di pila	Stack AMS (infrastruttura AMS all'interno di un account cliente) o stack Customer (infrastruttura gestita da AMS che supporta le applicazioni dei clienti). Ad esempio: AMS, CUSTOMER
Instance Patch Group	Nome del gruppo di patch utilizzato per raggruppare le istanze e applicare la stessa finestra di manutenzione. Se il gruppo di patch non è assegnato, il valore sarà «Non assegnato»
Tipo di gruppo di patch di istanze	Tipo di gruppo di patch. PREDEFINITO: gruppo di patch predefinito con finestra di manutenzione predefinita, determinato dal `AMSDefaultPatchGroup:True` tag sull'istanza CLIENTE: gruppo di patch creato dal cliente NON ASSEGNATO: nessun gruppo di patch assegnato
Stato dell'istanza	Stato all'interno del ciclo di vita dell' EC2 istanza. Ad esempio: TERMINATED, RUNNING, STOPPING, STOPED, SHUTTING-DOWN, PENDING Per ulteriori informazioni, consulta Ciclo di vita dell'istanza.
ID della finestra di manutenzione	Identificatore della finestra di manutenzione
Stato della finestra di manutenzione	I valori possibili sono ABILITATI o DISABILITATI.
Tipo di finestra di manutenzione	Tipo di finestra di manutenzione

Nome del campo	Definizione
Finestra di manutenzione Data e ora di esecuzione successiva	La prossima volta è prevista l'esecuzione della finestra di manutenzione. Se NULL, esecuzione a finestra singola, cioè non ricorrente
Finestra di manutenzione dell'ultima esecuzione	L'ultima volta in cui è stata eseguita la finestra di manutenzione
Durata della finestra di manutenzione (ore)	La durata della finestra di manutenzione in ore
Copertura della finestra di manutenzione	La copertura della finestra di manutenzione
ID di base della patch	Linea di base della patch attualmente associata all'istanza
Stato della patch	Stato di conformità generale delle patch. Ad esempio: COMPLIANT, NON_COMPLIANT. Se manca almeno una patch, l'istanza viene considerata non conforme, altrimenti conforme.
Conforme: totale	Numero di patch conformi (tutte le severità)
Non conforme: totale	Numero di patch non conformi (tutte le severità)
Conforme - Critico	Numero di patch conformi con severità «critica»
Conforme: elevato	Numero di patch conformi con severità «elevata»
Conforme: medio	Numero di patch conformi con severità «media»
Conforme: basso	Numero di patch conformi con severità «bassa»
Conforme: informativo	Numero di patch conformi con severità «informativa»
Conforme: non specificato	Numero di patch conformi con gravità «non specificata»

Nome del campo	Definizione
Non conforme: critico	Numero di patch non conformi con gravità «critica»
Non conforme: elevato	Numero di patch non conformi con severità «elevata»
Non conforme: medio	Numero di patch non conformi con gravità «media»
Non conforme: basso	Numero di patch non conformi con gravità «bassa»
Non conforme: informativo	Numero di patch non conformi con severità «informativa»
Non conforme: non specificato	Numero di patch non conformi con gravità «non specificata»

Rapporto Istanze a cui sono state perse le patch

Il report AWS Managed Services (AMS) Instances That Missed Patches fornisce dettagli sulle istanze che hanno perso le patch durante l'ultima finestra di manutenzione, tra cui:

1. Dati sulle patch mancanti a livello di ID della patch.
2. Dati su tutte le istanze in cui manca almeno una patch insieme ad attributi quali la gravità della patch, i giorni senza patch, l'intervallo e la data di rilascio della patch.

Nome del campo	Definizione
Data/ora del rapporto	La data e l'ora di generazione del rapporto.
ID account	ID account AWS a cui appartiene l'ID dell'istanza
Nome dell'account	Nome dell'account AWS

Nome del campo	Definizione
Account di produzione	Identificatore degli account AMS prod, non prod, a seconda che il nome dell'acco unt includa o meno il valore «PROD», «NONPROD».
Stato dell'account	Stato dell'account AMS. Ad esempio: ATTIVO o INATTIVO
Livello di servizio dell'account AMS	PREMIUM o PLUS
ID istanza	ID dell' EC2 istanza
Tipo di piattaforma dell'istanza	Tipo di sistema operativo (OS). Ad esempio: Windows
Stato dell'istanza	Stato del ciclo di vita dell' EC2 istanza. Ad esempio: TERMINATED, RUNNING, STOPPING, STOPED, SHUTTING-DOWN, PENDING Per ulteriori informazioni, consulta Instance lifecycle.
ID della patch	ID della patch rilasciata. Ad esempio: KB3172729
Gravità della patch	Severità della patch per editore. Ad esempio: CRITICO, IMPORTANTE, MODERATO, BASSO, NON SPECIFICATO
Classificazione delle patch	Classificazione delle patch per editore. Ad esempio: CRITICALUPDATES, SECURITYU PDATES, UPDATEROLLUPS, UPDATES, FEATUREPACKS
Data e ora di rilascio della patch (UTC)	Data di rilascio della patch per editore

Nome del campo	Definizione
Stato di installazione della patch	Stato di installazione della patch sull'istanza per SSM. Ad esempio: INSTALLATO, MANCANTE, NON APPLICABILE
Giorni senza patch	Numero di giorni in cui l'istanza non ha ricevuto le patch dall'ultima scansione SSM
Intervallo di giorni senza patch	Un sacco di giorni senza patch. Ad esempio: <30 GIORNI, 30-60 GIORNI, 60-90 GIORNI, 90+ GIORNI

Rapporto sulla copertura SSM sull'applicazione delle patch

Il rapporto AMS Patching SSM Coverage indica se nelle EC2 istanze dell'account è installato o meno l'agente SSM.

Nome del campo	Definizione
Nome cliente	Nome del cliente per situazioni in cui vi sono più clienti secondari
Regione delle risorse	AWS Regione in cui si trova la risorsa
Account name (Nome account)	Il nome dell'account
AWS ID dell'account	L'ID dell' AWS account
ID della risorsa	ID dell' EC2 istanza
Nome risorsa	Nome dell' EC2 istanza
Bandiera conforme	Indica se sulla risorsa è installato l'agente SSM («Compliant») o meno («NON_COMPLIANT»)

Report di AMS Backup

Report disponibili

- Rapporto Backup Job Success/Failure
- Rapporto di riepilogo del backup
- Summary/Coverage Rapporto di Backup

Rapporto Backup Job Success/Failure

Il Success/Failure rapporto Backup Job fornisce informazioni sui backup eseguiti nelle ultime settimane. Per personalizzare il rapporto, specifica il numero di settimane per cui desideri recuperare i dati. Il numero predefinito di settimane è 12. La tabella seguente elenca i dati inclusi nel rapporto:

Nome del campo	Definizione
ID account AWS	ID dell'account AWS a cui appartiene la risorsa
Nome dell'account	Nome dell'account AWS
ID Job di Backup	L'ID del job di Backup
ID risorsa	L'ID della risorsa di cui è stato eseguito il backup
Tipo di risorsa	Il tipo di risorsa di cui viene eseguito il backup
Regione delle risorse	La AWS regione della risorsa di cui è stato eseguito il backup
Stato di Backup	Lo stato del backup. Per ulteriori informazioni, vedere Stati dei job di Backup
ID del punto di ripristino	L'identificatore univoco del punto di ripristino
Messaggio di stato	Descrizione degli errori o degli avvisi che si sono verificati durante il processo di backup
Dimensioni del backup	Dimensioni del backup in GB

Nome del campo	Definizione
ARN del punto di ripristino	L'ARN del backup creato
Durata del punto di ripristino in giorni	Numero di giorni trascorsi dalla creazione del punto di ripristino
Meno di 30 giorni	Indicatore dei backup che risalgono a meno di 30 giorni

Rapporto di riepilogo del backup

Nome del campo	Definizione
Nome del cliente	Nome del cliente per le situazioni in cui sono presenti più clienti secondari
Mese di backup	Mese del backup
Anno di Backup	Anno del backup
Tipo di risorsa	Il tipo di risorsa di cui viene eseguito il backup
Numero di risorse	Il numero di risorse di cui è stato eseguito il backup
Numero di punti di ripristino	Numero di istantanee distinte
Backup risalenti a meno di 30 giorni	Numero di backup che risalgono a meno di 30 giorni
Età massima dei punti di ripristino	L'età più vecchia del punto di ripristino (in giorni)
Pagina minima dei punti di ripristino	Età del punto di ripristino più recente, espressa in giorni

Summary/Coverage Rapporto di Backup

Il Summary/Coverage rapporto di Backup elenca quante risorse non sono attualmente protette da alcun AWS Backup piano. Discutete con il vostro CDSM un piano appropriato per aumentare la copertura, ove possibile, e ridurre il rischio di perdita dei dati.

Nome del campo	Definizione
Nome del cliente	Nome del cliente per le situazioni in cui sono presenti più clienti secondari
Regione	AWS regione in cui si trova la risorsa
Account name (Nome account)	Il nome dell'account
AWS ID dell'account	L'ID dell' AWS account
Tipo di risorsa	Il tipo di risorsa. Le risorse sono supportat e da AWS Backup (Aurora, DocumentDB, DynamoDB, EBS, EFS EC2, RDS e S3) FSx
ARN risorsa	ARN della risorsa
ID risorsa	ID della risorsa
Copertura	Indica se la risorsa è coperta o meno («COVERED» o «NOT_COVERED»)
Numero di risorse	Numero di risorse supportate nell'account
perc_coverage	Percentuale di risorse supportate con un backup eseguito negli ultimi 30 giorni.

Incidenti evitati e monitoraggio dei report di Top Talker

Rapporti disponibili

- Rapporto sugli incidenti evitati
- Rapporto Monitoring Top Talkers

Rapporto sugli incidenti evitati

Il rapporto Incidents Prevented elenca gli CloudWatch allarmi Amazon a cui è stato posto automaticamente rimedio, prevenendo un possibile incidente. Per ulteriori informazioni, consulta Riparazione automatica. La tabella seguente elenca le informazioni incluse in questo rapporto:

Nome del campo	Definizione
execution_start_time_utc	Data in cui è stata eseguita l'automazione
nome_cliente	Nome del cliente dell'account
account_name	Il nome dell'account
AwsAccountId	L'ID dell'account AWS
nome_documento	Il nome del documento SSM o dell'automazione eseguita
durata_in_minuti	La durata dell'automazione in minuti
Regione	AWS Regione in cui si trova la risorsa
automation_execution_id	L'ID dell'esecuzione
automation_execution_status	Lo stato dell'esecuzione

Rapporto Monitoring Top Talkers

Il rapporto Monitoring Top Talkers presenta il numero di CloudWatch avvisi Amazon generati in un periodo di tempo specifico e fornisce visualizzazioni delle risorse che generano il maggior numero di avvisi. Questo rapporto ti aiuta a identificare le risorse che generano il maggior numero di avvisi. Queste risorse potrebbero essere idonee per eseguire l'analisi della causa principale per risolvere il problema o per modificare le soglie di allarme per evitare attivazioni non necessarie quando non esiste un problema effettivo. La tabella seguente elenca le informazioni incluse in questo rapporto:

Nome del campo	Definizione
Nome cliente	Nome del cliente

Nome del campo	Definizione
AccountId	L'ID dell' AWS account
Categoria di avviso	Il tipo di avviso attivato
Descrizione	Descrizione dell'avviso
ID risorsa	ID della risorsa che ha attivato l'avviso
Nome risorsa	Nome della risorsa che ha attivato l'avviso
Regione	AWS Regione in cui si trova la risorsa
Stato dell'incidente	Stato più recente dell'incidente generato dall'allarme
Prima occorrenza	Prima volta che l'avviso è stato attivato
Evento recente	L'ultima volta in cui è stato attivato l'avviso
Numero di avvisi	Numero di avvisi generati tra la prima e la recente occorrenza

Rapporto sui dettagli degli addebiti di fatturazione

Il rapporto AWS Managed Services (AMS) Billing Charges Details fornisce dettagli sui costi di fatturazione AMS con account collegati e i rispettivi servizi AWS, tra cui:

- Costi a livello di servizio AMS, percentuali di uplift, livelli di servizio AMS a livello di account e tariffe AMS.
- Account e costi AWS di utilizzo collegati

Nome del campo	Definizione
Mese di fatturazione	Il mese e l'anno del servizio fatturato

Nome del campo	Definizione
ID del conto di pagamento	L'ID a 12 cifre che identifica l'account che sarà responsabile del pagamento degli addebiti AMS
ID dell'account collegato	L'ID a 12 cifre che identifica l'account AMS che utilizza i servizi che generano spese
AWS Nome del servizio	Il AWS servizio che è stato utilizzato
AWS Addebiti	I AWS costi per il nome del AWS servizio elencati in AWS Service Name
Piano tariffario	Il nome del piano tariffario associato all'account collegato
Proporzione di rialzo	La percentuale di aggiornamento (come V.WXYZ decimale) basata su pricing_plan, SLA e servizio AWS
Costi AWS adeguati	AWS utilizzo adattato per AMS
Costi AWS aumentati	La percentuale di addebiti AWS da addebitare per AMS; adjusted_aws_charges * uplift_percent
Istanze RDS Spend EC2	Istanze Spend on EC2 e RDS
Addebiti AMS	Costi AMS totali per il prodotto; uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp
Tariffa minima ripartita proporzionalmente	L'importo che addebitiamo per soddisfare il minimo contrattuale
Tariffa minima	Commissioni minime AMS (se applicabile)
Costi totali AMS dell'account collegato	Somma di tutti gli addebiti per il linked_account

Nome del campo	Definizione
Costi totali AMS del conto di pagamento	Somma di tutti gli addebiti relativi al conto del pagatore

Report di Trusted Remediator

Rapporti disponibili

- Rapporto riepilogativo di Trusted Remediator Remediation
- Rapporto di riepilogo sulla configurazione di Trusted Remedi
- Trusted Advisor Controlla il rapporto di riepilogo

Rapporto riepilogativo di Trusted Remediator Remediation

Il rapporto sullo stato di Trusted Remediator Remediation fornisce informazioni sulle riparazioni avvenute durante i cicli di riparazione precedenti. Il numero predefinito di settimane è 1. Per personalizzare il rapporto, specifica il numero di settimane in base al programma di riparazione.

Nome del campo	Definizione
Data	La data in cui i dati sono stati raccolti.
ID account	L'ID AWS dell'account a cui appartiene la risorsa
Nome dell'account	Il nome AWS dell'account
Controlla la categoria	La categoria di AWS Trusted Advisor controllo
Controlla il nome	Il nome del controllo corretto Trusted Advisor
ID di controllo	L'ID del controllo corretto Trusted Advisor
Modalità di esecuzione	La modalità di esecuzione configurata per il Trusted Advisor controllo specifico

Nome del campo	Definizione
OpsItem ID	L'ID del codice OpsItem creato da Trusted Advisor per la riparazione
OpsItem Stato	Lo stato del codice OpsItem creato Trusted Advisor al momento della segnalazione
ID risorsa	L'ARN della risorsa creata per la riparazione

Rapporto di riepilogo sulla configurazione di Trusted Remedi

Il rapporto di riepilogo della configurazione di Trusted Remediator fornisce informazioni sulle configurazioni correnti di Trusted Remediator Remediation per ogni controllo. Trusted Advisor

Nome del campo	Definizione
Data	La data in cui i dati sono stati raccolti.
ID account	L'ID AWS dell'account a cui si applica la configurazione
Nome dell'account	Il nome AWS dell'account
Controlla la categoria	La categoria di AWS Trusted Advisor controllo
Controlla il nome	Il nome del Trusted Advisor controllo corretto a cui si applica la configurazione
ID di controllo	L'ID del Trusted Advisor controllo corretto a cui si applica la configurazione
Modalità di esecuzione	La modalità di esecuzione configurata per il Trusted Advisor controllo specifico
Passa a Automated	Lo schema di tag, se configurato, per sostituire la modalità di esecuzione su Automated

Nome del campo	Definizione
Sovrascrivi a Manuale	Lo schema di tag, se configurato, per sostituir e la modalità di esecuzione impostandola su Manuale

Trusted Advisor Controlla il rapporto di riepilogo

Il rapporto Trusted Advisor Check Summary fornisce informazioni sui Trusted Advisor controlli correnti. Questo rapporto raccoglie i dati dopo ogni programma di riparazione settimanale. Il numero predefinito di settimane è 1. Per personalizzare il rapporto, specifica il numero di settimane in base al ciclo di riparazione.

Nome del campo	Definizione
Data	La data in cui i dati sono stati raccolti.
ID account	L'ID AWS dell'account a cui si applica la configurazione
Nome del cliente	Il nome AWS dell'account
Controlla la categoria	La categoria di AWS Trusted Advisor controllo
Controlla il nome	Il nome del Trusted Advisor controllo corretto a cui si applica la configurazione
ID di controllo	L'ID del Trusted Advisor controllo corretto a cui si applica la configurazione
Stato	Lo stato di avviso del controllo. Gli stati possibili sono ok (verde), warning (giallo), error (rosso) o not_available
Risorse contrassegnate	Il numero di AWS risorse che sono state contrassegnate (elencate) dal controllo. Trusted Advisor

Nome del campo	Definizione
Risorse ignorate	Il numero di AWS risorse che sono state ignorate Trusted Advisor perché le hai contrassegnate come soppresse.
Risorse in stato critico	Il numero di risorse in stato critico
Risorse in stato di allerta	Il numero di risorse in stato di avviso

Report self-service

I report self-service (SSR) di AWS Managed Services (AMS) sono una funzionalità che raccoglie dati da vari AWS servizi nativi e fornisce l'accesso ai report sulle principali offerte AMS. SSR fornisce informazioni che puoi utilizzare per supportare operazioni, gestione della configurazione, gestione degli asset, gestione della sicurezza e conformità.

Usa SSR per accedere ai report dalla console AMS e ai set di dati dei report tramite i bucket Amazon S3 (un bucket per account). Puoi collegare i dati al tuo strumento di business intelligence (BI) preferito per personalizzare i report in base alle tue esigenze specifiche. AMS crea questo bucket S3 (nome del bucket S3: (ams-reporting-data-a<Account_ID>) nella AWS regione principale e i dati vengono condivisi dal piano di controllo AMS ospitato nella regione us-east-1.

Important

Per accedere a questa funzionalità, devi avere uno dei seguenti ruoli:

- Zona di atterraggio con più account: AWSManagedServicesReadOnlyRole
- Zona di destinazione per account singolo: Cliente_ _Ruolo ReadOnly

Important

Utilizzo di chiavi personalizzate con AWS Glue
Per crittografare i AWS Glue metadati con una chiave KMS gestita dal cliente, è necessario eseguire i seguenti passaggi aggiuntivi per consentire ad AMS di aggregare i dati dall'account:

1. Apri la AWS Key Management Service console in https://console.aws.amazon.com/kms, quindi scegli Customer Managed Keys.
2. Seleziona l'ID della chiave che intendi utilizzare per crittografare i metadati. AWS Glue
3. Scegli la scheda Alias, quindi scegli Crea alias.
4. Nella casella di testo, immettete AmsReportingFlywheelCustomKey, quindi scegliete Crea alias.

Argomenti

Operazioni API interne

Se monitorate le operazioni delle API, potreste vedere chiamate alle seguenti operazioni solo interne:

- `GetDashboardUrl`
- `ListReportsV2`

Funzionamento interno dell'API: GetDashboardUrl

Questa operazione appare nei log di sistema quando viene richiamata dalla console AMS. Non ha altri casi d'uso. Non è disponibile per l'uso diretto.

Restituisce l'URL della dashboard incorporata per il rapporto corrispondente. Questa operazione accetta un valore `dashboardName` restituito da`ListReports`.

Sintassi della richiesta

```
HTTP/1.1 200
Content-type: application/json
{
    "dashboardName": "string"
}
```

Elementi della richiesta

`dashboardName`: il nome della QuickSight dashboard per la quale viene richiesto l'URL. Il nome del dashboard viene restituito nella ListReports versione 2.

- Tipo: stringa

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json
{
  "url": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200. I dati seguenti vengono restituiti in formato JSON mediante il servizio.

`url`: restituisce l' QuickSight URL della richiesta. `dashboardName`

- Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le azioni, vedi Errori comuni.

`BadRequestException`:

La richiesta inviata non è valida. Ad esempio, se l'input è incompleto o errato. Per i dettagli, consulta il messaggio di errore allegato.

Codice di stato HTTP: 400

`NotFoundException`:

La risorsa richiesta non è stata trovata. Assicurati che l'URI della richiesta sia corretto.

Codice di stato HTTP: 404

`TooManyRequestsException`:

La richiesta ha raggiunto il limite di limitazione. Riprova dopo il periodo di tempo specificato.

Codice di stato HTTP: 429

`UnauthorizedException`:

La richiesta viene rifiutata perché il chiamante non dispone di autorizzazioni sufficienti.

Codice di stato HTTP: 401

Funzionamento dell'API interna: ListReports V2

Questa API appare nei log di sistema quando viene richiamata dalla console AMS. Non ha altri casi d'uso. Non è disponibile per l'uso diretto.

Restituisce un elenco di report operativi disponibili per un account specifico.

Sintassi della richiesta

La richiesta non ha un corpo della richiesta.

Sintassi della risposta

```
HTTP/1.1 200
Content-type: application/json
{
  "reportsList": [
    {
        "dashboard": "string",
        "lastUpdatedTime": "string",
    }
  ],
  "reportsType": "string"
}
```

Elementi di risposta

Se l'operazione riesce, il servizio restituisce una risposta HTTP 200. I dati seguenti vengono restituiti in formato JSON mediante il servizio.

`reportsList`: L'elenco dei report operativi disponibili.

Tipo: matrice di oggetti del dashboard

`reportsType`: Indica se un rapporto è aggregato su più account o meno.

-Tipo: stringa

Errori

Per informazioni sugli errori comuni a tutte le azioni, consulta Errori comuni.

`BadRequestException`:

La richiesta inviata non è valida. Ad esempio, l'input è incompleto o errato. Per i dettagli, consulta il messaggio di errore allegato.

Codice di stato HTTP: 400

`NotFoundException`:

La risorsa richiesta non è stata trovata. Assicurati che l'URI della richiesta sia corretto.

Codice di stato HTTP: 404

`TooManyRequestsException`:

La richiesta ha raggiunto il limite di limitazione. Riprova dopo il periodo di tempo specificato.

Codice di stato HTTP: 429

`UnauthorizedException`:

La richiesta viene rifiutata perché il chiamante non dispone di autorizzazioni sufficienti.

Codice di stato HTTP: 401

Rapporto sulle patch (giornaliero)

Report disponibili

-
- Dettagli della patch
- Istanze in cui non sono state apportate le patch

Si tratta di un rapporto informativo che aiuta a identificare tutte le istanze inserite in Patch Orchestrator (PO), lo stato dell'account, i dettagli dell'istanza, la copertura della finestra di manutenzione, il tempo di esecuzione della finestra di manutenzione, i dettagli dello stack e il tipo di piattaforma.

Questo set di dati fornisce:

- Dati sulle istanze di produzione e non di produzione di un account. Le fasi di produzione e non produzione derivano dal nome dell'account e non dai tag dell'istanza.
- Dati sulla distribuzione delle istanze per tipo di piattaforma. Il tipo di piattaforma 'N/A' si verifica quando AWS Systems Manager (SSM) non è in grado di ottenere le informazioni sulla piattaforma.
- Dati sulla distribuzione dello stato delle istanze, sul numero di istanze in esecuzione, interrotte o terminate.

Nome del campo della console	Nome del campo del set di dati	Definizione
Restrizioni di accesso	restrizioni di accesso	Regioni a cui l'accesso è limitato
ID dell'account	aws_account_id	AWS ID dell'account a cui appartiene l'ID dell'istanza
ID dell'account di amministr atore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
Nome dell'account	account_name	AWS nome dell'account
Stato dell'account	account_status	stato dell'account AMS
	account_sla	Impegno al servizio dell'acco unt AMS
Tipo di account	malz_role	ruolo MALZ
Nome del gruppo con scalabili tà automatica	nome_istanza	Nome dell'Auto Scaling Group (ASG) che contiene l'istanza

Nome del campo della console	Nome del campo del set di dati	Definizione
ID dell'istanza	instance_id	ID dell' EC2 istanza
Nome dell'istanza	nome_istanza	Nome dell'istanza EC2
Instance Patch Group	instance_patch_group	Nome del gruppo di patch utilizzato per raggruppare le istanze e applicare la stessa finestra di manutenzione
Tipo di gruppo di patch di istanze	instance_patch_group_type	Tipo di gruppo di patch
Tipo di piattaforma di istanza	instance_platform_type	Tipo di sistema operativo (OS)
Nome della piattaforma dell'istanza	instance_platform_name	Nome del sistema operativo (OS)
Stato dell'istanza	instance_state	Stato all'interno del ciclo di vita dell'istanza EC2
Tag di istanza	ec2_tags	I tag associati all'ID dell' EC2 istanza Amazon
Zona di atterraggio	malz_flag	Contrassegna l'account relativo a MALZ
Copertura della finestra di manutenzione	mw_covered_flag	Se un'istanza ha almeno una finestra di manutenzione abilitata con date di esecuzion e future, viene considerata coperta, altrimenti non coperta
Data e ora di esecuzione della finestra di manutenzione	time_window_execution_time	La prossima volta è prevista l'esecuzione della finestra di manutenzione

Nome del campo della console	Nome del campo del set di dati	Definizione
Data e ora di esecuzione della finestra di manutenzione	time_window_execution_time	La prossima volta è prevista l'esecuzione della finestra di manutenzione
Account di produzione	prod_account	Identificatore degli account AMS prod e non prod, a seconda che il nome dell'acco unt includa o meno il valore «PROD», «NONPROD».
Data/ora del rapporto	dataset_datetime	La data e l'ora di generazione del report.
Nome stack	instance_stack_name	Nome dello stack che contiene l'istanza
Tipo di pila	instance_stack_type	Stack AMS (infrastruttura AMS all'interno dell'account del cliente) o Customer stack (infrastruttura gestita da AMS che supporta le applicazioni dei clienti)

Dettagli della patch

Questo rapporto fornisce i dettagli delle patch e la copertura della finestra di manutenzione di varie istanze.

Questo rapporto fornisce:

- Dati sui gruppi di patch e sui relativi tipi.
- Dati sulle finestre di manutenzione, durata, termine ultimo, date future di esecuzione della finestra di manutenzione (pianificazione) e istanze interessate da ciascuna finestra.
- Dati su tutti i sistemi operativi dell'account e numero di istanze in cui il sistema operativo è installato.

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	La data e l'ora di generazione del report.
ID dell'account	aws_account_id	AWS ID dell'account a cui appartiene l'ID dell'istanza
Nome dell'account	account_name	AWS nome dell'account
Stato dell'account	account_status	stato dell'account AMS
Conforme - Critico	comliant_critical	Numero di patch conformi con gravità «critica»
Conforme: elevato	comliant_high	Numero di patch conformi con severità «elevata»
Conforme: medio	comliant_medium	Numero di patch conformi con severità «media»
Conforme: basso	comliant_low	Numero di patch conformi con severità «bassa»
Conforme: informativo	comliant_informativo	Numero di patch conformi con severità «informativa»
Conforme: non specificato	comliant_non specificato	Numero di patch conformi con gravità «non specificata»
Conforme: totale	totale_conforme	Numero di patch conformi (tutte le severità)
Id dell'istanza	instance_id	ID dell' EC2 istanza
Nome dell'istanza	nome_istanza	Nome dell'istanza EC2
	account_sla	Livello di servizio dell'account AMS

Nome del campo	Nome del campo del set di dati	Definizione
Tipo di piattaforma di istanza	instance_platform_type	Tipo di sistema operativo (OS)
Nome della piattaforma dell'istanza	instance_platform_name	Nome del sistema operativo (OS)
Tipo di gruppo di patch di istanze	instance_patch_group_type	PREDEFINITO: gruppo di patch predefinito con finestra di manutenzione predefinita, determinato dal tag:TRUE sull'istanza AMSDefault PatchGroup CLIENTE: gruppo di patch creato dal cliente NOT_ASSIGNED: nessun gruppo di patch assegnato
Gruppo di patch di istanze	instance_patch_group	Nome del gruppo di patch utilizzato per raggruppare le istanze e applicare la stessa finestra di manutenzione
Stato dell'istanza	instance_state	Stato all'interno del ciclo di vita dell'istanza EC2
Tag di istanza	ec2_tags	I tag associati all'ID dell' EC2 istanza Amazon
Finestra di manutenzione dell'ultima esecuzione	last_execution_window	L'ultima volta in cui è stata eseguita la finestra di manutenzione
ID della finestra di manutenzione	window_id	ID finestra di manutenzione

Nome del campo	Nome del campo del set di dati	Definizione
Stato della finestra di manutenzione	window_state	stato della finestra di manutenzione
Tipo di finestra di manutenzione	tipo_finestra	Tipo di finestra di manutenzione
Finestra di manutenzione Data e ora di esecuzione successiva	window_next execution_time	La prossima volta è prevista l'esecuzione della finestra di manutenzione
Durata della finestra di manutenzione (ore)	finestra_duration	La durata della finestra di manutenzione in ore
Copertura della finestra di manutenzione	mw_covered_flag	Se un'istanza ha almeno una finestra di manutenzione abilitata con date di esecuzione future, viene considerata coperta, altrimenti non coperta
Non conforme: critico	noncomliant_critical	Numero di patch non conformi con gravità «critica»
Non conforme: elevato	noncomliant_high	Numero di patch non conformi con gravità «elevata»
Non conforme: medio	noncomliant_medium	Numero di patch non conformi con gravità «media»
Non conforme: basso	non conforme (basso)	Numero di patch non conformi con gravità «bassa»
Non conforme: informativo	non conforme _informativo	Numero di patch non conformi con severità «informativa»

Nome del campo	Nome del campo del set di dati	Definizione
Non conforme: non specificato	non conforme _non specificato	Numero di patch non conformi con gravità «non specificata»
Non conforme: totale	noncomliant_total	Numero di patch non conformi (tutte le severità)
ID di base della patch	patch_baseline_id	Linea di base della patch attualmente associata all'istan za
Stato della patch	patch_status	Stato generale di conformità delle patch. Se manca almeno una patch, l'istanza viene considerata non conforme, altrimenti conforme.
Account di produzione	prod_account	Identificatore degli account AMS prod e non prod, a seconda che il nome dell'acco unt includa o meno il valore «PROD», «NONPROD».
Tipo di pila	instance_stack_type	Stack AMS (infrastruttura AMS all'interno dell'account del cliente) o Customer stack (infrastruttura gestita da AMS che supporta le applicazioni dei clienti)
	window_next_exec_yyyy	Un anno fa parte di window_next_execution_time
	finestra_next_exec_mm	Fa parte del mese di window_next_execution_time

Nome del campo	Nome del campo del set di dati	Definizione
	Window_next_exec_d	Fa parte del giorno di window_next_execution_time
	finestra_successiva _exec_HMI	Ora:parte in minuti di window_next_execution_time

Istanze in cui non sono state apportate le patch

Questo rapporto fornisce dettagli sulle istanze che non hanno ricevuto le patch durante l'ultima finestra di manutenzione.

Questo rapporto fornisce:

- Dati sulle patch mancanti a livello di ID della patch.
- Dati su tutte le istanze con almeno una patch mancante e attributi come la gravità della patch, i giorni senza patch, l'intervallo e la data di rilascio della patch.

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	La data e l'ora di generazione del report
ID dell'account	aws_account_id	AWS ID dell'account a cui appartiene l'ID dell'istanza
Nome dell'account	account_name	AWS nome dell'account
Nome cliente Genitore	customer_name_parent	
Nome cliente	nome_cliente	
Account di produzione	prod_account	Identificatore degli account AMS prod o non prod, a

Nome del campo	Nome del campo del set di dati	Definizione
		seconda che il nome dell'acco unt includa il valore «PROD» o «NONPROD».
Stato dell'account	account_status	stato dell'account AMS
Tipo di account	tipo_conto	
	account_sla	Livello di servizio dell'account AMS
ID dell'istanza	instance_id	ID della tua EC2 istanza
Nome dell'istanza	nome_istanza	Nome della tua istanza EC2
Tipo di piattaforma dell'istanza	instance_platform_type	Tipo di sistema operativo (OS)
Stato dell'istanza	instance_state	Stato all'interno del ciclo di vita dell'istanza EC2
Tag di istanza	ec2_tags	I tag associati all'ID dell' EC2 istanza Amazon
ID della patch	patch_id	ID della patch rilasciata
Severità della patch	patch_sev	Severità della patch per editore
Classificazione delle patch	patch_class	Classificazione delle patch in base all'editore della patch
Data e ora di rilascio della patch (UTC)	release_dt_utc	Data di rilascio della patch per editore
Stato di installazione della patch	install_state	Installa lo stato della patch sull'istanza per SSM

Nome del campo	Nome del campo del set di dati	Definizione
Giorni senza patch	giorni senza patch	Numero di giorni in cui l'istanza è stata priva di patch dall'ultima scansione SSM
Intervallo di giorni senza patch	days_unpatched_bucket	Un sacco di giorni senza patch

Rapporto di Backup (giornaliero)

Il rapporto di backup copre le regioni primarie e secondarie (se applicabile). Copre lo stato dei backup (successo/fallimento) e i dati sulle istantanee scattate.

Questo rapporto fornisce:

- Stato del backup
- Numero di istantanee scattate
- Punto di ripristino
- Informazioni sul piano di backup e sul vault

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	La data e l'ora di generazione del report.
ID dell'account	aws_account_id	ID account AWS a cui appartiene l'ID dell'istanza
ID dell'account amministratore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
Nome dell'account	account_name	Nome dell'account AWS
SLA dell'account	account_sla	Impegno al servizio dell'acco unt AMS

Nome del campo	Nome del campo del set di dati	Definizione
	malz_flag	Contrassegna l'account relativo a MALZ
	malz_role	ruolo MALZ
	restrizioni_accesso	Regioni a cui l'accesso è limitato
Data/ora di inizio pianificata dello snapshot di backup	start_by_dt_utc	Indicatore temporale in cui è pianificato l'inizio dell'ista ntanea
Data/ora di inizio effettiva dell'istantanea di backup	creation_dt_utc	Indicatore temporale in cui l'istantanea inizia effettiva mente
Data/ora di completamento dello snapshot di backup	completion_dt_utc	Timestamp al momento del completamento dell'istantanea
Data/ora di scadenza dello snapshot di backup	expiration_dt_utc	Indicatore temporale alla scadenza dell'istantanea
Stato del Backup Job	backup_job_status	Stato dell'istantanea
Tipo di backup	tipo_backup	Tipo di backup
ID Job di Backup	backup_job_id	L'identificatore univoco del job di backup
Dimensioni di backup in byte	backup_size_in_bytes	La dimensione del backup in byte
Piano di backup ARN	backup_plan_arn	Il piano di backup ARN
ID del piano di backup	backup_plan_id	Identificatore univoco del piano di backup

Nome del campo	Nome del campo del set di dati	Definizione
Nome del piano di backup	nome_piano di backup	Il nome del piano di Backup
Versione del piano di backup	versione del piano di backup	La versione del piano di backup
ID regola di backup	backup_rule_id	L'id della regola di backup
ARN di Backup Vault	backup_vault_arn	ARN del vault di backup
Nome del vault di backup	nome_vault_backup_	Il nome del backup vault
Ruolo IAM ARN	iam_role_arn	Il ruolo IAM (ARN)
Id dell'istanza	instance_id	ID univoco dell'istanza
Stato dell'istanza	instance_state	Stato istanza
Tag di istanza	ec2_tags	I tag associati all'ID dell'istanza EC2
ARN risorsa	resource_arn	Il nome della risorsa Amazon
ID della risorsa	resource_id	L'identificatore univoco della risorsa
Regione delle risorse	resource_region	Le aree primarie (e secondarie, se applicabile) della risorsa.
Tipo di risorsa	tipo_risorsa	Il tipo di risorsa
ARN del punto di ripristino	recovery_point_arn	L'ARN del punto di ripristino
ID del punto di ripristino	recovery_point_id	L'identificatore univoco del punto di ripristino
Stato del punto di ripristino	recovery_point_status	Stato del punto di ripristino

Nome del campo	Nome del campo del set di dati	Definizione
Eliminazione del punto di ripristino dopo giorni	recovery_point_delete_after_days	Eliminazione del punto di ripristino dopo giorni
Il punto di ripristino passa alla conservazione a freddo dopo giorni	recovery_point_move_to_cold_storage_after_days	Numero di giorni dopo la data di completamento in cui lo snapshot di backup viene spostato in cold storage
Stato della crittografia del punto di ripristino	recovery_point_is_encrypted	stato di crittografia del punto di ripristino
Chiave di crittografia del punto di ripristino (ARN)	recovery_point_encryption_key_arn	Chiave di crittografia del punto di ripristino ARN
ID dello stack	stack_id	Identificatore univoco dello stack di Cloudformation
Nome stack	stack_name	Nome stack
Tag: Gruppo di patch predefinito AMS	tag_ams_default_patch_group	Valore del tag: AMS Default Patch Group
Tag: App Id	tag_app_id	Valore del tag: ID app
Tag: nome dell'app	tag_app_name	Valore del tag: nome dell'app
Tag: Backup	tag_backup	Valore del tag: Backup
Tag: Compliance Framework	tag_compliance_framework	Valore del tag: Compliance Framework
Tag: Centro di costo	tag_cost_center	Valore del tag: Centro di costo
Tag: Cliente	tag_cliente	Valore del tag: cliente
Tag: Classificazione dei dati	tag_data_classification	Valore del tag: classificazione dei dati

Nome del campo	Nome del campo del set di dati	Definizione
Tag: Tipo di ambiente	tag_environment_type	Valore del tag: tipo di ambiente
Tag: Orario di apertura	tag_ore_di funzionamento	Valore del tag: ore di funzionamento
Tag: Owner Team	tag_owner_team	Valore del tag: Owner Team
Tag: Email del team del proprietario	tag_owner_team_email	Valore del tag: Owner Team Email
Tag: Patch Group	tag_patch_group	Valore del tag: Patch Group
Tag: Support Priority	tag_support_priority	Valore del tag: Support Priority
Stato del volume	volume_state	Stato del volume

Rapporto sull'incidente (settimanale)

Questo rapporto fornisce l'elenco aggregato degli incidenti insieme alla priorità, alla gravità e allo stato più recente, tra cui:

- Dati sui casi di assistenza classificati come incidenti sull'account gestito
- Informazioni sugli incidenti necessarie per visualizzare le metriche degli incidenti per l'account gestito
- Dati sulle categorie di incidenti e sullo stato di riparazione di ogni incidente

Sia la visualizzazione che i dati sono disponibili per il rapporto settimanale sugli incidenti.

- È possibile accedere alla visualizzazione tramite la console AMS dell'account tramite la pagina Report.
- È possibile accedere al set di dati con lo schema seguente tramite il bucket S3 nell'account gestito.
- Utilizza i campi di data forniti per filtrare gli incidenti in base al mese, trimestre, settimana, and/or giorno in cui l'incidente è stato creato o risolto.

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	La data e l'ora di generazione del report.
ID dell'account	aws_account_id	AWS ID dell'account a cui appartiene l'incidente.
ID dell'account amministratore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
Nome dell'account	account_name	AWS nome dell'account.
ID del caso	case_id	L'ID dell'incidente.
Mese di creazione	created_month	Il mese in cui è stato creato l'incidente.
Priorità	priority	La priorità dell'incidente.
Gravità	severity	La gravità dell'incidente.
Stato	stato	Lo stato dell'incidente.
Categoria	yuma_category	La categoria dell'incidente.
Giorno di creazione	giorno_creato	Il giorno in cui l'incidente è stato creato nel formato. YYYY-MM-DD
Settimana creata	created_wk	La settimana in cui l'inciden te è stato creato nel formato YYYYY-WW. Da domenica a sabato vengono contati come inizio e fine settimana. La settimana va dalla 01 alla 52. La settimana 01 è sempre la settimana che contiene il primo giorno dell'anno

Nome del campo	Nome del campo del set di dati	Definizione
		. Ad esempio, 2023-12-3 1 e 2024-01-01 sono nella settimana 2024-01.
Trimestre creato	created_qtr	Il trimestre in cui l'incidente è stato creato nel formato YYYYY-Q. Dal 01/01 al 31/03 è definito come Q1 e così via.
Giorno risolto	giorno_risolto	Il giorno in cui l'incidente è stato risolto in formato. YYYY-MM-DD
Settimana risolta	resolved_wk	La settimana in cui l'inciden te è stato risolto nel formato YYYYY-WW. Da domenica a sabato vengono contati come inizio e fine settimana. La settimana va dalla 01 alla 52. La settimana 01 è sempre la settimana che contiene il primo giorno dell'anno. Ad esempio, il 2023-12-31 e il 2024-01-01 sono nella settimana 2024-01.
Mese risolto	resolved_month	Il mese in cui l'incidente è stato risolto nel formato YYYY-MM.
Trimestre risolto	resolved_qtr	Il trimestre in cui l'incidente è stato risolto nel formato YYYYY-Q. Dal 01/01 al 31/03 è definito come Q1 e così via.

Nome del campo	Nome del campo del set di dati	Definizione
Regola di raggruppamento creata	grouping_rule	La regola di raggruppamento che si applica all'incidente. O «no_grouping» o «instance _grouping».
Istanza IDs	instance_ids	L'istanza associata all'incid ente.
Numero di avvisi	numero_di_avvisi	Il numero di avvisi associati a quell'incidente. Se hai abilitato il raggruppamento, questo numero può essere maggiore di 1. Se il raggruppamento non è abilitato, sarà sempre 1.
Creato alle	created_at	Il timestamp in cui è stato creato l'incidente.
Allarme ARNs	alarm_arns	L'Amazon Resource Name («arn») degli allarmi associati al tuo incidente.
Allarmi correlati	related_alarms	I nomi leggibili dall'uomo di tutti gli allarmi associati all'incidente.

Rapporto di fatturazione (mensile)

Dettagli sugli addebiti di fatturazione

Questo report fornisce dettagli sugli addebiti di fatturazione di AMS con account collegati e rispettivi servizi AWS.

Questo rapporto fornisce:

- Dati sui costi a livello di servizio AMS, sulle percentuali di upgrade, sui livelli di servizio AMS a livello di account e sulle tariffe AMS.
- Dati sugli account collegati e sui costi di utilizzo di AWS.

> **Important**
>
> Il rapporto di fatturazione mensile è disponibile solo nel tuo account di gestione dei pagamenti (MPA) o nel tuo account di addebito definito. Questi sono gli account a cui viene inviata la fattura mensile AMS. Se non riesci a individuare questi account, contatta il tuo Cloud Service Delivery Manager (CSDM) per ricevere assistenza.

Nome del campo	Nome del campo del set di dati	Definizione
Data di fatturazione	data	Il mese e l'anno del servizio fatturato
ID del conto di pagamento	payer_account_id	L'ID a 12 cifre che identific a l'account responsabile del pagamento degli addebiti AMS
ID dell'account collegato	linked_account_id	L'ID a 12 cifre che identifica l'account AMS che utilizza i servizi che genera espansioni
AWS Nome del servizio	product_name	Il AWS servizio che è stato utilizzato
AWS Addebiti	aws_charges	I AWS costi per il nome del AWS servizio in Service Name AWS
Piano tariffario	piano_tariffario	Il piano tariffario associato all'account collegato

Nome del campo	Nome del campo del set di dati	Definizione
Gruppo di assistenza AMS	tier_uplifting_groups	Codice del gruppo di servizi AMS che determina la percentuale di uplift
Proporzione di sollevamento	uplift_percent	La percentuale di aggiornamento (in formato decimale V.WXYZ) basata su pricing_plan, SLA e service AWS
AWS Addebiti adeguati	adjusted_aws_usage	AWS utilizzo adattato per AMS
Costi aumentati AWS	uplifted_aws_charges	La percentuale degli AWS addebiti da addebitare per AMS; adjusted_aws_charges * uplift_percent
Istanze RDS Spend EC2	instances_ec2_rds_spend	Istanze Spend on e RDS EC2
Costi per istanze riservate	ris_charges	Costi per istanze riservate
Costi aumentati per le istanze riservate	uplifted_ris	La percentuale dei costi delle istanze riservate da addebitare per AMS; ris_charges * uplift_percent
Costi del Savings Plan	sp_charges	SavingsPlan costi di utilizzo
Costi del piano Uplifted Savings Plan	uplifted_sp	La percentuale degli addebiti dei piani di risparmio da addebitare per AMS; sp_charges * uplift_percent
Tariffe AMS	ams_charges	Costi totali ams per il prodotto; uplifted_aws_charges + instance_ec2_rds_spend + uplifted_ris + uplifted_sp

Nome del campo	Nome del campo del set di dati	Definizione
Tariffa minima ripartita proporzionalmente	ripartito_minimo	L'importo che addebitiamo per soddisfare il minimo contrattuale
Costi totali AMS dell'account collegato	linked_account_total ams_charges	Somma di tutti gli addebiti per il linked_account
Costi totali AMS del conto di pagamento	payer_account_total ams_charges	Somma di tutti gli addebiti relativi al conto di pagamento
Tariffa minima	tariffe_minime	Commissioni minime AMS (se applicabile)
Sconto Reserved Instance e Savings Plan	adj_ri_sp_charges	RI/SP discount to be applied against RI/SPaddebiti (applicabili in determinate circostanze)

Rapporti aggregati

I report self-service aggregati (SSR) offrono una visualizzazione dei report self-service esistenti aggregati a livello di organizzazione, su più account. Questo vi offre visibilità sulle principali metriche operative, come la conformità delle patch, la copertura dei backup e gli incidenti, su tutti gli account gestiti da AMS all'interno della vostra azienda. AWS Organizations

L'SSR aggregato è disponibile in tutte le attività commerciali in Regioni AWS cui è disponibile AWS Managed Services. Per un elenco completo delle regioni disponibili, consulta la tabella delle regioni.

Abilita i report aggregati

È necessario gestire l'SSR aggregato da un account di gestione. AWS Organizations L'account di gestione è l' AWS account che hai usato per creare la tua organizzazione.

Per abilitare l'SSR aggregato per un account di AWS Organizations gestione integrato in AMS, accedi alla console AMS e vai a Reports. Seleziona Organization Access nell' top-right-handangolo per aprire il riquadro AWS Managed Services Console: Organization View. Da questo riquadro, puoi gestire la funzionalità Aggregated SSR.

AWS Organizations gli account di gestione che non sono integrati in AMS non hanno accesso alla console AMS. Per abilitare Aggregated SSR per un account di AWS Organizations gestione non registrato su AMS, esegui prima l'autenticazione sul tuo Account AWS, quindi accedi alla AWS console e cerca Managed Services. Si apre la pagina AMS Marketing. In questa pagina, seleziona il link Organization Access nella barra di navigazione per aprire la console AWS Managed Services: Organization View, dove puoi gestire la funzionalità Aggregated SSR.

La prima volta che accedi alla console AWS Managed Services: Organization View, completa i seguenti passaggi:

1. Se non l'hai già configurata AWS Organizations, scegli Abilita AWS Organizations dalla tua console. Per ulteriori informazioni sulla configurazione AWS Organizations, consulta la Guida AWS Organizations per l'utente. Puoi saltare questo passaggio se lo usi AWS Organizations già.
2. Per abilitare il servizio Aggregated Self-Service Reporting, seleziona Abilita accesso affidabile sulla console.
3. (Facoltativo) Registra un amministratore delegato per avere accesso in lettura alla visualizzazione organizzativa.

Visualizza i report aggregati come amministratore delegato

Un amministratore delegato è l'account scelto per l'accesso in lettura ai report aggregati. L'amministratore delegato deve essere un account registrato su AMS ed essere l'unico account con accesso in lettura ai report aggregati.

Per scegliere un amministratore delegato, inserisci l'ID dell'account nel passaggio 3 nella Console AWS Managed Services: Organization View. Puoi avere un solo account amministratore delegato registrato alla volta. Tieni presente che l'account amministratore delegato deve essere un account gestito da AMS.

Per aggiornare un account amministratore delegato, accedi alla Console AWS Managed Services: Organization View e seleziona Rimuovi l'amministratore delegato. La console richiede di inserire un nuovo ID account per registrarti come amministratore delegato.

Leggi i report aggregati

Se non registri un amministratore delegato e il tuo account di AWS Organizations gestione viene inserito in AMS, per impostazione predefinita l'account di AWS Organizations gestione ottiene l'accesso in lettura ai report aggregati. Se l'account di AWS Organizations gestione non è gestito da AMS, devi scegliere un account amministratore delegato per avere accesso in lettura ai report aggregati.

In qualsiasi momento, solo un singolo account inserito in AMS ha accesso in lettura ai report aggregati, sia l'account di AWS Organizations gestione che l'amministratore delegato registrato. Tutti gli altri account membri all'interno dell'organizzazione (e inseriti in AMS) hanno ancora accesso solo ai report relativi a un singolo account per ogni singolo account.

Dopo aver abilitato l'SSR aggregato, accedi ai tuoi Rapporti. Tutti i report self-service esistenti sono elencati in questa sezione e un tag blu indica che sono stati aggregati. Tieni presente che devi accedere alla console AMS dall'account che hai scelto per avere accesso in lettura ai report aggregati. Si tratta dell'account di AWS Organizations gestione o dell'account amministratore delegato.

Dopo aver abilitato l'SSR aggregato, i report aggregati sono disponibili a partire dal ciclo di rendicontazione successivo.

Disattiva i report aggregati

Per disabilitare Aggregated SSR, apri la Console AWS Managed Services: Organization View. Seleziona Disabilita l'accesso affidabile. Dopo aver disabilitato l'accesso affidabile per Aggregated SSR, i report self-service AMS smettono di essere aggregati a livello di organizzazione, tra gli account. Tieni inoltre presente che la disattivazione ha effetto a partire dal successivo ciclo di segnalazione.

Dopo aver disabilitato l'SSR aggregato, è necessario attendere che i report nella console AMS vengano visualizzati come report per account singolo. Questo ritardo si verifica perché la disattivazione della funzionalità ha effetto a partire dal ciclo di segnalazione successivo.

Dashboard di report self-service AMS

I report self-service AMS offrono due dashboard: e. Dashboard Resource Tagger Dashboard Security Config Rules

Dashboard Resource Tagger

La dashboard di AMS Resource Tagger fornisce informazioni dettagliate sulle risorse supportate da Resource Tagger, nonché sullo stato attuale dei tag che Resource Tagger è configurato per applicare a tali risorse.

Copertura di Resource Tagger per tipo di risorsa

Questo set di dati è costituito da un elenco di risorse con tag gestiti da Resource Tagger.

La copertura delle risorse per tipo di risorsa viene visualizzata come quattro grafici a linee che descrivono le seguenti metriche:

- Numero di risorse: il numero totale di risorse nella regione, per tipo di risorsa.
- Risorse con tag gestiti mancanti: il numero totale di risorse nella regione, per tipo di risorsa, che richiedono tag gestiti ma non sono etichettate da Resource Tagger.
- Risorse non gestite: il numero totale di risorse nella regione, per tipo di risorsa, a cui non sono stati applicati tag gestiti da Resource Tagger. Ciò significa in genere che queste risorse non corrispondono a nessuna configurazione di Resource Tagger o sono esplicitamente escluse dalle configurazioni.
- Risorse gestite: analoga alla metrica delle risorse non gestite (Resource Count - Unmanaged Resources).

La tabella seguente elenca i dati forniti da questo rapporto.

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	Data e ora di generazione del report (ora UTC)
Account AWS ID	aws_account_id	Account AWS ID
ID account amministratore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
Regione	Regione	Regione AWS

Nome del campo	Nome del campo del set di dati	Definizione
Tipo di risorsa	tipo_risorsa	Questo campo identifica il tipo di risorsa. Sono inclusi solo i tipi di risorse supportati da Resource Tagger.
Numero di risorse	resource_count	Numero di risorse (del tipo di risorsa specificato) distribuite in questa regione.
ResourcesMissingManagedTags	resource_missing_managed_tags_count	Numero di risorse (del tipo di risorsa specificato) che richiedono tag gestiti, in base ai profili di configurazione, ma non sono ancora state taggate da Resource Tagger.
UnmanagedResources	unmanaged_resource_count	Numero di risorse (del tipo di risorsa specificato) senza tag gestiti applicati da Resource Tagger. In genere, queste risorse non corrispondono a nessun blocco di configurazione di Resource Tagger o sono esplicitamente escluse dai blocchi di configurazione.

Conformità alle regole di configurazione Resource Tagger

Questo set di dati è costituito da un elenco di risorse in un Regione AWS determinato tipo di risorsa a cui è applicato un determinato profilo di configurazione. Viene visualizzato come un grafico a linee.

La tabella seguente elenca i dati forniti da questo rapporto.

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	Data e ora di generazione del report (ora UTC)
Account AWS ID	aws_account_id	Account AWS ID
ID account amministratore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
Regione	Regione	Regione AWS
Tipo di risorsa	tipo_risorsa	Questo campo identifica il tipo di risorsa. Sono inclusi solo i tipi di risorse supportati da Resource Tagger.
ID del profilo di configurazione	configuration_profile_id	L'ID del profilo di configurazione Resource Tagger. Un profilo di configurazione viene utilizzato per definire le politiche e le regole utilizzate per etichettare le risorse.
MatchingResourceCount	resource_count	Numero di risorse (del tipo di risorsa specificato) che corrispondono all'ID del profilo di configurazione Resource Tagger. Affinché una risorsa corrisponda al profilo di configurazione, il profilo deve essere abilitato e la risorsa deve corrispondere alla regola del profilo.

Risorse non conformi a Resource Tagger

Questo set di dati è costituito da un elenco di risorse non conformi per una singola configurazione di Resource Tagger. Questi dati sono un'istantanea quotidiana della conformità delle risorse e mostrano lo stato delle risorse dei clienti nel momento in cui questi report vengono consegnati agli account dei clienti (non è disponibile una visualizzazione storica). Viene visualizzato come una tabella pivot composta da risorse non conformi a una determinata configurazione.

La tabella seguente elenca i dati forniti da questo rapporto.

Nome del campo	Nome del campo del set di dati	Definizione
Data/ora del rapporto	dataset_datetime	Data e ora di generazione del report (ora UTC)
Account AWS ID	aws_account_id	Account AWS ID
ID account amministratore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
Regione	Regione	Regione AWS
Tipo di risorsa	tipo_risorsa	Questo campo identifica il tipo di risorsa. Sono inclusi solo i tipi di risorse supportati da Resource Tagger.
ID risorsa	resource_id	L'identificatore univoco per le risorse supportate da Resource Tagger.
Stato di copertura	coverage_state	Questo campo indica se la risorsa è etichettata come configurato dall'ID di configura zione Resource Tagger.
ID del profilo di configurazione	configuration_profile_id	L'ID del profilo di configura zione Resource Tagger. Un profilo di configurazione

Nome del campo	Nome del campo del set di dati	Definizione
		viene utilizzato per definire le politiche e le regole utilizzate per etichettare le risorse.

Dashboard Security Config Rules

Il Security Config Rules Dashboard fornisce una panoramica approfondita sulla conformità delle risorse e delle regole degli AWS Config account AMS. Puoi filtrare il rapporto in base alla gravità della regola per dare priorità ai risultati più critici. La tabella seguente elenca i dati forniti da questo rapporto.

Nome del campo	Nome del campo del set di dati	Definizione
Account AWS ID	Account AWS ID	L'ID dell'account legato alle risorse correlate.
ID dell'account amministratore	aws_admin_account_id	Account affidabile abilitato da te. AWS Organizations
rapporto data/ora	Data del rapporto	La data e l'ora di generazione del rapporto.
nome_cliente	Nome del cliente	Il nome del cliente.
account_name	Nome dell'account	Il nome associato all'ID dell'account
resource_id	ID risorsa	Un identificatore per una risorsa.
resource_region	Regione delle risorse	La posizione Regione AWS in cui si trova la risorsa.

Nome del campo	Nome del campo del set di dati	Definizione
tipo_risorsa	Tipo di risorsa	Il Servizio AWS tipo di risorsa or.
nome_risorsa	Nome risorsa	Il nome della risorsa.
resource_ams_flag	Bandiera AMS di risorsa	Se la risorsa è di proprietà di AMS, questo flag è impostato su TRUE. Se la risorsa è di proprietà del cliente, questo flag è impostato su FALSE. Se la proprietà non è nota, questo flag è impostato su UNKNOWN.
config_rule	Regola di configurazione	Il nome non personalizzabile per la regola di configurazione.
config_rule_description	Descrizione della regola di Config	Una descrizione della regola di configurazione.
source_identifier	Identificatore di origine	Un identificatore univoco per la regola di configurazione gestita e nessun identificatore per una regola di configura zione personalizzata.
compliance_flag	Bandiera di conformità	Mostra se le risorse sono conformi o non conformi alle regole di configurazione.
tipo_regola	Tipo di regola	Indica se la regola è predefini ta o creata su misura.

Nome del campo	Nome del campo del set di dati	Definizione
eccezione_flag	Bandiera di eccezione	Il flag di eccezione della risorsa mostra l'accettazione del rischio nei confronti di una risorsa non conforme. Se il contrassegno di eccezione della risorsa è TRUE per una risorsa, la risorsa viene esentata. Se il flag di eccezione è NULL, la risorsa non è esentata.
cal_dt	Data	La data di valutazione della regola.
descrizione_riparazione	Descrizione della riparazione	Una descrizione di come porre rimedio alla conformità alle regole.
severity	Gravità	La severità delle regole di configurazione indica l'impatto della non conformità.
azione_cliente	Azione del cliente	Azioni necessarie per porre rimedio a questa regola.
raccomandazione	Raccomandazione	Una descrizione di ciò che verifica la regola di configura zione.
categoria_di riparazione	Categoria di riparazione	Le azioni predefinite che AMS intraprende quando questa regola diventa non conforme.

Policy di conservazione dei dati

AMS SSR applica una politica di conservazione dei dati per rapporto. Dopo il periodo di riferimento, i dati vengono cancellati e non sono più disponibili.

Nome del rapporto	Console SSR per la conservazione dei dati	Bucket SSR S3 per la conservazione dei dati
Riepilogo dei dettagli dell'istanza (Patch Orchestrator)	2 mesi	2 anni
Dettagli della patch	2 mesi	2 anni
Istanze in cui non sono state apportate le patch durante l'esecuzione della finestra di manutenzione	2 mesi	2 anni
Dettagli sulle spese di fatturazione AMS	2 anni	2 anni
Report di Backup giornaliero	1 mese	2 anni
Rapporto settimanale sugli incidenti	2 mesi	2 anni
Dashboard delle regole di configurazione di sicurezza	3 mesi	2 anni
Dashboard Resource Tagger	1 anno	2 anni

Fuori bordo da SSR

Per abbandonare il servizio SSR, crea una richiesta di servizio (SR) tramite la console AMS. Dopo aver inviato il SR, un tecnico operativo AMS ti aiuterà a uscire dall'SSR. Nella SR, indica il motivo per cui desideri abbandonare l'imbarco.

Per trasferire un account ed eseguire una pulizia delle risorse, crea un SR tramite la console AMS. Dopo aver inviato il SR, un tecnico operativo AMS ti aiuterà a eliminare il bucket SSR Amazon S3.

Se esci da AMS, vieni automaticamente espulso dalla console AMS SSR. AMS interrompe automaticamente l'invio di dati al tuo account. AMS elimina il bucket SSR S3 come parte del processo di offboarding.

Segnalazioni di incidenti, richieste di assistenza e domande di fatturazione in AMS

Argomenti

Con AWS Managed Services (AMS), puoi richiedere assistenza per problemi e richieste operativi in qualsiasi momento tramite la console AMS. I tecnici operativi AMS sono disponibili per rispondere agli incidenti e alle richieste di assistenza 24 ore su 24, 7 giorni su 7, con tempi di risposta Service Level Agreements (SLAs) e Service Level Objectives (SLOs), a seconda dell'account Service Tier (Plus, Premium) selezionato. I tecnici operativi AMS ti informano in modo proattivo di avvisi e domande importanti utilizzando gli stessi meccanismi.

Gestione degli incidenti

Argomenti

Gli incidenti sono problemi di Servizio AWS prestazioni che influiscono sull'ambiente gestito, come stabilito da AWS Managed Services (AMS) o da te. Gli incidenti identificati dal team AMS vengono inizialmente percepiti come «eventi»: un cambiamento nello stato del sistema rilevato dal monitoraggio. Se viene superata una soglia configurata, l'evento attiva un allarme, chiamato anche avviso. Il team operativo AMS determina se l'evento non ha alcun impatto, se si tratta di un incidente (interruzione o deterioramento del servizio) o se è un problema (la causa principale di uno o più incidenti risolti).

Il team AMS riceve anche gli incidenti identificati da te tramite il Supporto centro o in modo programmatico utilizzando l'API AWS Support con il codice del servizio. `sentinel-report-incident`

Una volta ricevuto dal team operativo AMS, l'incidente viene esaminato per garantire che non sia meglio classificato come richiesta di servizio. Se deve essere classificato come richiesta di servizio, viene immediatamente riclassificato e il team di richiesta di assistenza AMS prende il sopravvento e l'utente riceve una notifica. Se l'incidente può essere risolto dall'operatore ricevente, vengono prese le misure necessarie per risolverlo immediatamente. Gli operatori AMS consultano la documentazione interna per una risoluzione e, se necessario, inoltrano l'incidente ad altre risorse di supporto fino alla risoluzione dell'incidente. Per rimanere informati su ogni fase del processo di risoluzione degli incidenti, assicurati di compilare l'opzione CC Emails e, se intendi connetterti tramite federazione, accedi prima di seguire il link contenuto nell'e-mail inviata da AMS. Una volta risolto, il team operativo AMS documenta l'incidente e la risoluzione per usi futuri.

Se la risoluzione di un incidente richiede modifiche all'infrastruttura, potrebbe essere necessaria una revisione della sicurezza. Le modifiche all'infrastruttura che potrebbero richiedere una revisione della sicurezza includono quelle relative a IAM, alle politiche basate sulle risorse o all'approvazione dei rischi. Questi tipi di incidenti richiedono che un tecnico AMS Operations crei una RFC prima di apportare la modifica ed è necessaria l'approvazione di tale RFC da parte dell'utente. Ad esempio, se la risoluzione degli incidenti richiede l'aggiornamento di una policy IAM, verrà effettuata una revisione della sicurezza AMS e quindi un tecnico AMS Operations creerà una RFC con il tipo Management | Advanced stack components | Identity and Access Management (IAM) and Access Management (IAM) | Update entity o policy change (ct-27tuth19k52b4) e aspetterà l'approvazione della RFC prima di procedere.

> **Note**
>
> AMS ora consente la risoluzione degli incidenti che richiedono modifiche all'infrastruttura senza la fase aggiuntiva dell'approvazione RFC. Se le modifiche necessarie per risolvere l'incidente NON richiedono una revisione di sicurezza (la modifica non è correlata a IAM, alla politica basata sulle risorse o all'approvazione del rischio), AMS può apportare le modifiche in base all'approvazione ricevuta nell'incidente, senza bisogno di un'approvazione separata in una RFC.

Per le definizioni dei termini di gestione degli incidenti, consulta i Termini chiave di AMS.

Per comprendere il percorso di crescita degli incidenti, consulta Ottenere assistenza.

Per una descrizione della risposta di AMS agli incidenti, consulta AMS Incident Response.

Cos'è la gestione degli incidenti?

La gestione degli incidenti è il processo utilizzato da AMS per registrare, intervenire, comunicare lo stato di avanzamento e fornire la notifica degli incidenti attivi.

L'obiettivo del processo di gestione degli incidenti è garantire che il normale funzionamento del servizio gestito venga ripristinato il più rapidamente possibile, l'impatto aziendale sia ridotto al minimo e tutte le parti interessate siano tenute informate.

Alcuni esempi di incidenti includono (ma non sono limitati a) la perdita o il deterioramento della connettività di rete, un processo o un'API che non rispondono o un'attività pianificata che non viene eseguita (ad esempio, un backup fallito).

L'immagine seguente mostra il flusso di lavoro di un incidente segnalato dall'utente ad AMS.

Questo grafico mostra il flusso di lavoro di un incidente segnalato da AMS all'utente.

Priorità dell'incidente

Gli incidenti creati nel centro di supporto AWS, nella console o nell'API Support (SAPI) hanno classificazioni diverse rispetto agli incidenti creati nella console AMS.

- Basso: le funzioni non critiche del servizio o dell'applicazione aziendale relative alle risorse AWS o AMS ne risentono.
- Medio: un servizio o un'applicazione aziendale relativi alle risorse AWS and/or AMS subisce un impatto moderato e funziona in uno stato degradato.
- Alto: la tua azienda ne risente in modo significativo. Le funzioni critiche dell'applicazione relative alle risorse AWS and/or AMS non sono disponibili. Riservato alle interruzioni più critiche che interessano i sistemi di produzione.

> **Note**
>
> La console AWS Support offre cinque livelli di priorità degli incidenti che traduciamo nei tre livelli AMS.

Problema vs incidente

Quando AMS ritiene che un incidente riveli un difetto o una configurazione errata più grave e possa ripresentarsi, viene considerato un problema e non un semplice incidente. In questi casi, AMS analizza il problema e offre suggerimenti per risolverlo.

Impegni del servizio di gestione degli incidenti

Impegni del servizio di gestione degli incidenti

Evento o azione	Misurazione dell'impegno nel servizio
Caso 1: viene generato un evento con un impatto noto. AMS apre un incidente e ti informa. Caso 2: AMS ti contatta per confermare l'impatto dell'evento. Confermi che l'evento è un incidente. Caso 3: si nota un problema e si invia una segnalazione sull'incidente.	L'orologio per la risposta e la risoluzione degli incidenti inizia quando: Caso 1: AMS crea un incidente. Caso 2: confermi che l'avviso è un incidente. Caso 3: si segnala un incidente. Gli impegni di servizio dipendono dalla priorità dell'incidente creato.
Se invii l'incidente, AMS invia una risposta per confermarlo. Se AMS crea l'incidente per tuo conto, non viene inviata una risposta all'incidente separata.	Il tempo per la risoluzione degli incidenti continua a ticchettare. L'orologio per il tempo di risposta all'incidente si interrompe quando AMS invia la conferma dell'incidente. **Note** Il tempo impiegato in attesa dei vostri input è escluso dai calcoli dei tempi di risoluzione degli incidenti. Per gli incidenti creati da AMS, il tempo di risposta iniziale è il momento della

Evento o azione	Misurazione dell'impegno nel servizio
	creazione della notifica iniziale dell'inci dente all'utente.
Per le risorse e i servizi in questione, AMS verifica lo stato di salute per verificare se: • L'evento rilevato da AMS o l'incidente inviato dal cliente si qualifica come incidente e • all'incidente viene assegnata correttamente la priorità, e Se a un incidente inviato non viene assegnata correttamente la priorità, AMS riassegna la priorità. Se AMS modifica la priorità di un incidente, ti viene inviata una notifica insieme alle motivazioni alla base della modifica della priorità. In alcuni casi, un problema che hai segnalato potrebbe non essere considerato un incidente, a seconda della causa. In questi casi, AMS chiude l'incidente e ti invia una notifica spiegandone il motivo. Indipendentemente dalla classificazione degli eventi, AMS collabora con voi per assistervi se necessario. Per comprendere le regole per la categoriz zazione degli incidenti, consulta. Priorità dell'incidente	Nel caso in cui la priorità dell'incidente cambi, è applicabile l'impegno di servizio per la nuova priorità; il tempo continua a scorrere. Nei casi in cui un incidente viene chiuso perché non soddisfa la definizione di incidente, gli impegni di servizio non sono applicabili; il tempo si ferma.

Evento o azione	Misurazione dell'impegno nel servizio
AMS lavora sull'incidente per risolverlo nel rispetto degli impegni di servizio. In alcuni casi, se AMS stabilisce che gli stack o le risorse non disponibili non possono essere risolti tempestivamente, AMS offrirà Infrastru cture Restore come opzione di risoluzione. Infrastructure Restore prevede la ridistribuzione degli stack esistenti, in base ai modelli degli stack interessati, e l'avvio di un ripristino dei dati basato sull'ultimo punto di ripristino noto (snapshot EBS/RDS), se non diversamente specificato dall'utente. I dati temporanei sulle singole istanze andranno persi. EC2 Se non autorizzi un ripristino dell'infrastruttura come consigliato da AWS, non avrai diritto a un credito di servizio per l'Incident Resolution Time Service Commitment associato.	L'orologio si ferma quando: • AMS ha ripristinato tutti i servizi o le risorse non disponibili relativi a quell'Incidente allo stato disponibile, oppure • viene avviato un ripristino dell'infrastruttura.
A volte, AMS necessita di chiarimenti da parte dell'utente o di un'attività da parte del cliente per portare avanti le iniziative di risoluzione degli incidenti, a meno che non si disponga di un'azione predefinita e approvata. Di conseguenza, vi è una comunicazione tra AMS e l'utente al fine di risolvere gli incidenti	L'orologio si interrompe quando: AMS è in attesa di una risposta o di un'azione da parte tua. L'orologio si riavvia quando: AMS riceve la risposta da te o l'azione richiesta da AMS è completata.

> **Note**
>
> Per un elenco completo degli impegni di servizio, scarica l'AMS Service Level Agreement.

Esempi di gestione degli incidenti

Esempi di gestione degli incidenti.

Argomenti

I seguenti esempi descrivono l'utilizzo della console AMS per inviare un incidente. Una volta inviato, il team AMS collabora con voi per risolvere l'incidente in base al Service Level Agreement (SLA).

Test degli incidenti

Quando testiamo gli incidenti inviati da AMS, ti chiediamo di includere nel testo dell'oggetto questo contrassegno:. AMSTestNoOpsActionRequired Questo flag indica ad AMS che la segnalazione dell'incidente è solo a scopo di test. Quando i tecnici operativi di AMS vedono quella bandiera, non risponderanno in alcun modo alla segnalazione dell'incidente.

Segnalazione di incidenti

Utilizza 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 chiamate telefoniche 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 che non sono ancora stati 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. Scegli 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 Incidenti.

YouTube Video: Come posso segnalare un incidente dalla console AWS Managed Services?

Monitoraggio e aggiornamento degli incidenti

È possibile aggiornare, monitorare ed esaminare i report sugli incidenti e le richieste di assistenza, entrambi denominati casi, utilizzando la console AMS o a livello di codice utilizzando l'API. Supporto Per informazioni sull'utilizzo dell' Supporto API, consulta `DescribeCases`operazione.

Per monitorare un caso, un incidente o una richiesta di assistenza, utilizzando la console AMS, segui questi passaggi.

1. Nella dashboard dei report sugli incidenti o delle richieste di assistenza della console AMS, accedi a un caso e scegli l'oggetto per aprire una pagina di dettagli con lo stato attuale e le corrispondenze.

   Quando un incidente segnalato o un caso di richiesta di assistenza viene aggiornato dal team operativo AMS, ricevi un'e-mail e un link all'incidente nella console AMS in modo da poter rispondere. Non puoi rispondere alla corrispondenza relativa all'incidente rispondendo all'e-mail.

   > **Important**
   >
   > È necessario aver inserito un indirizzo e-mail per ricevere notifiche di cambio di stato per una richiesta di servizio o un caso imprevisto. Le notifiche vengono inviate solo all'indirizzo e-mail aggiunto al caso al momento della creazione.

Il collegamento contenuto nell'e-mail di notifica non funzionerà a meno che non si utilizzi un server di posta elettronica sulla rete federata AMS. Tuttavia, puoi rispondere alla corrispondenza accedendo alla tua console AMS e utilizzando la pagina dei dettagli del caso.

2. Se nell'elenco sono presenti molti casi, puoi utilizzare l'opzione Filtro:
   - Tutti aperti (impostazione predefinita): utilizza questo filtro per visualizzare tutti i casi che non sono stati risolti.
   - Non assegnato: da utilizzare se hai appena inviato il caso e non hai ricevuto alcuna notifica che lo stato del caso è cambiato. Tieni presente che gli incidenti e i casi di richiesta di assistenza vengono risolti con rapidità diversa a seconda della priorità inviata (incidenti) o del contratto sul livello di servizio (richieste di assistenza).
   - Aperto: utilizza questa opzione se hai ricevuto una notifica che indica che il caso è in sospeso da Amazon; ciò significa che il caso è stato assegnato ma il lavoro non è ancora iniziato.
   - Riaperto: utilizza questa opzione se hai ricevuto la notifica che il caso è stato riaperto dopo essere stato risolto.
   - Lavori in corso: utilizza se hai ricevuto la notifica che un operatore ha iniziato a lavorare sul caso.
   - Intervento in sospeso da parte del cliente: utilizza questa opzione se hai ricevuto una richiesta di intervento da parte tua da parte di un operatore.
   - Azione del cliente completata: utilizza questa opzione se hai ricevuto una notifica che la tua azione sul caso è stata elaborata.
   - Risolto: utilizza per visualizzare i casi che sai essere stati risolti. I casi risolti vengono conservati nella cronologia per dodici mesi.
   - Qualsiasi stato: utilizza questo filtro per visualizzare tutti i casi, indipendentemente dallo stato.
3. Per verificare lo stato più recente, aggiorna la pagina.
4. Se le corrispondenze sono così numerose che non compaiono tutte nella pagina, scegli Carica altro.
5. Per aggiornare lo stato del caso, scegli Rispondi, inserisci la nuova corrispondenza, quindi scegli Invia.
6. Per chiudere il caso dopo che è stato risolto in modo soddisfacente, scegli Chiudi caso.

   Assicurati di assegnare al servizio una valutazione da 1 a 5 stelle per far sapere ad AMS come stiamo!

Gestione degli incidenti con l'API AWS Support

L'API AWS Support ti consente di creare incidenti e aggiungere corrispondenza durante le indagini sui problemi e le interazioni con lo staff di AWS Support. L'API AWS Support modella gran parte del comportamento dell'AWS Support Center. Per ulteriori dettagli su come utilizzare questo servizio di supporto AWS, consulta Programming an AWS Support Case.

> **Note**
>
> Quando usi l'API AWS Support, o SAPI, per gli incidenti AMS Advanced, usa questo codice di servizio:. `sentinel-report-incident`

Risposta agli incidenti generati da AMS

AMS monitora in modo proattivo le tue risorse; per ulteriori informazioni, consulta Monitoraggio e gestione degli eventi. A volte AMS identifica e crea un caso di incidente, il più delle volte per avvisare l'utente di un incidente. Nel caso in cui sia necessaria un'azione da parte dell'utente per risolvere un incidente, AMS invia una notifica alle informazioni di contatto fornite per l'account. Rispondi a questo incidente nello stesso modo in cui risponderesti a qualsiasi altro incidente. Di solito rispondi agli incidenti tramite la console AMS; in alcuni casi è necessario il contatto via e-mail o telefono.

> **Note**
>
> AMS invia le comunicazioni al tuo indirizzo e-mail principale sul tuo account AWS; ti consigliamo di aggiungere un alias email di contatto Operations alternativo per facilitare il processo di gestione degli incidenti. Questo è coperto durante il processo di onboarding di AMS e la relativa documentazione di onboarding. Se hai fornito ad AMS contatti non basati sulle risorse (di cui hai informato il CSDM) durante l'onboarding, tali contatti vengono utilizzati. Ad esempio, potresti fornire un elenco di contatti denominati "SecurityContacts" da utilizzare per incidenti o notifiche CSDMs/CAs relativi alla sicurezza. I tag di contatto presenti sull'utente instances/resources vengono utilizzati per gli incidenti generati da AMS, se l'utente ha fornito il consenso al CSDM per l'utilizzo delle informazioni sui tag.
> Per ulteriori informazioni su questo servizio di notifica, consulta Notifiche.

Gestione delle richieste di assistenza

Argomenti

Le richieste di assistenza sono comunicazioni ad AMS create dall'utente per chiedere informazioni o consigli. Un buon esempio di richiesta di assistenza standard è la guida o l'assistenza nella configurazione di un servizio AMS, come Alarm Manager, Patch Orchestrator e così via. È inoltre possibile ricevere richieste di assistenza da AMS, denominate richieste di servizio in uscita o notifiche di servizio. Per visualizzare un elenco delle richieste di servizio e delle richieste di servizio in uscita (notifiche di servizio) inviate da AMS, consulta la pagina Richieste di assistenza della console AMS.

Per ulteriori informazioni sulle richieste di assistenza in uscita, consulta. Risposta a una richiesta di assistenza generata da AMS

Puoi creare una richiesta di servizio AWS Managed Services (AMS) utilizzando la console AMS o, a livello di codice, utilizzando l' Supporto API. Per i dettagli sull'utilizzo dell'API, consulta Supporto API. Per AMS scegli il codice `sentinel-service-request` di servizio.

Una volta ricevuta la richiesta di assistenza dal team operativo AMS, viene assegnata una priorità in base al contratto sul livello di servizio stipulato. Per rimanere informati su ogni fase del processo di risoluzione delle richieste di assistenza, assicurati di compilare l'opzione CC Emails e, se intendi connetterti tramite federazione, accedi prima di seguire il link contenuto nell'e-mail inviata da AMS.

Utilizzate la pagina Create Service Request della console AMS per eseguire le seguenti attività:

- Creare e aggiornare una richiesta di assistenza
- Ottieni un elenco e informazioni dettagliate su tutte le tue attuali richieste di assistenza
- Restringi la ricerca delle richieste di servizio in base alle date e agli identificatori degli incidenti, comprese le richieste che sono state risolte

- Aggiungi comunicazioni e file allegati alle tue richieste e aggiungi destinatari e-mail per la corrispondenza dei casi
- Risolvi le richieste di assistenza
- Valuta le comunicazioni relative alle richieste di assistenza

Quando utilizzare una richiesta di assistenza

Gli esempi seguenti descrivono una richiesta di assistenza:

- AMS o linee guida AWS generali
- Domande relative a Patch MW
- Domande relative alla pianificazione del backup
- Domande sulla funzionalità dei AWS servizi

Di seguito sono riportati alcuni esempi di ciò che non dovrebbe essere indicato in una richiesta di servizio:

- Problemi di accesso
- Errore nella patch
- Errore di backup
- Errore RFC o RFC che causa l'interruzione dell'attività (Use Incident for business interruption)
- Domande RFC o input aggiuntivi o modifica dell'ambito RFC (utilizzare la corrispondenza bidirezionale RFC)

Come funziona la gestione delle richieste di assistenza

Le richieste di assistenza vengono gestite dal team operativo AMS disponibile su richiesta.

Dopo che la richiesta di assistenza è stata ricevuta dal team operativo AMS, viene esaminata per garantire che non venga classificata più correttamente come incidente. Se deve essere classificato come incidente, viene immediatamente riclassificato, il team di gestione degli incidenti di AMS prende il sopravvento e tu ricevi una notifica.

Se la richiesta di assistenza può essere risolta con l'invio di una RFC, l'operatore incaricato della revisione ti invia un'e-mail in cui ti richiede di inviare la RFC appropriata (vengono forniti i dettagli).

Se l'operatore AMS è in grado di risolvere la richiesta di assistenza, le misure necessarie vengono prese immediatamente. Ad esempio, se la richiesta di assistenza riguarda consigli di architettura o altre informazioni, l'operatore indirizza l'utente alle risorse appropriate o risponde direttamente alla domanda.

Se l'analisi della richiesta di servizio identifica un bug o una richiesta di funzionalità, AMS invia all'utente una notifica tramite la richiesta di servizio. Poiché non esiste un ETA per le richieste di funzionalità o la correzione di bug, la richiesta di servizio originale viene chiusa. Contatta il tuo CSDM per domande di follow-up relative alla richiesta di servizio originale.

Se la richiesta di servizio non rientra nell'ambito delle operazioni di AMS, l'operatore invia la richiesta al vostro responsabile della fornitura dei servizi cloud, in modo che possa comunicare con voi, oppure al team AWS operativo appropriato, inviandovi un'e-mail con le informazioni sulle misure da intraprendere.

La richiesta di assistenza non viene risolta finché non avrai dichiarato di essere soddisfatto del risultato.

> **Note**
>
> Ti consigliamo di fornire un indirizzo email, un nome e un numero di telefono di contatto in tutti i casi per facilitare le comunicazioni.

Test di una richiesta di servizio in AMS

Quando testate le richieste di assistenza AMS, vi chiediamo di includere nel testo dell'oggetto questo contrassegno: AMSTestNoOpsActionRequiredper far sapere ad AMS che la richiesta di servizio è solo a scopo di test. Quando i tecnici operativi di AMS vedono quel segnale, non rispondono alla richiesta di assistenza.

Creazione di una richiesta di servizio in AMS

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. Scegli 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 domande relative alla fatturazione, crea un caso di richiesta di assistenza dalla console di Support Center.

YouTube Video: Come e quando inviare richieste di assistenza dalla console AWS e quali sono gli obiettivi del livello di servizio?

Monitoraggio e aggiornamento delle richieste di servizio in AMS

È possibile aggiornare, monitorare ed esaminare i report sugli incidenti e le richieste di assistenza, in entrambi i casi, utilizzando la console AMS o utilizzando l' Supporto API a livello di codice. Per informazioni sull'utilizzo dell' Supporto API, consulta `DescribeCases`operazione.

Per monitorare un caso, un incidente o una richiesta di assistenza, utilizzando la console AMS, segui questi passaggi.

1. Nella dashboard dei report sugli incidenti o delle richieste di assistenza della console AMS, accedi a un caso e scegli l'oggetto per aprire una pagina di dettagli con lo stato attuale e le corrispondenze.

   Quando un incidente segnalato o un caso di richiesta di assistenza viene aggiornato dal team operativo AMS, ricevi un'e-mail e un link all'incidente nella console AMS in modo da poter rispondere. Non puoi rispondere alla corrispondenza relativa all'incidente rispondendo all'e-mail.

> **Important**
>
> È necessario aver inserito un indirizzo e-mail per ricevere notifiche di cambio di stato per una richiesta di servizio o un caso imprevisto. Le notifiche vengono inviate solo all'indirizzo e-mail aggiunto al caso al momento della creazione.
> Il collegamento contenuto nell'e-mail di notifica non funzionerà a meno che non si utilizzi un server di posta elettronica sulla rete federata AMS. Tuttavia, puoi rispondere alla corrispondenza accedendo alla tua console AMS e utilizzando la pagina dei dettagli del caso.

2. Se nell'elenco sono presenti molti casi, puoi utilizzare l'opzione Filtro:

   - Tutti aperti (impostazione predefinita): utilizza questo filtro per visualizzare tutti i casi che non sono stati risolti.
   - Non assegnato: da utilizzare se hai appena inviato il caso e non hai ricevuto alcuna notifica che lo stato del caso è cambiato. Tieni presente che gli incidenti e i casi di richiesta di assistenza vengono risolti con rapidità diversa a seconda della priorità inviata (incidenti) o del contratto sul livello di servizio (richieste di assistenza).
   - Aperto: utilizza questa opzione se hai ricevuto una notifica che indica che il caso è in sospeso da Amazon; ciò significa che il caso è stato assegnato ma il lavoro non è ancora iniziato.
   - Riaperto: utilizza questa opzione se hai ricevuto la notifica che il caso è stato riaperto dopo essere stato risolto.
   - Lavori in corso: utilizza se hai ricevuto la notifica che un operatore ha iniziato a lavorare sul caso.
   - Intervento in sospeso da parte del cliente: utilizza questa opzione se hai ricevuto una richiesta di intervento da parte tua da parte di un operatore.
   - Azione del cliente completata: utilizza questa opzione se hai ricevuto una notifica che la tua azione sul caso è stata elaborata.
   - Risolto: utilizza per visualizzare i casi che sai essere stati risolti. I casi risolti vengono conservati nella cronologia per dodici mesi.
   - Qualsiasi stato: utilizza questo filtro per visualizzare tutti i casi, indipendentemente dallo stato.

3. Per verificare lo stato più recente, aggiorna la pagina.
4. Se le corrispondenze sono così numerose che non compaiono tutte nella pagina, scegli Carica altro.

5. Per aggiornare lo stato del caso, scegli Rispondi, inserisci la nuova corrispondenza, quindi scegli Invia.
6. Per chiudere il caso dopo che è stato risolto in modo soddisfacente, scegli Chiudi caso.

   Assicurati di assegnare al servizio una valutazione da 1 a 5 stelle per far sapere ad AMS come stiamo!

Risposta a una richiesta di assistenza generata da AMS

La gestione delle patch AMS invia le richieste di servizio (note anche come notifiche di servizio) prima dell'orario della finestra di manutenzione impostata; per ulteriori informazioni, consulta la finestra di manutenzione AMS. AMS ti invia anche notifiche di servizio quando esiste la possibilità che un AWS servizio influisca sulla tua infrastruttura o quando potrebbe essere necessario riavviare un' EC2 istanza del tuo account; per ulteriori informazioni, consulta Notifiche di servizio.

> **Note**
>
> AMS invia le comunicazioni all'indirizzo e-mail principale del tuo AWS account che hai fornito; ti consigliamo di aggiungere un alias email di contatto Operations alternativo per facilitare la richiesta di servizio o il processo di gestione delle notifiche di servizio. L'aggiunta di queste e-mail è prevista durante il processo di onboarding di AMS e la relativa documentazione di onboarding.

Domande sulla fatturazione

Per inviare una domanda relativa alla fatturazione, completa i seguenti passaggi:

1. Apri il Supporto AWS Centro a casa#/ https://console.aws.amazon.com/support/.
2. Scegli Account e fatturazione.
3. Scegli Crea caso.
4. Scegli Account e fatturazione, quindi segui le istruzioni per inviare la tua richiesta.

Operazioni su richiesta

Operations on Demand (OOD) è una funzionalità di AWS Managed Services (AMS) che estende l'ambito standard del piano operativo AMS fornendo servizi operativi che attualmente non sono offerti nativamente dai piani operativi AMS o AWS. Una volta selezionata, l'offerta del catalogo viene fornita da una combinazione di automazione e risorse AMS altamente qualificate. Non sono previsti impegni a lungo termine o contratti aggiuntivi, il che consente di estendere l'AMS e AWS le operazioni e le funzionalità esistenti in base alle esigenze. L'utente accetta di acquistare blocchi di ore (blocchi OOD), 20 ore per blocco, su base mensile.

Puoi scegliere dal catalogo di offerte standardizzate e avviare un nuovo impegno OOD tramite una richiesta di servizio. Esempi di offerte OOD includono l'assistenza per la manutenzione di Amazon EKS, le operazioni e la gestione dei AWS Control Tower cluster SAP. Le nuove offerte di cataloghi vengono aggiunte regolarmente in base alla domanda e ai casi d'uso operativi che vediamo più spesso.

OOD è disponibile per i piani operativi di AMS Advanced e AMS Accelerate ed è disponibile Regioni AWSovunque sia disponibile AMS.

AMS esegue il Customer Security Risk Management (CSRM) mentre implementa le modifiche richieste. Per ulteriori informazioni sul processo CSRM, consulta Change Request Security Reviews.

Catalogo di offerte Operations on Demand

Operations on Demand (OOD) offre i servizi descritti nella tabella seguente.

> **Note**
>
> Per le definizioni dei termini chiave, consulta la documentazione di AWS Managed Services Key Terms.

Piano operativo	Titolo	Descrizione	Risultati attesi
AMS Accelerate	Manutenzione dei cluster Amazon EKS	AMS libera gli sviluppatori di container gestendo la manutenzione continua delle distribuzioni di Amazon Elastic Kubernete	I team dei clienti hanno fornito assistenza nelle operazioni di base

		s Service (Amazon EKS). AMS esegue le end-to-end procedure necessarie per aggiornare un cluster occupandosi dei component i del piano di controllo, dei componenti aggiuntivi e dei nodi. AMS esegue l'aggiornamento ai tipi di nodi gestiti e a un set curato di componenti aggiuntivi Amazon EKS e Kubernetes.	relative all'aggio rnamento dei cluster Amazon EKS.
AMS Accelerate	Edilizia e vendita AMI	AMS fornisce ai clienti la gestione continua degli edifici e dei distribut ori AMI. I nostri ingegneri eseguono una versione mensile di versioni sottoscritte AMIs, rilasciate su richiesta AMIs per attività di patching emergenti, gestiscono le modifiche utilizzando i runbook e monitorano le build AMI utilizzando Monitoring. CloudWatch Forniamo inoltre assistenza per la risoluzio ne dei problemi e report dettaglia ti per tutti gli account utilizzati negli account designati. AMIs Questa offerta richiede l'implementazione di AMI build Pipelines tramite EC2 Image Builder. AMS non supporta nessun'altra automazio ne o servizio che interagisce con Image Builder. EC2	Il livello di sicurezza dei clienti è migliorat o e il tempo dedicato dai clienti alla costruzione e alla vendita è stato ridotto. AMIs

AMS Accelerate	Esecuzione delle modifiche curata	Collaborate con i nostri tecnici operativi qualificati per tradurre i vostri requisiti aziendali in richieste di modifica convalidate che possono essere eseguite in sicurezza all'interno del vostro AWS ambiente. Sfruttate il nostro approccio unico all'automazione e alla conoscenza delle migliori pratiche operative (ad esempio, valutazione dell'impatto, rollback, regola delle due persone), che si tratti di un semplice cambiamen to su larga scala o di un'azione complessa con impatti a valle.	I clienti ci hanno aiutato a definire, creare ed eseguire richieste di modifica personalizzate. Le modifiche possono essere manuali o automatizzate (CloudFormation, SSM). Include la consulenza Supporto per una guida alla configurazione, se necessario. Non destinato alle modifiche al codice dell'appl icazione, all'insta llazione/distribuzione dell'applicazione, alla migrazione dei dati o alle modifiche alla configurazione del sistema operativo.

AMS Accelerate	AWS Network Firewall Operazioni	AMS collabora con te per integrare il firewall e implementare e gestire le politiche e le regole per le operazioni continue del firewall. I nostri ingegneri lo fanno sfruttando le nostre migliori pratiche operative e l'automazione per configurare politiche e regole standardizzate e abilitando il monitoraggio per rilevare le modifiche apportate al di fuori del processo di automazione. AMS notifica rapidamente le modifiche indesiderate e offre opzioni per includerle, se richiesto, o ripristinare l'account a una configurazione precedente per garantire la stabilità complessiva dei sistemi.	I team dei clienti hanno contribuito a ridurre il sovraccarico di gestione rilevando rapidamente le modifiche involontarie del firewall di rete, con conseguente migliore risoluzione degli incidenti e riduzione dei tempi di analisi delle cause principali per i problemi previsti e imprevisti.
AMS Accelerate	AWS Control Tower operazioni	Operazioni e gestione continue della zona di AWS Control Tower atterraggio, incluso AWS Transit Gateway e AWS Organizations fornitura di una soluzione completa per le zone di atterraggio. Gestiamo la vendita degli account, la gestione di SCP e OU, la correzione degli errori, la gestione degli utenti SSO e AWS Control Tower gli aggiornamenti con la nostra libreria di controlli e guardrail personalizzati.	I team dei clienti hanno fornito assistenza in alcune delle attività operative di base relative alla gestione AWS Control Tower di AWS Transit Gateway e AWS Organizations.

AMS Accelerate	AWS landing zone Accelera le operazioni	AMS fornisce operazioni continue delle zone di AWS atterraggio utilizzate tramite AWS Landing Zone Accelerator (LZA). I nostri ingegneri gestiscono le modifiche ai file di configura zione, la gestione dell'ambiente AWS Control Tower (CT) (vendita di account, creazione di unità organizzative, guardrail CT), la gestione delle policy di controllo dei servizi (SCP), il rilevamento e la correzione delle deviazioni CT, la gestione della configurazione di rete e gli aggiornamenti a CT e al framework LZA. AWS LZA fornisce un mezzo per configurare e gestire un ambiente sicuro con più AWS account utilizzando best practice e servizi operativi come. AWS Control Tower	I team dei clienti hanno fornito assistenza nelle operazioni e nella gestione continue della soluzione AWS Landing Zone Accelerator.

AMS Accelerate	SAP Cluster Assist	Allarmi, monitoraggio, applicazione di patch ai cluster, backup e risoluzione degli incidenti dedicati per i cluster SAP. Questo articolo del catalogo consente di delegare parte del lavoro operativo in corso del team operativo SAP in modo che possa concentrarsi sulla gestione della capacità e sull'ottimizzazione delle prestazioni.	I team SAP dei clienti o dei partner hanno fornito assistenza in alcune delle attività operative sottostanti. Richiede comunque al cliente di fornire altre funzionalità SAP come gestione della capacità, ottimizzazione delle prestazioni, DBA e amministrazione di base SAP.
AMS Accelerate	SQL Server on Operations EC2	AMS collabora con voi per integrare, implementare e gestire le operazioni in corso dei database SQL Server distribuiti sulle istanze. EC2 I nostri ingegneri sfruttano le nostre best practice operative e l'automazione per liberare i team di database eseguendo attività come backup e patch, estendendo il supporto operativo AMS alle patch di SQL Server per includere aggiornamenti continui con riconoscimento del cluster, servizi di backup e ripristino in linea con la nostra strategia di difesa dal ransomware e monitorando l'aderenza ai controlli di backup e patching forniti dal cliente.	I clienti di SQL Server hanno fornito assistenza nell'offload delle operazioni di patching e backup del database per migliorare la resilienza e il livello di sicurezza dei loro carichi di lavoro, oltre a ottimizzare i costi delle licenze portando le proprie licenze (BYOL) a EC2.

AMS Advanced	Manutenzione del cluster Amazon EKS	AMS libera gli sviluppatori di container gestendo la manutenzione e l'integrità continue delle distribuzioni di Amazon Elastic Kubernetes Service (Amazon EKS). AMS esegue le end-to-end procedure necessarie per aggiornare un cluster rivolgendosi ai componenti del piano di controllo, dei componenti aggiuntivi e dei nodi. AMS esegue l'aggiornamento ai tipi di nodi gestiti e a un set curato di componenti aggiuntivi Amazon EKS e Kubernetes.	I team dei clienti hanno fornito assistenza nelle operazioni di base relative all'aggiornamento dei cluster Amazon EKS.
AMS Advanced	Esecuzione RFC prioritaria	Capacità di un tecnico operativo AMS incaricato di dare priorità all'esecuzione delle richieste di modifica (RFC). Tutti gli invii ricevono un livello di risposta più elevato e l'ordine di priorità può essere modificato interagendo direttamente con gli ingegneri tramite una sala riunioni Amazon Chime.	I clienti ricevono una risposta SLO di 8 ore per. RFCs

AMS Advanced e AMS Accelere	Aggiornamento del sistema operativo legacy	Evita la migrazione delle istanze aggiornando le istanze a una versione del sistema operativo supportata. Possiamo eseguire un aggiornamento sul posto sulle istanze selezionate sfruttando l'automazione e le funzionalità di aggiornamento dei fornitori di software (ad esempio, da Microsoft Windows 2008 R2 a Microsoft Windows 2012 R2). Questo approccio è ideale per le applicazioni legacy che non possono essere facilmente reinstallate su una nuova istanza e offre una protezione aggiuntiva dalle minacce alla sicurezza note e non mitigate sulle versioni precedenti del sistema operativo. I seguenti sistemi operativi sono supportati per gli aggiornamenti in loco: • Da Microsoft Windows 2012 R2 a Microsoft Windows 2016 e versioni successive • Da Microsoft Windows 2016 a Microsoft Windows 2022 e versioni successive • Da Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8 • Da Red Hat Enterprise Linux 8 a Red Hat Enterprise Linux 9 • Da Oracle Linux 7 a Oracle Linux 8	Questa soluzione viene fornita per le applicazioni che non possono più essere reinstallate su una nuova istanza (ad esempio, perdita del codice sorgente, ISV fuori servizio e così via). È possibile ripristinare lo stato originale degli aggiornamenti non riusciti. Dal punto di vista operativo, il rollback è preferibile perché pone l'istanza in uno stato più supportabile con le patch di sicurezza più recenti.

Argomenti

Richiedere AMS Operations On Demand

AWS Managed Services (AMS) Operations on Demand (OOD) è disponibile per tutti Account AWS coloro che sono stati inseriti in AMS. Per sfruttare Operations on Demand, richiedi ulteriori informazioni al tuo cloud service delivery manager (CSDM), Solutions Architect (SA), account manager o Cloud Architect (CA). Le offerte OOD disponibili sono elencate nella precedente tabella delle offerte del catalogo di Operations on Demand. Dopo aver completato l'ambito del coinvolgimento, invia una richiesta di servizio ad AMS Operations per avviare un incarico per OOD.

Ogni richiesta di servizio OOD deve contenere le seguenti informazioni dettagliate relative all'incarico:

- Le offerte OOD specifiche richieste e per ogni offerta OOD specifica:
  - Il numero di blocchi (un blocco equivale a 20 ore di risorse operative in un determinato mese di calendario, da addebitare alla tariffa standard in vigore in quel momento per l'offerta Operations on Demand applicabile) da allocare alla specifica offerta OOD. AWS
  - L'ID dell'account per ogni account AWS Managed Services per il quale viene richiesta l'offerta OOD specifica.

Le richieste di servizio OOD devono essere inviate dall'utente tramite:

- L'account AWS Managed Services che riceve le offerte Operations on Demand applicabili, oppure
- Un account AWS Managed Services che è un account di AWS Organizations gestione in modalità con tutte le funzionalità, per conto di qualsiasi account membro che sia un account AWS Managed Services.

Dopo aver ricevuto la richiesta di servizio OOD, AMS Operations esamina e aggiorna gli account con la loro approvazione, approvazione parziale o rifiuto.

Una volta approvata la richiesta di servizio dell'offerta OOD, tu e AMS vi coordinate per iniziare l'incarico. Nessuna offerta OOD viene avviata finché la richiesta di servizio non viene approvata e non viene concordata una data di inizio dell'incarico.

AMS utilizza un'assegnazione mensile di blocchi OOD in abbonamento. Assegniamo il numero di blocchi approvato mensilmente, a partire dalla data di inizio dell'impegno, fino a quando non richiedi di rinunciare tramite una nuova richiesta di servizio. I blocchi OOD sono validi per un mese solare. I blocchi, o porzioni di blocchi, non vengono ribaltati o riportati ai mesi futuri.

Ti viene fatturato almeno un blocco OOD ogni mese, indipendentemente dal numero di ore effettivamente utilizzate. Qualsiasi blocco OOD aggiuntivo allocato in cui non sono state utilizzate ore non viene fatturato.

Apportare modifiche alle offerte Operations on Demand

Per richiedere modifiche agli impegni in corso per le offerte Operations on Demand (OOD), invia una richiesta di servizio contenente le seguenti informazioni:

- Le modifiche richieste e
- La data richiesta per l'entrata in vigore delle modifiche.

Dopo aver ricevuto la richiesta di servizio OOD, AMS Operations la esamina e la aggiorna con la propria approvazione oppure richiede che il CSDM assegnato collabori con voi per determinare l'ambito e le implicazioni della modifica. Se si ritiene che la modifica richieda uno sforzo di definizione dell'ambito da parte del CSDM, è necessario inviare una seconda richiesta di servizio OOD per avviare l'intervento modificato dopo il completamento dell'esercizio di definizione dell'ambito.

Una volta approvata, l'allocazione di blocchi modificata più di recente diventa e continua a rimanere attiva, sostituendo qualsiasi allocazione di blocchi precedente, salvo diverso accordo tra l'utente e l'utente. AWS

Cronologia dei documenti

La tabella seguente descrive le modifiche importanti in ogni versione della AMS Advanced User Guide. Per ricevere notifiche sugli aggiornamenti di questa documentazione, è possibile sottoscrivere un feed RSS.

- Versione API: 2019-05-21
- Nuovo o aggiornato CTs e procedure dettagliate: AMS Advanced Change Type Reference Document History.
- Nuovo AMS:. AMIs Immagini di macchine AMS Amazon (AMIs)

Modifica	Descrizione	Data
Tabella aggiornata per AWS Identity and Access Management (IAM) nei controlli standard nella sezione AMS Advanced	Informazioni aggiornate nella tabella relative alle policy IAM e all'accesso ai bucket Amazon S3.	25 settembre 2025
Fase aggiornata per le domande relative alla fatturazione	Fase aggiornata per la creazione di richieste di servizio per le domande relative alla fatturazione nella sezione Creazione di una richiesta di servizio in AMS.	25 settembre 2025
Informazioni aggiornate per le notifiche e-mail relative ai tipi di modifica	Informazioni aggiornate ed esempi per l'aggiunta di notifiche e-mail per i tipi di modifica nella sezione Configura le notifiche e-mail RFC (console).	25 settembre 2025
Tipo di modifica aggiornato	Sezione di etichettatura automatica dell'infrastruttura AMS aggiornata con tipo	25 settembre 2025

	di modifica per l'etichettatura delle risorse create da AMS.	
Domande frequenti sulla macchina virtuale aggiornata a Import/Export in AWS Managed Services	È stata aggiornata la RFC utilizzata per richiedere un profilo dell'istanza per consentire agli strumenti di eseguire comandi dall'istanza.	24 settembre 2025
Request for change (RFC) aggiornata per il lancio di un'istanza di SUSE Linux Enterprise Server for SAP Applications 15 SP6	È stato aggiornato il passaggio 2 su come avviare una nuova istanza di SUSE Linux Enterprise Server for SAP Applications 15 SP6 con la RFC corretta.	22 settembre 2025
Richiesta di modifica aggiornata (RFC)	Aggiornato AWS Elastic Disaster Recovery nella sezione Domande frequenti su AWS Managed Services con la RFC corretta per creare i ruoli IAM necessari all'interno del tuo account.	22 settembre 2025

Aggiunti 4 nuovi controlli di ottimizzazione dei Trusted Advisor costi supportati da Trusted Remediator	Sono stati aggiunti i seguenti controlli di ottimizzazione dei costi: • c1z7kmr00n - Consigli di ottimizzazione dei costi di Amazon per le istanze EC2 • c1z7kmr02n - Raccomand azioni per l'ottimizzazione dei costi di Amazon EBS per i volumi • c1z7kmr03n - Consigli per l'ottimizzazione dei costi di Amazon RDS per le istanze DB • c1z7kmr05n - AWS Lambda consigli per l'ottimizzazione dei costi per le funzioni	22 settembre 2025
Nota aggiornata per le zone di disponibilità () AZs	Informazioni aggiornate sui gruppi di sicurezza in AMS.	5 settembre 2025
Tipo di modifica aggiornato	Sezione delle domande frequenti su Amazon FSx in AWS Managed Services aggiornata con il tipo di modifica per condividere Managed AD con l'account dell'applicazione.	5 settembre 2025
Tipo di modifica aggiornato	Aggiornamento della sezione Domande frequenti su Amazon DocumentDB in AWS Managed Services con il tipo di modifica da utilizzare per l'eliminazione. APIs	5 settembre 2025

Tipo di modifica aggiornato	Sezione delle domande frequenti su Alexa for Business in AWS Managed Services aggiornata con tipo di modifica a due utenti IAM ad accesso limitato per l'install azione e il funzionamento del gateway Alexa for Business.	5 settembre 2025
Tipo di modifica aggiornato	Aggiornamento AppStream 2.0 nella sezione Domande frequenti su AWS Managed Services con tipo di modifica per creare e scegliere un ruolo IAM che sarà disponibile su tutte le istanze di streaming della flotta	5 settembre 2025
Tipo di modifica aggiornato	Aggiornamento EventBrid ge nella sezione Domande frequenti su AWS Managed Services con tipo di modifica per richiedere un ruolo di EventBridge servizio prima di EventBridge utilizzarlo per attivare altre AWS risorse.	5 settembre 2025
Supporto aggiornato per i controlli Trusted Advisor di sicurezza da parte di Trusted Remediator	Aggiornati i parametri e i vincoli preconfigurati supportat i per il controllo Hs4Ma3G108: i trail devono essere integrati con Amazon Logs CloudTrail CloudWatch	5 settembre 2025

Supporto aggiornato per i controlli Trusted Advisor di sicurezza da parte di Trusted Remediator	Controllo Trusted Advisor di sicurezza aggiornato per aggiungere la versione 2 di Hs4Ma3G184: la registrazione di Application Load Balancers e Classic Load Balancers deve essere abilitata	5 settembre 2025
Controlli di eccellenza Trusted Advisor operativa aggiornati supportati dalla sezione Trusted Remediator	Controlli di eccellenza Trusted Advisor operativa aggiornati supportati dalla sezione Trusted Remediator per aggiungere un nuovo controllo supportato c1fd6b96l4 Amazon S3 Access Logs Enabled.	28 agosto 2025
Tipo di modifica aggiornato	Tipo di modifica per il ruolo IAM personalizzato.	25 agosto 2025
Aggiornato utilizzando CloudWatch Application Insights for .Net e SQL server nella sezione AMS	Tipo di modifica rivisto per utilizzare CloudWatch Application Insights.	25 agosto 2025
Richiesta di modifica aggiornata (RFC)	Request for change (RFC) per aggiungere altri tag al bucket Amazon S3.	25 agosto 2025
Richiesta di modifica aggiornata (RFC)	Request for change (RFC) per etichettare tutte le risorse create da AMS a fini di gestione.	25 agosto 2025
Lambda nella sezione Domande frequenti su AWS Managed Services aggiornata	Tipo di modifica rivisto per l'accesso ad altri AWS servizi per creare sorgenti di eventi.	25 agosto 2025

Lambda nella sezione Domande frequenti su AWS Managed Services aggiornata	Tipo di modifica rivisto per fornire le funzioni Lambda.	25 agosto 2025
Sezione aggiornata per la creazione, la modifica o l'eliminazione dei gruppi di sicurezza	Tipo di modifica rivisto per creare un gruppo di sicurezza al di fuori degli stack e. VPCs	25 agosto 2025
Sezione Trusted Remediator aggiornata per includere nuovi contenuti per Compute Optimizer	Sezione Trusted Remediator aggiornata per includere nuovi contenuti per i consigli supportati. AWS Compute Optimizer	18 agosto 2025
Link al glossario TOC rimosso	AWS Glossario.	8 agosto 2025
Raccomandazione precisa del tipo di modifica	Per integrare la metrica del cliente nel sistema di monitoraggio delle applicazioni, richiedi ad AMS di creare un argomento Amazon SNS per la metrica inviando una RFC con Deployment | Monitoring and notification | SNS | Create CT (ct-3dfnglm4ombbs).	8 agosto 2025
Raccomandazione precisa del tipo di modifica	Per eliminare i volumi di istanze segnaposto, invia un tipo di modifica Management | Advanced stack components | EBS Volume | Delete change (ct-3e3h8u0sp5z80).	8 agosto 2025

SecureChannelFailure Nuovi avvisi di monitoraggio: e Broken Secure Channel	Avvisi derivanti dal monitoraggio di base in AMS AMS (correzione automatica degli avvisi).	8 agosto 2025
Nuovi controlli Trusted Remediator	Trusted Advisor controlli di ottimizzazione dei costi supportati dai controlli di Trusted Advisor sicurezza Trusted Remediator supportati da Trusted Remediator Hs4Ma3G120— AWSManagedServices-TerminateEC2InstanceStoppedForPeriodOfTime, Hs4Ma3G230— 2 e c18d2gz150— 2. AWSManagedServices-TrustedRemediator EnableBucketAccessLoggingV AWSManagedServices-TerminateEC InstanceStoppedForPeriodOfTime	8 agosto 2025
Aggiornamento dello standard IAM al punto 3.2	Linguaggio chiarito e rimossa la menzione dei tag.	25 luglio 2025
Aggiornamento delle opzioni di disattivazione degli avvisi	L'aggiunta di un tag consente di disattivare altri due avvisi.	25 luglio 2025
Obsoletezza del servizio di provisioning self-service	Il servizio di fornitura CloudEndure self-service è obsoleto a favore di. AWS Application Migration Service	25 luglio 2025
Nuova funzionalità per i backup	Personalizza le notifiche sugli archivi di backup con un nuovo tag.	25 luglio 2025

Tabella dei controlli aggiornata	Sono stati rimossi alcuni controlli duplicati nella sezione della tabella AMS-STD-002 - AWS Identity and Access Management (IAM).	26 giugno 2025
Prerequisiti del servizio SSP aggiornati AWS Transfer Family	Sono state aggiunte informazioni alla sezione dei prerequisiti.	26 giugno 2025
Esempio di policy IAM aggiornato	Esempio di policy IAM aggiornato con ulteriori restrizioni, come consigliato.	26 giugno 2025
AMI aggiornata supportata OSes	È stato aggiunto Ubuntu Linux 24.04 in Ubuntu Linux 22.04 e tutti i riferimenti sono stati modificati in SP5 . SP6	26 giugno 2025
Servizio di fornitura self-service, obsoleto MediaStore	È stata aggiunta una nota di deprecazione per. AWS Elemental MediaStore	26 giugno 2025
Servizio di provisioning self-service, Amazon Inspector Classic obsoleto	È stata aggiunta una nota di deprecazione per Amazon Inspector Classic.	26 giugno 2025
Servizio di provisioning self-service, Amazon Connect obsoleto	È stata aggiunta una nota di deprecazione per Amazon Connect.	26 giugno 2025
Sezione aggiornata per le configurazioni supportate in AMS	Configurazioni supportate e aggiornate per i sistemi operativi supportati e i sistemi operativi Supported End of Support (EOS) in AMS.	25 giugno 2025

Servizio di fornitura self-service, obsoleto WorkDocs	Pagina rimossa e riferimenti a dati obsoleti. WorkDocs	19 giugno 2025
Gestione delle patch: importante nota di sicurezza per archivi di patch alternativi	Nota importante sulla sicurezza e best practice per l'utilizzo di repository di patch alternativi in AMS.	10 giugno 2025
Aggiornamenti dei sistemi operativi supportati	I sistemi operativi supportati da AMS Advanced vengono aggiornati, alcuni aggiunti, altri rimossi.	22 maggio 2025
Solo interno APIs	Solo interni APIs che appaiono in alcuni registri. CloudWatch	22 maggio 2025
Aggiornamenti di AMS Trusted Remediator	Come utilizzare un nuovo parametro per personalizzare i `preconfigured-parameters` Trusted Advisor controlli in Trusted Remediator.	22 maggio 2025
Aggiornamenti del registro SSP Amazon Elastic Container	Altri ruoli vengono assegnati automaticamente quando effettui l'onboarding del servizio Amazon ECR.	8 maggio 2025

Domande frequenti e aggiornamenti su AMS Advanced Trusted Remediator.	Diversi aggiornamenti ai Trusted Advisor controlli supportati, domande frequenti su Trusted Remediator (aggiunta «Quali risorse distribuisce Trusted Remediator ai tuoi account?») e altro ancora. Vedi anche Trusted Advisor i controlli supportati da Trusted Remediator.	8 maggio 2025
Aggiornamento dei controlli di sicurezza AMS Advanced Standard.	Aggiunti i controlli di «Condivisione dei gruppi di sicurezza».	8 maggio 2025
Namespace protetti AMS Advanced.	Namespace di nomi protetti da `EPSMarketplaceSubscriptionRole` AMS e aggiunti. `EPS`	24 aprile 2025
Posizioni dei log di AMS Advanced.	Sono state aggiunte altre posizioni di registro.	24 aprile 2025
Aggiornamento della modalità AMS Advanced Self-Service Provisioning per i prerequisiti AppStream 2.0.	È stato aggiunto un prerequisito per la AppStream versione 2.0: è necessario includere un nome di bucket Amazon S3 quando si invia la RFC di provisioning per il servizio.	24 aprile 2025
AMS Advanced Nuovo avviso di riparazione automatica di Amazon RDS.	ID avviso: - 0224, si attiva quando lo storage allocato richiesto raggiunge o supera la soglia di archiviazione massima configurata.	27 marzo 2025

AMS Advanced AWS ha chiuso l'accesso di nuovi clienti ad Amazon CloudSearch a partire dal 25 luglio 2024.	I clienti esistenti possono ancora utilizzare il servizio, ma non ci saranno nuove funzionalità.	27 marzo 2025
AMS Advanced AWS ha chiuso l'accesso a AWS CodeCommit nuovi clienti a partire dal 25 luglio 2024.	I clienti esistenti possono ancora utilizzare il servizio, ma non ci saranno nuove funzionalità.	27 marzo 2025
Trusted Remediator è ora disponibile.	Trusted Remediator, una soluzione AWS Managed Services che automatizza la correzione dei AWS Trusted Advisor controlli, è ora disponibile.	19 marzo 2025
AMS Advanced Nuovo avviso RDS per riparazioni automatiche.	RDS-EVENT-0224 aggiunto.	17 marzo 2025
AMS Advanced Nuova funzionalità: notifiche di incidenti.	È possibile utilizzarla AppRegistry per creare applicazioni e personalizzare le notifiche di incidenti per tali applicazioni.	13 marzo 2025
Aggiornamento AMS alla soglia di monitoraggio degli allarmi RDS.	La soglia di allarme di utilizzo medio della CPU RDS è stata modificata dal 75% al 90%.	20 febbraio 2025

Report self-service aggiornati con nuove opzioni di dati per la visualizzazione aggregata dei report	Sono state aggiunte opzioni di dati che includono nuovi nomi di campo:**`Admin Account ID`**, nome campo del set di dati: `aws_admin_account_id` e definizione: `Trusted AWS Organization account enabled by the customer` per i seguenti report self-service: • Rapporto sulle patch (giornaliero) • Rapporto di Backup (giornaliero) • Rapporto sull'incidente (settimanale)	28 gennaio 2025
Aggiornamento alla SSP AWS Batch	Puoi utilizzare la seguente RFC per il provisioning AWS Batch nel tuo account AMS: Gestione | Servizio AWS | Servizio self-provisioned | Aggiungi (ct-1w8z66n899dct).	28 gennaio 2025
Nuova funzionalità AMS: report self-service aggregati	I report self-service aggregati (SSR) offrono una visualizzazione dei report self-service esistenti aggregati a livello di organizzazione, su più account.	21 gennaio 2025

Aggiornamento alla sezione Forecast SSP	Nota aggiunta: 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.	10 gennaio 2025
Aggiornamento alla sezione dei namespace protetti da AMS	È stato aggiunto uno spazio dei nomi protetto mancante (*mc, *MC e *Mc) all'elenco dei namespace protetti da AMS.	9 gennaio 2025
Aggiornamento alla sezione Come funziona il monitoraggio	Sono state aggiunte informazioni su una nuova funzionalità, sulla configurazione delle notifiche di avviso per risorsa o ID di istanza, anziché per incidente.	8 gennaio 2025
Aggiornato: contenuto dell'aggiornamento basato su tag	È stato corretto un errore di battitura nel nome chiave e il percorso errato del file di configurazione è stato corretto.	6 gennaio 2025
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	21 novembre 2024
Tabella delle offerte Operations On Demand aggiornata	I seguenti sistemi operativi sono supportati per gli aggiornamenti in loco: • Da Microsoft Windows 2016 a Microsoft Windows 2022 e versioni successive	11 novembre 2024

Tabella delle offerte di Operations On Demand aggiornata	I seguenti sistemi operativi sono supportati per gli aggiornamenti in loco: • Da Microsoft Windows 2012 R2 a Microsoft Windows 2016 e versioni successive • Da Red Hat Enterprise Linux 7 a Red Hat Enterprise Linux 8 • Da Red Hat Enterprise Linux 8 a Red Hat Enterprise Linux 9 • Da Oracle Linux 7 a Oracle Linux 8	1 novembre 2024
Configurazioni supportate aggiornate	Sistemi operativi Oracle Linux supportati aggiornati a 9.0-9.3, 8.0-8.9, 7.5-7.9.	24 ottobre 2024
Immagini di macchine AMS Amazon aggiornate (AMIs)	Aggiornamento basato su Windows AMIs per rimuovere Windows 2012 e 2012 R2. Basato su Linux aggiornato AMIs per rimuovere diverse AMI che non sono più supportate e per aggiungere quanto segue: • Amazon Linux (2ARM64) • RHEL 9 • SUSE Linux Enterprise Server 15 SP5	24 ottobre 2024

Ora puoi includere più indirizzi e-mail negli avvisi basati su tag.	Gli indirizzi e-mail multipli sono ora supportati negli avvisi basati su tag.	20 settembre 2024
È stata aggiunta la sezione delle revisioni di sicurezza delle richieste di modifica.	È stata aggiunta una nuova sezione che fornisce dettagli sul processo di revisione della sicurezza delle richieste di modifica.	17 settembre 2024
È stata aggiunta una nuova sezione.	È ora disponibile una nuova sezione che descrive come avvengono le revisioni della sicurezza delle richieste di modifica in AMS Advanced.	12 settembre 2024
Nuovo servizio supportato da AMS Advanced.	AWS Resilience Hub è ora supportato da AMS Advanced.	30 agosto 2024
Nuovi servizi supportati da AMS Advanced.	Cinque nuovi servizi sono ora supportati da AMS Advanced: • Amazon Bedrock • Amazon Kendra • Database Amazon Quantum Ledger (Amazon QLDB) • AWS Service Catalog AppRegistry • Amazon Managed Service per Prometheus	21 agosto 2024
È ora disponibile una nuova impostazione predefinita della rete di sicurezza degli endpoint.	La fonte degli aggiornamenti è ora inclusa nelle impostazioni di rete predefinite di EPS.	21 agosto 2024

Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	30 luglio 2024
AMS ora supporta Amazon Route 53 Resolver DNS Firewall.	AMS ora supporta Amazon Route 53 Resolver DNS Firewall	30 luglio 2024
AWS DataSync Aggiornamento SSPS	AWS DataSync non richiede più il prefisso «datasync-» sui nomi dei bucket Amazon S3.	30 luglio 2024
Dashboard delle regole di configurazione di sicurezza	Il dashboard delle regole di configurazione di sicurezza è ora disponibile nella reportistica self-service.	24 luglio 2024
AMS ora supporta Oracle Linux 8.9, RHEL 8.10 e RHEL 9.4.	AMS ora supporta Oracle Linux 8.9, RHEL 8.10 e RHEL 9.4.	5 luglio 2024
Amazon Bedrock ora disponibile in modalità di provisioning self-service	Ora puoi richiedere Amazon Bedrock in modalità AMS SSP.	27 giugno 2024
Eventi del firewall DNS di Amazon Route 53 Resolver in Security Incident Response	AMS ora monitora gli eventi del firewall DNS di Amazon Route 53 Resolver in Security Incident Response	21 giugno 2024
Sono state aggiunte ulteriori informazioni su come abilitare la funzione AMS bring your own EPS (BYOEPS).	Sono state aggiunte ulteriori informazioni su come abilitare la funzione AMS bring your own EPS (BYOEPS).	5 giugno 2024

Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	23 maggio 2024
Informazioni aggiunte sull'utilizzo di un ruolo personalizzato AWS Amplify in modalità di provisioning self-service (solo ambienti MALZ).	Sono state aggiunte istruzioni su come gli ambienti MALZ possono utilizzare un ruolo personalizzato AWS Amplify in modalità di provisioning self-service.	23 maggio 2024
Amazon Kendra è ora disponibile in modalità Self-Service Provisioning.	Amazon Kendra è ora disponibile in modalità Self-Service Provisioning.	23 maggio 2024
AMS Advanced supporta sistemi operativi aggiuntivi.	AMS Advanced supporta Red Hat Enterprise Linux (RHEL) 9.x e Ubuntu 20.04 e 22.04.	25 aprile 2024
AMS Advanced supporta l' ARM64 architettura per Amazon Linux 2.	AMS Advanced supporta l' ARM64 architettura per Amazon Linux 2.	25 aprile 2024
Aggiornamento della sezione Offboard from multi-account landing zone accounts (MALZ) landing zone.	Sono state aggiunte informazioni dettagliate su come effettuare l'offboard degli account Application e Core dalla landing zone con più account.	11 aprile 2024
Aggiornamento: descrizione della gestione delle richieste di assistenza.	Descrizione aggiornata della gestione delle richieste di assistenza nell'argomento Descrizione del servizio.	21 marzo 2024

Aggiornato: sezione Impegni del servizio di gestione degli incidenti.	È stato aggiunto un collegamento al Service Level Agreement di AMS.	21 marzo 2024
Aggiornamento: sezione Come funziona la gestione delle richieste di assistenza.	Sono stati aggiunti chiarimenti su come AMS gestisce le richieste di servizio che contengono una richiesta di funzionalità o un bug.	21 marzo 2024
Aggiornamento: sezione Richiedi assistenza.	La sezione Richiedi assistenza è stata aggiornata per includere una nuova sezione Domande sulla fatturazione.	21 marzo 2024
Aggiornato: AMS Automated IAM Provisioning	Aggiornamento di AMS Automated IAM Provisioning con informazioni personalizzate sugli elenchi di negati	21 marzo 2024

Aggiornamenti precedenti

La tabella seguente descrive le modifiche importanti alla documentazione della guida AMS Advanced prima di marzo 2024.

Modifica	Descrizione	Link
febbraio 2024		
Sistemi operativi supportati aggiornati	Sistemi operativi supportati aggiornati per includere SUSE Linux Enterprise Server 15 SP5.	Per informazioni, consultare Configurazioni supportate.
È stata aggiunta una nota agli avvisi del monitoraggio di base in AMS.	È stata aggiunta una nota che indica che l'allarme per l'utilizzo del volume EC2 non root è	Per informazioni, consultare Avvisi dal monitoraggio di base in AMS.

Modifica	Descrizione	Link
	disabilitato per impostazione predefinita.	
È stata aggiunta una nuova sezione AMS Event Router al monitoraggio e alla gestione degli eventi.	È stata aggiunta una nuova sezione che illustra l'AMS Advanced Event Router.	Per informazioni, consultare Utilizzo di Amazon EventBridge Managed Rules in AMS.
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	VediAMIs. csv-and-notes02.2024
febbraio 2024		
Aggiunta una nuova sezione per il ruolo collegato ad Amazon EventBridge rule service per AMS Advanced	È stata aggiunta una nuova sezione per il ruolo collegato ad Amazon EventBridge rule service per AMS Advanced nella sezione Infrastructure Security.	Vedi il ruolo collegato ai servizi di Amazon EventBridge rule per AMS Advanced
Sezione aggiornata sulla modalità di fornitura self-service	È stata aggiunta una nuova sezione per il nuovo Amazon Inspector in modalità Self Servicing Provision.	Vedi Amazon Inspector Classic (AMS SSPS)
gennaio 2024		
Sezione aggiornata sulla gestione degli eventi pianificati (PEM)	Sono stati aggiunti ulteriori dettagli e una FAW alla gestione degli eventi pianificati (PEM).	Per informazioni, consultare Gestione pianificata degli eventi in AWS Managed Services.

Modifica	Descrizione	Link
Aggiunta una nuova sezione per l'installazione automatica di SSM Agent	È stata aggiunta una nuova sezione per l'installazione automatica dell'agente SSM nella configurazione automatizzata dell' EC2 istanza.	Per informazioni, consultare Installazione automatica di SSM Agent.
Aggiunto AWS Resilience Hub (AMS SSPS)	Aggiunto un nuovo servizio SSPS.	Per informazioni, consultare Utilizza AMS SSP per il provisioning AWS Resilience Hub nel tuo account AMS.
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	VediAMIs. csv-and-notes01.2024
dicembre 2023		
Modalità Direct Change aggiornata in AMS	È stata aggiunta una nuova sottosezione, Casi d'uso della modalità Direct Change, alla modalità Direct Change in AMS.	Per informazioni, consultare Modalità Direct Change in AMS.
Aggiornato AWS Amplify (AMS SSPS)	Domande frequenti aggiornate per chiarire che è necessaria un'accettazione del rischio per richiedere Amplify.	Per informazioni, consultare Utilizza AMS SSP per il provisioning AWS Amplify nel tuo account AMS.
Nuovo AWS Elastic Disaster Recovery (AMS SSPS)	Aggiunto un nuovo servizio SSPS	Per informazioni, consultare Utilizza AMS SSP per il provisioning AWS Elastic Disaster Recovery nel tuo account AMS.

Modifica	Descrizione	Link
Nuovo servizio gestito da Amazon per Prometheus (AMS SSPS)	Aggiunto un nuovo servizio SSPS	Per informazioni, consultare Usa AMS SSP per fornire Amazon Managed Service for Prometheus nel tuo account AMS.
Aggiornata la sezione Come funziona la gestione della continuità.	È stata aggiunta una nuova sottosezione, monitoraggio e reportistica dei backup AMS.	Per informazioni, consultare Come funziona la gestione della continuità.
Nuovo Amazon DevOps Guru (AMS SSPS)	Aggiunto un nuovo servizio SSPS	Per informazioni, consultare Usa AMS SSP per effettuare il provisioning di Amazon DocumentDB (con compatibilità MongoDB) nel tuo account AMS.
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	VediAMIs. csv-and-notes12.2023
novembre 2023		
Amazon CloudWatch Synthetics (AMS SSPS) aggiornato	Aggiornato FAQs per utilizzare i nomi di ruolo corretti.	Per informazioni, consultare Usa AMS SSP per effettuare il provisioning di Amazon CloudWatch Synthetics nel tuo account AMS.
Modalità di provisioning self-service di Amazon API Gateway aggiornata	È stato aggiunto un ruolo aggiuntivo`customer_apigateway_cloudwatch_role` , alla sezione API Gateway.	Per informazioni, consultare Usa AMS SSP per effettuare il provisioning di Amazon API Gateway nel tuo account AMS.

Modifica	Descrizione	Link
È stato aggiunto un nuovo servizio alla modalità Self-service Provisioning	Aggiunto AWS Service Catalog AppRegistry alla sezione sulla modalità Self-Service Provisioning	Per informazioni, consultare Utilizza AMS SSP per il provisioning AWS Service Catalog AppRegistry nel tuo account AMS.
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	VediAMIs. csv-and-notes11.2023
settembre 2023		
Aggiunta una nota all'uso di Patch Orchestrator	È stata aggiunta la seguente nota alla sezione Utilizzo di Patch Orchestrator: «Gli avvisi di errore delle patch non vengono creati per le istanze con sistemi operativi non supportati o che vengono interrotte durante la finestra di manutenzione»	Per informazioni, consultare Gestione delle patch in AMS.
Crittografia dei dati aggiornata con servizi aggiuntivi	Servizi aggiunti alla crittografia dei dati in AMS.	Per informazioni, consultare Protezione dei dati in AMS.
Aggiunto un nuovo paragrafo ai messaggi di errore RFC.	È stato aggiunto un nuovo paragrafo per aggiungere il link Crea una richiesta di servizio.	Per informazioni, consultare Risoluzione degli errori RFC in AMS.
Nomi dei ruoli IAM corretti.	È stato corretto il nome del ruolo IAM customer_emr_cluster_autoscaling_role.	Per informazioni, consultare Modalità Self-Service Provisioning in AMS.

Modifica	Descrizione	Link
Informazioni di monitoraggio di base aggiornate	È stato rimosso il riferimento a due allarmi obsoleti. RDSRead LatencyAlarm RDSWrite LatencyAlarm	Per informazioni, consultare Avvisi dal monitoraggio di base in AMS.
agosto 2023		
Aggiunto: AMS Security Incident Response	È stata aggiunta documentazione per l'utilizzo di AMS Security Incident Response.	Per informazioni, consultare Risposta agli incidenti di sicurezza in AMS.
luglio 2023		
Aggiunto: provisioning IAM automatizzato	È stata aggiunta documentazione per l'utilizzo del provisioning IAM automatizzato.	Per informazioni, consultare Provisioning IAM automatizzato (AMS).
Aggiornamento: tabella dei ruoli di accesso	Aggiunti ruoli mancanti per AMS Access.	Per informazioni, consultare Ruoli IAM di accesso all'account cliente AMS.
giugno 2023		
Aggiornato: elenco degli avvisi RDS monitorati.	È stato aggiornato l'elenco degli avvisi RDS per il monitoraggio di base di AMS. Sono stati aggiunti 9 nuovi tipi di avvisi RDS e sono stati rimossi 3 tipi di avvisi RDS esistenti.	Per informazioni, consulta Avvisi dal monitoraggio di base in AMS.
Aggiornamento: tabella dei ruoli di accesso	Nuovi ruoli per AMS Security.	Per informazioni, consultare Ruoli IAM di accesso all'account cliente AMS.
maggio 2023		

Modifica	Descrizione	Link
Aggiornamento: politica sulla data di inizio della fatturazione del servizio.	Definizioni aggiornate della data di inizio della fatturazi one.	Per informazioni, consulta Termini chiave AMS.
aprile 2023		
Aggiornato: rapporto self-serv ice sulla fatturazione mensile.	Nota aggiunta: i report di fatturazione mensile sono disponibili solo in un account Management Payer (landing zone multi-account AMS Advanced), ma sono disponibi li per tutti gli account gestiti da AMS Accelerate collegati.	Per informazioni, consulta Rapporto di fatturazione (mensile).
Aggiornato: contenuto «Standard Patching» rimosso	AMS utilizza Patch Orchestra tor.	Gestione delle patch in AMS
Aggiornato: cos'è AMS?	Alcuni argomenti sono stati spostati in precedenza in Cos'è AMS? per far parte della descrizione del servizio AMS.	Descrizione del servizio
Aggiornato: Offboarding: landing zone multi-account	Ha fatto diverse precisazioni.	Fuori bordo dagli account AMS con più account landing zone
Aggiornamento: AWS Transfer Family (AMS SSPS)	È stato aggiunto un link al tutorial sulla configurazione del trasferimento.	Utilizza AMS SSP per il provisioning AWS Transfer Family nel tuo account AMS
Contenuto aggiornato: fornitura self-service	Sostituito CodeSuite "" con «Code services» per AWS legal.	Utilizza AMS SSP per fornire i servizi AMS Code nel tuo account AMS

Modifica	Descrizione	Link
Contenuto aggiornato: CloudWatch metriche e allarmi	Aggiunto link a Esempio: Conta le occorrenze di un termine.	Creazione di CloudWatch metriche e allarmi personalizzati in AMS
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	AMIs. csv-and-notes4.04.2023
marzo 2023		
Contenuto aggiornato: Offboarding da AMS	È stato chiarito quali risorse vengono eliminate quando si escono dagli account multi-account landing zone	Fuori bordo dagli account AMS con più account landing zone
Aggiornato: AMS AMIs	Aggiunto un collegamento al file ZIP AMI per ogni mese nella sezione Cronologia dei documenti.	Cronologia dei documenti
Aggiornato: riparazione automatica	È stato rimosso il supporto LVM per l'automazione dei EC2 volumi.	Correzione automatica degli avvisi con AMS
Aggiornato: Patch RACI	Diversi aggiornamenti e chiarimenti al RACI per l'applicazione delle patch.	Matrice di responsabilità AMS (RACI)
Contenuto aggiornato: fornitura self-service	È stato aggiunto un bullet per le domande frequenti. Per avviare un nuovo agente AWS Datasync, non è richiesta l'ingestione di WIGS.	Modalità Self-Service Provisioning in AMS

Modifica	Descrizione	Link
Contenuto aggiornato: fornitura self-service	È stato aggiunto un bullet per le domande frequenti. Per avviare un nuovo agente AWS Datasync, non è richiesta l'ingestione di WIGS.	Modalità Self-Service Provisioning in AMS
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	AMIs. csv-and-notes03/2023
febbraio 2023		
Contenuto aggiornato: Offboarding da AMS	È stato chiarito come effettuar e l'offboard di ambienti di landing zone con più account e account VPCs Application	Account AMS fuori bordo
Contenuto aggiornato: Finding ARNs	Aggiunta la CLI di `describe-table` DynamoDB per trovare una tabella DynamoDB ARN	Trova Amazon Resource Names (ARNs) in AMS

Modifica	Descrizione	Link
Contenuto aggiornato: Self-Service Provisioning	È stata rimossa l'opzione "CodeSuite" AMS in quanto non si tratta di un vero e proprio SSPS. È comunque possibile utilizzare l'opzione Management | AWS service | Self-provisioned service | Add (review required) (ct-3qe6io8t6jtny) cambia tipo e richiede i tre servizi:, e. CodeBuild CodeDeploy CodePipeline AMS fornirà quindi i seguenti ruoli IAM al tuo account:, e. `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 di federazione.	Modalità Self-Service Provisioning in AMS
Contenuto aggiornato: aggiornamento di Secrets Manager	Ruoli corretti necessari per multi-account landing zone (MALZ) e single-account landing zone (SALZ).	Domande frequenti sulla condivisione delle chiavi con Secrets Manager
Contenuto aggiornato: correzione automatica degli avvisi da parte di AMS	È stato aggiunto il supporto per i volumi Logical Volume Manager (LVM).	EC2 automazione della correzione dell'utilizzo dei volumi

Modifica	Descrizione	Link
Contenuto aggiornato: AMS Amazon Machine Images (AMIs)	È stata aggiunta la sezione Offboarding AMS AMIs con codice di esempio AMIs da rimuovere dal tuo account.	Immagini di macchine AMS Amazon (AMIs)
Contenuto aggiornato: IAM User Role	Aggiornamento della politica IAM: AMSBilling Policy.	Ruolo utente IAM in AMS
Nuovo contenuto: non supportato OSes	Sono state aggiunte informazioni sui servizi forniti da AMS per i sistemi operativi non supportati ()OSes.	Funzionalità per sistemi operativi non supportati in AMS
Contenuto aggiornato: report su richiesta	Alcuni report su richiesta non sono disponibili in AMS Advanced e sono stati erroneamente mostrati come disponibili.	Report su richiesta
Contenuto aggiornato: Offboarding AMS Accounts	Istruzioni chiarite per l'offboarding degli account dell'applicazione MALZ.	Account applicativi AMS Offboard
Contenuto aggiornato: Secrets Manager	Sono stati corretti i nomi dei ruoli IAM necessari per utilizzare Secrets Manager.	Domande frequenti su Secrets Manager in AWS Managed Services
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	AMIs. csv-and-notes02/2023
gennaio 2023		

Modifica	Descrizione	Link
Nuovi contenuti: AWS Device Farm (AMS SSPS)	Aggiunto un nuovo servizio SSPS: AWS Device Farm.	Utilizza AMS SSP per il provisioning AWS Device Farm nel tuo account AMS
Aggiornato: versioni di Windows supportate	È stato aggiunto il supporto per Windows Server 2022.	Immagini di macchine AMS Amazon (AMIs), Configurazioni supportate e Notifiche AMI AMS con SNS
Aggiornato: gestione della continuità	Sono state aggiornate le regole nel piano di backup AMS predefinito.	Piani di backup predefiniti, landing zone multi-account
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	AMIs. csv-and-notes0,01.2023
dicembre 2022		
Aggiornato: utilizzo dei bastioni	Corretto un collegamento errato.	Accesso alle istanze tramite bastioni
Aggiornato: Resource Scheduler	Sono stati apportati diversi miglioramenti e aggiunto collegamenti a AWS Instance Scheduler per un maggiore contesto.	AWS Managed Services Resource Scheduler

Modifica	Descrizione	Link
Aggiornato: Windows AMIs e configurazioni supportate (per i nuovi Windows) AMIs	Contenuti AMI AMS aggiornati aggiunti da EC2 Launch (Windows Server 2016 e versioni successive) a EC2 Launch (Windows Server 2016 e Windows Server 2019) e aggiunto EC2 LaunchV2 (Windows Server 2022 e versioni successive). Basato su Windows aggiornato da AMIs Microsoft Windows Server (2012, 2012 R2, 2016 e 2019) a Microsoft Windows Server (2012, 2012 R2, 2016, 2019 e 2022).	Immagini di macchine AMS Amazon (AMIs) e Descrizione del servizio
Aggiornamento: sezione Resourced Scheduler	Metodi migliorati per l'implementazione e la personalizzazione di AMS Resource Scheduler.	AWS Managed Services Resource Scheduler
Aggiornamento: configurazione di AMS: DNS privato e pubblico	Aggiornato il diagramma dell'architettura DNS.	Configurazione di DNS privati e pubblici
Aggiornato: architettura di rete MALZ	È stato aggiornato il diagramma e sono state aggiunte linee guida per gli account delle applicazioni Accelerate.	Architettura di rete MALZ

Modifica	Descrizione	Link
Aggiornato: configurazione: utilizzo dei tag	Nuova nota: i tag personalizzati sono supportati solo per gli account delle applicazioni MALZ, non per gli account principali.	Etichettatura automatica dell'infrastruttura AMS
Aggiornato: gestione degli accessi: utilizzo dei bastioni	Introduzione aggiornata per includere i bastioni RDP.	Riduzione dei costi sui bastioni della single-account landing zone (SALZ)
Aggiornato: impostazioni predefinite di AMS: avvisi	EC2 Istanza aggiunta: Non-Root Volume Usage alla tabella degli avvisi.	Avvisi dal monitoraggio di base in AMS
Aggiornato: Continuity Management	Sono state aggiunte indicazioni sui backup continui.	Come funziona la gestione della continuità
Aggiornato: configurazione automatica dell' EC2 istanza	È stato aggiunto il supporto per PowerBroker Identity Service (PBIS) e On Instance Code (OIC).	Aggiorna automaticamente PBIS su istanze Linux e Aggiorna automaticamente il codice sulle istanze Linux
Aggiornamento: Provisioning self-service per Secrets Manager	Aggiornato il CT per l'aggiunta di Secrets Manager al tuo account (sotto FAQs).	Utilizza AMS SSP per il provisioning Gestione dei segreti AWS nel tuo account AMS
Aggiornato: gestione dei registri	Aggiornato l'elenco dei log a EC2 livello di sistema.	Amazon Elastic Compute Cloud (Amazon EC2) - log a livello di sistema
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	AMIs. csv-and-notes.12,2022

Modifica	Descrizione	Link
novembre 2022		
Aggiornamento: AMS Amazon Machine Images (AMIs)	Versioni SUSE Linux supportate aggiornate.	Immagini di macchine AMS Amazon (AMIs)
Aggiornato: account MALZ	Sono state aggiunte linee guida per l'eliminazione di un account di applicazione gestito dal cliente.	Account applicativi gestiti dal cliente
Aggiornamento: configura zione di AMS	Aggiunto `customer-ams-amazon2-security-enhanced` .	Notifiche AMI AMS con SNS
Aggiornato: come funziona il monitoraggio	Spiegazione aggiornata delle notifiche di servizio e dei report sugli incidenti.	Come funziona il monitoraggio
Aggiornato: tipi di account dell'applicazione MALZ	Migliorata la spiegazione dei tipi di account.	Tipi di account dell'appl icazione
Aggiornato: modalità sviluppat ore	Aggiunto un avviso sulla modalità Sviluppatore.	Prima di iniziare con la modalità AMS Developer
Aggiornato: gestione pianifica ta degli eventi	Aggiunta la sezione: Tipi di PEM	Gestione pianificata degli eventi in AWS Managed Services
Aggiornamento: Amazon Machine Images (AMIs)	Versioni SUSE Linux supportate aggiornate	Immagini di macchine AMS Amazon (AMIs)
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	AMIs. csv-and-notes11.2022

Modifica	Descrizione	Link
ottobre 2022		
Novità: configurazione automatica delle istanze	La nuova sezione descrive il processo di configurazione automatizzata delle istanze.	Configurazione automatica delle istanze in AMS Advanced
Novità: solo la CT manuale è accettabile per alcuni SSPS	Il servizio di fornitura self-service di oltre 50 anni è stato aggiornato FAQs per utilizzare la CT manuale e non la CT automatizzata per l'aggiunta di SSPS.	Modalità Self-Service Provisioning in AMS
Aggiornamento: configurazione di AMS	Sono state aggiunte due policy ai profili delle istanze Amazon EC2 IAM per MALZ.	EC2 Profilo dell'istanza IAM
Novità: libreria di regole investigative e preventive personalizzate.	È stata aggiunta una serie di esempi di policy di controllo del servizio (SCPs) e controlli preventivi delle regole di Config basati sulle esperienze acquisite da più clienti.	Regole curate SCPs e di Config
Aggiornamento: avviso AWS Backup	È stato aggiunto un avviso: «Non modificate i piani di backup AMS poiché le modifiche potrebbero andare perse. Invece, crea nuovi piani di backup usando ct-2hyozbpa0sx0m per le tue configurazioni personalizzate».	Come funziona la gestione della continuità
AWS Backup Aggiornamento: attenzione	È stata aggiunta una nota sull'aggiunta di nuovi ruoli IAM alla federazione.	Implementazione di risorse IAM in AMS Advanced

Modifica	Descrizione	Link
Aggiornamento: gestione del monitoraggio	Gli avvisi generano report sugli incidenti, non richieste di assistenza.	Come funziona il monitoraggio
Aggiornamento: porta il tuo EPS	Si applica sia a SALZ che a MALZ.	AMS porta il tuo EPS
Aggiornamento: account Accelerate Application	Abbiamo chiarito che il tuo account Accelerate è un account Application.	Tipi di account dell'applicazione
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	AMIs. csv-and-notes10.2022
settembre 2022		
Aggiornato: esempi di comandi CLI per la ricerca di risorse	È stato aggiunto un nuovo esempio e l'`--region`opzione potrebbe essere necessaria.	Ricerca dei dati necessari (SKMS), AMS
Aggiornato: provisioning dei ruoli IAM	I ruoli IAM possono ora essere creati e gestiti con. `AWSManagedServices CloudFormationAdminRole`	Creazione di pile utilizzando la modalità Direct Change
Aggiornato: standard tecnici AMS	Registrazione AMS-STD-007: (#20) Requisiti di inoltro chiariti.	Sicurezza e conformità

Modifica	Descrizione	Link
Aggiornamento: come funziona la gestione della continuità	La formulazione di Start Backup Job è stata modificat a in «on-demand» anziché «esistente».	Come funziona la gestione della continuità
Aggiornato: sicurezza e conformità	Descrizione e linee guida aggiornate per lo standard AMS-STD-007 numero 20: inoltro dei log tra account.	Sicurezza e conformità
Aggiornamento: casi d'uso della gestione delle modifiche	È stato rimosso un collegame nto interrotto alla precedente Guida per l'utente di Change Management.	Casi d'uso della gestione delle modifiche
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	AMIs. csv-and-notes09.2022
11 agosto 2022		

Modifica	Descrizione	Link
Aggiornamento: per motivi di coerenza e leggibilità, i titoli dei capitoli sono stati spostati in sezioni più appropriate	«Architettura di rete MALZ» e «architettura di rete SALZ» sono ora entrambe sottosezioni della sezione «Architettura di rete» di primo livello, precedentemente denominata sezione «Architettura di rete AMS» «Modi per la gestione delle modifiche» è la nuova rubrica «Gestione delle modifiche» «Impostazioni predefinite» è ora una sottosezione di «Configurazione di AMS» «Regola di attestazione ADFS e impostazioni SAML» (precedentemente "regola di attestazione di ActiveDirectory Federation Services (ADFS) e impostazioni SAML) è ora una sottosezione di «Configurazione di AMS» «Gestione degli accessi» è la nuova rubrica «Accesso in AMS» e viene spostata in alto nel sommario «Trovare i dati necessari» è la nuova rubrica «Gestione della conoscenza dei servizi»	Che cos'è AWS Managed Services?

Modifica	Descrizione	Link
	«Rapporti e opzioni» è la nuova rubrica di «AMS Reporting» e si trova più in basso nel sommario «Operations on Demand» è ora l'ultimo argomento del sommario	
Aggiornato: Finding e ARN, Novità: ricerca di una risorsa con un ARN	Entrambe le procedure sono state completamente riscritte per motivi di utilità.	Trova Amazon Resource Names (ARNs) in AMS e Trova risorse tramite ARN in AMS.
Aggiornamento: connessione del CMA con Transit Gateway	L'automazione non supporta l'aggiunta di percorsi ai domini di routing principali e la procedura deve essere aggiornata.	Connessione del CMA con Transit Gateway
Aggiornato: prezzi dei componenti di base MALZ	Tutti i prezzi sono in dollari USA, formattati con i simboli del dollaro.	Componenti di base dell'ambiente AMS
Aggiornato: AMS AMI Notes	Il file zip include note sulle ultime immagini delle macchine AMS Amazon (AMIs) e un file CSV delle ultime AMIs.	AMIs. csv-and-notes08.2022
14 luglio 2022		
Aggiornato: reportistica self-service	Sono state aggiunte istruzioni per crittografare i AWS Glue metadati con le chiavi KMS.	Report self-service

Modifica	Descrizione	Link
Aggiornato: monitoraggio di base AMS	Aggiunto avviso DeleteRec overyPoint di backup.	Avvisi dal monitoraggio di base in AMS
Aggiornato: sistemi operativi supportati	Aggiunta la data di fine del supporto per Amazon Linux 2.	Configurazioni supportate
Aggiornato: Self-Service Provisioning	È stato aggiunto un prerequis ito per il Transfer SSPS. AWS	Utilizza AMS SSP per il provisioning AWS Transfer Family nel tuo account AMS
Aggiornato: AMS Reporting	È stata aggiunta una nota sulle regioni Opt-in.	Rapporti e opzioni
Aggiornato: corrispondenza e allegato RFC	Sono stati chiariti i tipi di file di testo consentiti; in particolare, i file YAML devono terminare con .yaml (non .yml).	Aggiungi corrispondenza e allegati RFC (console)
21 giugno 2022		
Contenuti aggiornati	La modalità AMS precedent emente nota come «modalità di gestione delle modifiche» o «modalità CM standard» è ora nota come «modalità RFC». La sezione delle modalità è stata ampliata.	Panoramica delle modalità.
Nuovo allarme	Aggiunta una AWS Backup sveglia.	Avvisi dal monitoraggio di base in AMS
16 giugno 2022		

Modifica	Descrizione	Link
Nuovo contenuto	Gestione degli incidenti . Gli incidenti che non rappresentano un rischio per la sicurezza possono ora essere risolti da AMS con l'approvazione dell'utente nel rapporto sull'incidente e non richiedono una RFC e un'approvazione separate.	Gestione degli incidenti
Contenuti aggiornati	MALZ: Diagramma dell'arch itettura di rete aggiornato. Aggiornamenti: il peering VPC per l'account principale VPC to shared services vpc deve essere rimosso in quanto non esiste.	Architettura degli account di rete
	Servizio self-service provision ed (SSPS) di Sagemaker . Aggiornato con un nuovo ruolo IAM aggiunto all'onboa rding per l'utilizzo da parte di Sagemaker.	Usa AMS SSP per effettuar e il provisioning di Amazon SageMaker AI nel tuo account AMS

Modifica	Descrizione	Link
	All'elenco delle notifiche SNS AMIs supportate: aggiunte customer-ams-sles 12, customer-ams-sles 15, customer-ams-amazon 1-security-enhanced, customer-ams-rhel 8, customer-ams-rhel 8-security-enhanced, 18, 2012, 2019 e 2019-secu rity-enhanced. customer-ams-ubuntu customer-ams-windows customer-ams-windows customer-ams-windows customer-ams-rhel AMIsRimossi 6 e 6-Security-Enhanced. customer-ams-rhel	Notifiche AMI AMS con SNS
	Email di escalation rimosse.	Ottenere assistenza in AWS Managed Services
	L'elenco degli argomenti è stato spostato sotto i paragrafi di apertura.	Che cos'è AWS Managed Services?
	Registri di servizio aggiornati con collegamenti migliori per i registri di bilanciamento del carico, anch'essi riformattati.	Log di servizio aggregati AMS
Servizio di fornitura self-serv ice EKS (SSPS). Sono state aggiunte informazioni sull'abil itazione della crittografia degli envelope secret nel cluster.	Usa AMS SSP per effettuare il provisioning di Amazon EKS AWS Fargate nel tuo account AMS	
09 giugno 2022		

Modifica	Descrizione	Link
Contenuti aggiornati, Come ricevere assistenza	Email con percorso di escalation rimosse. AMS fornisce metodi di comunicaz ione tramite segnalazioni di incidenti, richieste di assistenz a e. RFCs	Ottenere assistenza in AWS Managed Services
12 maggio 2022		
Nuovi contenuti, modello di abbonamento Operations on Demand (OOD)	AMS ha modificato l'onboard ing di Operations on Demand dall'attuale modello di registraz ione e rinnovo a un modello di allocazione degli abbonamen ti e di attivazione predefini to. Quando apri un account AMS, ora sei automatic amente iscritto a Operations on Demand.	Operazioni su richiesta
14 aprile 2022		
Nuovi contenuti, ottimizza zione dei costi	AMS fornisce consigli per l'ottimizzazione dei costi.	Ottimizzazione dei costi in AWS Managed Services
Contenuti aggiornati, account Accelerate in MALZ	Un nome di ruolo errato (CustomerDefaultAdminRole) è stato aggiornato con il nome di ruolo corretto (Accelera teDefaultAdminRole).	conti AMS AccelerateSezione «Accesso al tuo account Accelerate».
Contenuti aggiornati, accesso AMS ai ruoli IAM	Sono stati aggiunti altri ruoli AMS IAM utilizzati per accedere ai tuoi account.	Perché e quando AMS accede al tuo accountSezione «Accesso all'account cliente AMS ai ruoli IAM».

Modifica	Descrizione	Link
Contenuti aggiornati, piani di backup AMS	Aggiunti piani di backup gestiti da AMS.	Piani di backup AMS e casseforti di backup AMS
Contenuti aggiornati, AWS Secrets Manager	Sono state aggiornate le domande frequenti.	Utilizza AMS SSP per il provisioning Gestione dei segreti AWS nel tuo account AMS
Contenuti aggiornati, onboarding in Direct Change Mode (DCM)	AMS non supporta l'onboard ing dei clienti del Service Catalog su DCM.	Guida introduttiva alla modalità Direct Change
Contenuto aggiornato, descrizione del servizio	È stata chiarita la sezione Servizi supportati: • Amazon EKS su AWS Fargate -> Amazon Elastic Kubernetes Service su Fargate • Amazon ECS per Fargate -> Amazon Elastic Container Service su Fargate AWS • Amazon Kinesis -> Amazon Kinesis Data Streams	AWS Servizi supportati
Contenuti aggiornati, account MALZ Offboarding	Aggiornato per fare riferimen to a nuovi tipi di modifiche per gli account delle applicazioni di offboarding.	Account applicativi AMS Offboard

Modifica	Descrizione	Link
Contenuti aggiornati, gestione degli incidenti in modalità sviluppatore	Descrizione dello SLA dell'incidente aggiornata a: Lo SLA AMS non si applica alle risorse create o aggiornate al di fuori di AMS Change Management (modalità sviluppatore inclusa), pertanto, le risorse aggiornate o create in modalità Sviluppatore vengono automaticamente degradate a P3 e il supporto è il massimo sforzo.	Gestione degli incidenti in modalità AMS Developer
Contenuti aggiornati, onboarding DCM	Il modello RFC per il nuovo DCM ora include un campo per l'ARN del provider SAML.	Guida introduttiva alla modalità Direct Change
Contenuto aggiornato, DCM per CloudFormation	Le istruzioni per la creazione e l'aggiornamento CloudFormation degli stack ora includono esempi YAML.	Trasforma AMS
Contenuti aggiornati, account MALZ Tools	Esiste un nuovo ruolo IAM per le migrazioni:. `AWSManagedServicesMigrationRole`	AWS Servizio di migrazione delle applicazioni (AWS MGN) e Abilita l'accesso al nuovo account AMS Tools
Nuovi contenuti, account di landing zone con più account	Puoi creare un account Accelerate nel tuo account di gestione AMS per la landing zone multi-account.	conti AMS Accelerate

Modifica	Descrizione	Link
Contenuti aggiornati, installazione dell' API/CLI SDK	Le istruzioni di installazione Mac/Linux indicavano un nome di file errato per le installazioni e un comando errato. Questo problema è stato risolto.	Utilizzo dell'API e della CLI AMS
Contenuti aggiornati, account Accelerate in MALZ	Il nome della regola era errato (CustomerDefaultAdminRole), è stato aggiornato con quello corretto (AccelerateDefault AdminRole).	conti AMS Accelerate, sezione «Accesso al tuo account Accelerate»
Contenuti aggiornati, monitoraggio	Il monitoraggio dell'utilizzo dei root è stato rivisto dall'85% al 95%.	Avvisi dal monitoraggio di base in AMS
Contenuti aggiornati, notifiche AMI	Puoi creare molti tipi di notifiche SNS per i nuovi AMS AMIs, abbiamo aggiunto informazioni sulla creazione di vari tipi.	Notifiche AMI AMS con SNS
Contenuti aggiornati, impostazioni predefinite di AMS	Rimossi i riferimenti a Macie Classic, sostituiti da Macie.	Avvisi dal monitoraggio di base in AMS
Contenuti aggiornati, prefissi riservati AMS	Elenco alfabetico dei prefissi riservati.	Prefissi riservati AMS

Modifica	Descrizione	Link
Contenuto aggiornato, descrizione del servizio	Le sezioni relative alle funzionalità relative alla gestione delle modifiche e al provisioning self-service sono state aggiornate con ulteriori informazioni sulle modalità AMS.	AWS Managed Services (AMS) Caratteristiche del piano operativo AMS Advanced
Contenuti aggiornati, AWS Secrets Manager	Condivisione delle chiavi tramite Secrets Manager.	10 febbraio 2022
Nuovi contenuti, fornitura self-service, Amazon Connect	È stata aggiunta una domanda frequente su come richiedere l'aggiunta di un elenco di paesi per le chiamate in uscita o in entrata.	10 febbraio 2022
Nuovi contenuti, fornitura self-service, Amazon EKS su Fargate	È stata aggiunta una restrizio ne nelle domande frequenti secondo cui la distribuzione di cluster EKS tramite il AWS cloud development kit (CDK) o CloudFormation Ingest non è supportata in AMS.	10 febbraio 2022
Contenuto modificato, modalità sviluppatore	Correzione, non si utilizza una RFC o una richiesta di servizio per assegnare utenti alla soluzione di federazione, ma lo si fa autonomamente a seconda della soluzione.	10 febbraio 2022
Contenuto modificato, modalità Direct Change (DCM)	Tieni presente che IAM non è supportato in DCM.	10 febbraio 2022

Modifica	Descrizione	Link
	DCM, prendi nota delle convalide che eseguiamo.	10 febbraio 2022
	DCM, chiarisci le restrizioni dei diversi ruoli.	10 febbraio 2022
Contenuti modificati, monitoraggio degli avvisi di base	Gli avvisi sulle risorse del cluster Redshift sono stati modificati.	10 febbraio 2022
Contenuti modificati, reportistica self-service	È stato aggiunto il nome esatto del bucket s3, (ams-reporting-data-a<Account_ID>) che i clienti possono utilizzare per recuperare i report.	10 febbraio 2022

Modifica	Descrizione	Link
Contenuti modificati, contenuti aggiornati per fare riferimento ai tipi di modifica automatici anziché alla gestione manuale | Altro | Altro (MOO)	Contenuto aggiornato dell'account dell'applicazione multi-account landing zone (MALZ) per fare riferimento ai tipi di modifica automatizzata (tre, «Associazione dell'allegato TGW a una tabella di rotte», «Crea percorsi nelle tabelle delle rotte TGW per connetterti a questo VPC» e «Configurazione delle tabelle di routing VPC in modo che puntino al gateway di transito AMS Multi-Account Landing Zone»). Ricezione di avvisi generati da AMS Notifiche di avviso basate su tag	10 febbraio 2022
Contenuto modificato: AMS. AMIs	Sono state aggiunte nuove informazioni sulla sicurezza avanzata AMIs. VediConfigurazioni supportate,, Immagini di macchine AMS Amazon (AMIs) e. Sicurezza migliorata AMIs	27 gennaio 2022

Modifica	Descrizione	Link
Nuovi contenuti: fornitura self-service.	Aggiunto Amazon Fsx per OpenZFS. Per informazioni, consulta Usa AMS SSP per effettuare il provisioning di Amazon FSx for OpenZFS nel tuo account AMS.	27 gennaio 2022
Contenuto modificato: servizio di provisioning self-service (SSPS) Code-Deploy.	Nome del ruolo aggiuntivo e nota di restrizione aggiuntiva. Vedi. Utilizza AMS SSP per il provisioning AWS CodeDeploy nel tuo account AMS	27 gennaio 2022
Contenuto modificato: link aggiornati.	Collegamenti interrotti fissi: AMS-AMIs, Finding your settings, Finding a Stack ID, Finding a VPC ID ListVpcSummaries, ListStackSummaries, e. GetStack APIs Per un esempio, consulta Trova lo stack IDs in AMS.	13 gennaio 2022
Contenuto modificato: EKS Support for Fargate	Limitazione aggiunta a FAQs: La creazione o la gestione di EC2 gruppi di nodi con EKS non è supportata. Per informazioni, consulta Usa AMS SSP per effettuare il provisioning di Amazon EKS AWS Fargate nel tuo account AMS.	13 gennaio 2022

Modifica	Descrizione	Link
Contenuto modificato: CloudFormation Direct Change Mode (DCM)	Sono state aggiunte istruzioni per la creazione o l'aggiornamento di stack CF utilizzando. AmsStackTransform Per informazioni, consulta Creazione di pile utilizzando la modalità Direct Change.	13 gennaio 2022
Contenuto modificato: uniformità nei nomi dei servizi AWS	I riferimenti AMS devono corrispondere Servizi AWS esattamente ai AWS titoli o ai metadati ufficiali. In precedenza, c'erano piccole variazioni che complicavano la corrispondenza dei pattern. Per un esempio, consulta Usa AMS SSP per fornire Alexa for Business nel tuo account AMS.	13 gennaio 2022
Contenuto modificato: fornitura self-service di Elastic Container Registry (ECR)	È stata aggiunta una voce di domande frequenti sull'utilizzo di ECR per gestire le autorizzazioni degli utenti. Per informazioni, consulta Usa AMS SSP per effettuare il provisioning di Amazon Elastic Container Registry nel tuo account AMS.	13 gennaio 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.