Guida all'implementazione

Risposta di sicurezza automatizzata su AWS

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Risposta di sicurezza automatizzata su AWS: Guida all'implementazione

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

Panoramica della soluzione ... 1
Funzionalità e vantaggi ... 3
Casi d'uso ... 4
Concetti e definizioni ... 4
Panoramica dell'architettura ... 6
Diagramma architetturale ... 6
Considerazioni sulla progettazione di AWS Well-Architected ... 8
Eccellenza operativa ... 8
Sicurezza ... 8
Affidabilità ... 8
Efficienza delle prestazioni ... 9
Ottimizzazione dei costi ... 9
Sostenibilità ... 9
Dettagli architettonici ... 10
Integrazione con AWS Security Hub ... 10
Correzione tra account ... 10
Playbook ... 11
Registrazione centralizzata ... 11
Notifiche ... 12
Servizi AWS in questa soluzione ... 12
Pianifica la tua implementazione ... 14
Costo ... 14
Esempio di tabella dei costi ... 15
Esempi di prezzi (mensili) ... 20
Costo aggiuntivo per funzionalità opzionali ... 26
Sicurezza ... 28
Ruoli IAM ... 28
Regioni AWS supportate ... 28
Quote ... 30
Quote per i servizi AWS in questa soluzione ... 31
CloudFormation Quote AWS ... 31
CloudWatch Quote AWS ... 31
Amazon EventBridge regola le quote ... 31
Implementazione di AWS Security Hub ... 31

Stack e distribuzione StackSets ... 32
Implementa la soluzione ... 33
Decidere dove distribuire ogni stack ... 33
Decidere come distribuire ogni stack ... 34
Risultati di controllo consolidati ... 35
CloudFormation Modelli AWS ... 36
Supporto per account amministrativi ... 36
Ruoli dei membri ... 37
Account membri ... 37
Integrazione del sistema di ticket ... 38
Implementazione automatizzata - StackSets ... 38
Prerequisiti ... 38
Panoramica della distribuzione ... 39
(Facoltativo) Fase 0: Avvia uno stack di integrazione del sistema di ticket ... 41
Passaggio 1: avviare lo stack di amministrazione nell'account amministratore delegato di Security Hub ... 43
Fase 2: installa i ruoli di riparazione in ogni account membro di AWS Security Hub ... 44
Fase 3: Avvia lo stack di membri in ogni account membro e regione di AWS Security Hub ... 45
Distribuzione automatizzata - Stacks ... 47
Prerequisiti ... 47
Panoramica della distribuzione ... 47
(Facoltativo) Fase 0: Avvio di uno stack di integrazione del sistema di ticket ... 48
Fase 1: Avvia lo stack di amministrazione ... 50
Fase 2: installa i ruoli di riparazione in ogni account membro di AWS Security Hub ... 56
Passaggio 3: Avvia lo stack dei membri ... 58
Fase 4: (Facoltativo) Modifica le correzioni disponibili ... 63
Implementazione di Control Tower (CT) ... 64
Prerequisiti ... 64
Panoramica sulla distribuzione ... 64
Fase 1: Crea e distribuisci nel bucket S3 ... 66
Fase 2: distribuzione di Stacks su AWS Control Tower ... 69
Monitora le operazioni della soluzione con una CloudWatch dashboard di Amazon ... 73
Abilitazione di CloudWatch metriche, allarmi e dashboard ... 73
Utilizzo della dashboard CloudWatch ... 74
Modifica delle soglie di allarme ... 75
Iscrizione alle notifiche di allarme ... 78

Aggiornare la soluzione ... 79
Aggiornamento da versioni precedenti alla v1.4 ... 79
Aggiornamento dalla v1.4 e versioni successive ... 79
Aggiornamento dalla v2.0.x ... 79
Risoluzione dei problemi ... 81
Log delle soluzioni ... 81
Risoluzione di problemi noti ... 82
Problemi relativi a correzioni specifiche ... 84
PutS3 fallisce BucketPolicyDeny ... 85
Come disattivare la soluzione ... 85
Contattare Support. ... 86
Crea un caso ... 86
Come possiamo aiutarti? ... 87
Informazioni aggiuntive ... 87
Aiutaci a risolvere il tuo caso più velocemente ... 87
Risolvi subito o contattaci ... 87
Disinstalla la soluzione ... 88
V1.0.0-V1.2.1 ... 88
V1.3.x ... 88
V1.4.0 e versioni successive ... 89
Guida per amministratori ... 90
Abilitazione e disabilitazione di parti della soluzione ... 90
Esempio di notifiche SNS ... 91
Usa la soluzione ... 94
Tutorial: Guida introduttiva a Automated Security Response su AWS ... 94
Prepara i conti ... 94
Abilitazione di AWS Config ... 95
Abilita l'hub di sicurezza AWS ... 95
Abilita risultati di controllo consolidati ... 96
Configura l'aggregazione dei risultati tra regioni ... 97
Designare un account amministratore del Security Hub ... 97
Crea i ruoli per le autorizzazioni StackSets autogestite ... 98
Crea le risorse non sicure che genereranno risultati di esempio ... 99
Crea gruppi di CloudWatch log per i controlli correlati ... 100
Implementa la soluzione negli account tutorial ... 101
Implementa lo stack di amministrazione ... 101

Distribuisci lo stack dei membri ... 101
Implementa lo stack di ruoli dei membri ... 102
Iscriviti all'argomento SNS ... 103
Correggi i risultati degli esempi ... 103
Avvia la riparazione ... 104
Conferma che la riparazione ha risolto il problema ... 104
Traccia l'esecuzione della riparazione ... 104
EventBridge regola ... 104
Esecuzione di Step Functions ... 105
Automazione SSM ... 105
CloudWatch Gruppo di log ... 105
Abilita riparazioni completamente automatizzate ... 105
Conferma di non disporre di risorse a cui questo risultato potrebbe essere applicato accidentalmente ... 105
Abilita la regola ... 106
Configura la risorsa ... 106
Conferma che la correzione ha risolto il problema ... 107
Eliminazione ... 107
Eliminate le risorse di esempio ... 107
Elimina lo stack di amministrazione ... 108
Elimina lo stack di membri ... 108
Elimina lo stack dei ruoli dei membri ... 108
Eliminare i ruoli mantenuti ... 109
Pianifica l'eliminazione delle chiavi KMS conservate ... 109
Elimina gli stack per le autorizzazioni StackSets autogestite ... 110
Guida per sviluppatori ... 111
Codice sorgente ... 111
Playbook ... 111
Aggiungere nuove correzioni ... 183
Panoramica del flusso di lavoro manuale ... 184
Panoramica del flusso di lavoro CDK ... 185
Aggiungere un nuovo playbook ... 192
AWS Systems Manager Parameter Store ... 192
Argomento di Amazon SNS: avanzamento della riparazione ... 193
Filtraggio di un abbonamento a un argomento SNS ... 194
Argomento Amazon SNS: allarmi CloudWatch ... 195

Avvia Runbook su Config Findings 195
Riferimento 197
Raccolta di dati anonimizzata 197
Risorse correlate 198
Collaboratori 198
Revisioni 200
Note 201
..... ccii

Affronta automaticamente le minacce alla sicurezza con azioni di risposta e riparazione predefinite in AWS Security Hub

Questa guida all'implementazione fornisce una panoramica della soluzione Automated Security Response on AWS, della sua architettura e dei suoi componenti di riferimento, considerazioni per la pianificazione della distribuzione, i passaggi di configurazione per la distribuzione della soluzione Automated Security Response on AWS nel cloud Amazon Web Services (AWS).

Utilizza questa tabella di navigazione per trovare rapidamente le risposte a queste domande:

Se vuoi.	Leggi..
Conosci il costo di esecuzione di questa soluzione	Costo
Comprendi le considerazioni sulla sicurezza di questa soluzione	Sicurezza
Scopri come pianificare le quote per questa soluzione	Quote
Scopri quali regioni AWS sono supportate per questa soluzione	Regioni AWS supportate
Visualizza o scarica il CloudFormation modello AWS incluso in questa soluzione per distribuire automaticamente le risorse dell'infrastruttura (lo «stack») per questa soluzione	CloudFormation Modelli AWS
Accedi al codice sorgente e, facoltativamente, utilizza AWS Cloud Development Kit (AWS CDK) per distribuire la soluzione.	GitHub repository

La continua evoluzione della sicurezza richiede misure proattive per proteggere i dati, il che può rendere difficile, costosa e dispendiosa in termini di tempo la reazione dei team di sicurezza. La

soluzione Automated Security Response on AWS ti aiuta a reagire rapidamente per risolvere i problemi di sicurezza fornendo risposte predefinite e azioni correttive basate sugli standard di conformità del settore e sulle migliori pratiche.

Automated Security Response on AWS è una soluzione AWS che funziona con AWS Security Hub per migliorare la sicurezza e aiuta ad allineare i carichi di lavoro alle best practice fondamentali di Well-Architected Security (0). SEC1 Questa soluzione consente ai clienti di AWS Security Hub di risolvere più facilmente problemi di sicurezza comuni e migliorare la propria posizione di sicurezza in AWS.

È possibile selezionare playbook specifici da distribuire nell'account principale di Security Hub. Ogni playbook contiene le azioni personalizzate necessarie, i ruoli Identity and Access Management (IAM), EventBridge le regole Amazon, i documenti di automazione AWS Systems Manager, le funzioni AWS Lambda e AWS Step Functions necessari per avviare un flusso di lavoro di riparazione all'interno di un singolo account AWS o tra più account. Le riparazioni funzionano dal menu Azioni in AWS Security Hub e consentono agli utenti autorizzati di correggere un risultato su tutti i loro account gestiti da AWS Security Hub con un'unica azione. Ad esempio, puoi applicare i consigli del Center for Internet Security (CIS) AWS Foundations Benchmark, uno standard di conformità per la protezione delle risorse AWS, per garantire che le password scadano entro 90 giorni e applicare la crittografia dei log degli eventi archiviati in AWS.

> **Note**
>
> La riparazione è destinata a situazioni emergenti che richiedono un'azione immediata. Questa soluzione apporta modifiche ai risultati di correzione solo se avviata dall'utente tramite la console di gestione AWS Security Hub o quando la correzione automatica è stata abilitata utilizzando la EventBridge regola Amazon per un controllo specifico. Per ripristinare queste modifiche, è necessario riportare manualmente le risorse allo stato originale.
> Quando correggi le risorse AWS distribuite come parte dello CloudFormation stack, tieni presente che ciò potrebbe causare una deriva. Quando possibile, correggi le risorse dello stack modificando il codice che definisce le risorse dello stack e aggiornando lo stack. Per ulteriori informazioni, consulta What is drift? nella AWS CloudFormation User Guide.

Automated Security Response on AWS include il playbook di correzioni per gli standard di sicurezza definiti come parte di quanto segue:

- Centro per la sicurezza Internet (CIS) AWS Foundations Benchmark v1.2.0

- Benchmark CIS AWS Foundations v1.4.0
- Benchmark CIS AWS Foundations versione 3.0.0
- Best practice di sicurezza AWS Foundational (FSBP) v.1.0.0
- Standard di sicurezza dei dati del settore delle carte di pagamento (PCI-DSS) v3.2.1
- Istituto nazionale di standard e tecnologia (NIST) SP 800-53 Rev. 5

La soluzione include anche un playbook Security Controls (SC) per la funzionalità di risultati di controllo consolidati di AWS Security Hub. Per ulteriori informazioni, consulta Playbook.

Questa guida all'implementazione illustra le considerazioni architettoniche e le fasi di configurazione per la distribuzione della soluzione Automated Security Response on AWS nel cloud AWS. Include collegamenti a CloudFormation modelli AWS che avviano, configurano ed eseguono i servizi di calcolo, rete, storage e altri servizi AWS necessari per distribuire questa soluzione su AWS, utilizzando le best practice di AWS per la sicurezza e la disponibilità.

La guida è destinata agli architetti, agli amministratori e DevOps ai professionisti dell'infrastruttura IT che hanno esperienza pratica di architettura nel cloud AWS.

Funzionalità e vantaggi

L'Automated Security Response on AWS offre le seguenti funzionalità:

Correggi automaticamente i risultati per controlli specifici

Attiva EventBridge le regole Amazon per i controlli per correggere automaticamente i risultati relativi a tale controllo subito dopo la loro pubblicazione in AWS Security Hub.

Gestisci le riparazioni su più account e regioni da un'unica posizione

Da un account amministratore di AWS Security Hub configurato come destinazione di aggregazione per gli account e le regioni della tua organizzazione, avvia una correzione per un risultato in qualsiasi account e regione in cui è distribuita la soluzione.

Ricevi notifiche sulle azioni correttive e sui risultati

Iscriviti all'argomento Amazon SNS distribuito dalla soluzione per ricevere una notifica quando vengono avviate le riparazioni e se la riparazione ha avuto successo o meno.

Integra con sistemi di ticket come Jira o ServiceNow

Per aiutare l'organizzazione a reagire alle correzioni (ad esempio, l'aggiornamento del codice dell'infrastruttura), questa soluzione può inviare i ticket al sistema di ticketing esterno.

Usa AWSConfig le riparazioni nelle partizioni GovCloud e in Cina

Alcune delle riparazioni incluse nella soluzione sono riconfezionamenti di documenti di AWSConfig Remediation di proprietà di AWS disponibili nella partizione commerciale ma non in Cina. GovCloud Implementa questa soluzione per utilizzare questi documenti in quelle partizioni.

Estendi la soluzione con correzioni personalizzate e implementazioni di Playbook

La soluzione è progettata per essere estensibile e personalizzabile. Per specificare un'implementazione di riparazione alternativa, distribuisci documenti di automazione AWS Systems Manager personalizzati e AWS IAM Roles. Per supportare un set completamente nuovo di controlli non implementato dalla soluzione, distribuisci un Playbook personalizzato.

Casi d'uso

Implementa la conformità a uno standard in tutti gli account e le aree geografiche della tua organizzazione

Implementa il Playbook per uno standard (ad esempio, AWS Foundational Security Best Practices) per poter utilizzare le correzioni fornite. Avvia automaticamente o manualmente le riparazioni per le risorse in qualsiasi account e regione in cui è distribuita la soluzione per correggere le risorse che non sono conformi.

Implementa soluzioni o playbook personalizzati per soddisfare le esigenze di conformità della tua organizzazione

Utilizza i componenti Orchestrator forniti come framework. Crea soluzioni personalizzate per gestire le out-of-compliance risorse in base alle esigenze specifiche della tua organizzazione.

Concetti e definizioni

Questa sezione descrive i concetti chiave e definisce la terminologia specifica di questa soluzione:

riparazione, manuale di correzione

Un'implementazione di una serie di passaggi che risolve un problema. Ad esempio, una correzione per il controllo Security Control (SC) Lambda.1 «Le politiche della funzione Lambda dovrebbero

proibire l'accesso pubblico» modificherebbe la policy della funzione AWS Lambda pertinente per rimuovere le istruzioni che consentono l'accesso pubblico.

control runbook

Uno dei set di documenti di automazione di AWS Systems Manager (SSM) utilizzati da Orchestrator per indirizzare una correzione avviata per un controllo specifico al runbook di riparazione corretto. Ad esempio, le riparazioni per SC Lambda.1 e AWS Foundational Security Best Practices (FSBP) Lambda.1 sono implementate con lo stesso runbook di correzione. L'Orchestrator richiama il runbook di controllo per ogni controllo, che sono denominati rispettivamente ASR-AFSBP_Lambda.1 e ASR-SC_2.0.0_Lambda.1. Ogni runbook di controllo richiama lo stesso runbook di correzione, che in questo caso sarebbe ASR-. RemoveLambdaPublicAccess

orchestratore

Step Functions è distribuito dalla soluzione che prende come input un oggetto di ricerca da AWS Security Hub e richiama il runbook di controllo corretto nell'account e nella regione di destinazione. L'Orchestrator notifica inoltre alla soluzione SNS Topic quando la riparazione viene avviata e quando la riparazione ha esito positivo o negativo.

standard

Un gruppo di controlli definito da un'organizzazione come parte di un framework di conformità. Ad esempio, uno degli standard supportati da AWS Security Hub e da questa soluzione è AWS FSBP.

controllo

Una descrizione delle proprietà che una risorsa dovrebbe o non dovrebbe avere per essere conforme. Ad esempio, il controllo AWS FSBP Lambda.1 afferma che AWS Lambda Functions dovrebbe vietare l'accesso pubblico. Una funzione che consente l'accesso pubblico fallirebbe questo controllo.

risultati di controllo consolidati, controllo di sicurezza, visualizzazione dei controlli di sicurezza

Una funzionalità di AWS Security Hub che, quando attivata, mostra i risultati con il relativo controllo consolidato IDs anziché IDs quelli corrispondenti a uno standard particolare. Ad esempio, i controlli AWS FSBP S3.2, CIS v1.2.0 2.3, CIS v1.4.0 2.1.5.2 e PCI-DSS v3.2.1 S3.1 sono tutti mappati al controllo consolidato (SC) S3.2 «I bucket S3 dovrebbero vietare l'accesso pubblico in lettura». Quando questa funzionalità è attivata, vengono utilizzati i runbook SC.

Per un riferimento generale ai termini di AWS, consulta il Glossario AWS.

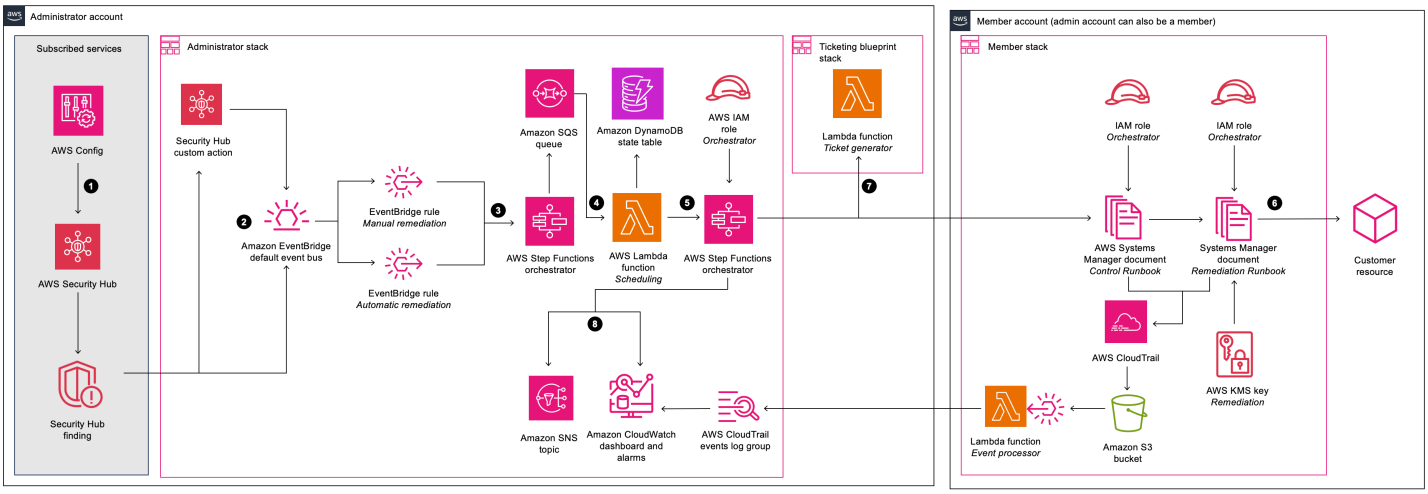
Panoramica dell'architettura

Questa sezione fornisce un diagramma dell'architettura di implementazione di riferimento per i componenti distribuiti con questa soluzione.

Diagramma architetturale

La distribuzione di questa soluzione con i parametri predefiniti crea il seguente ambiente nel cloud AWS.

Security Response automatizzato sull'architettura AWS



> **Note**
>
> Le CloudFormation risorse AWS vengono create a partire da costrutti di AWS Cloud Development Kit (AWS CDK).

Il flusso di processo di alto livello per i componenti della soluzione distribuiti con il CloudFormation modello AWS è il seguente:

1. Detect: AWS Security Hub offre ai clienti una visione completa del loro stato di sicurezza AWS. Li aiuta a misurare il loro ambiente rispetto agli standard e alle migliori pratiche del settore della sicurezza. Funziona raccogliendo eventi e dati da altri servizi AWS, come AWS Config, Amazon Guard Duty e AWS Firewall Manager. Questi eventi e dati vengono analizzati rispetto a standard

di sicurezza, come CIS AWS Foundations Benchmark. Le eccezioni vengono dichiarate come risultati nella console AWS Security Hub. Le nuove scoperte vengono inviate come EventBridge eventi Amazon.

2. Avvia: puoi avviare eventi in base ai risultati utilizzando azioni personalizzate, che generano eventi. EventBridge Le azioni e le EventBridge regole personalizzate di AWS Security Hub avviano Automated Security Response sui playbook AWS per risolvere i risultati. La soluzione implementa:

   a. Una EventBridge regola da abbinare all'evento di azione personalizzato

   b. Una regola di EventBridge evento per ogni controllo supportato (disattivata per impostazione predefinita) in modo che corrisponda all'evento di ricerca in tempo reale

   È possibile utilizzare il menu Azioni personalizzate nella console Security Hub per avviare la riparazione automatica. Dopo attenti test in un ambiente non di produzione, puoi anche attivare le riparazioni automatiche. È possibile attivare le automazioni per le singole riparazioni: non è necessario attivare gli avviamenti automatici per tutte le riparazioni.

3. Pre-riparazione: nell'account amministratore, AWS Step Functions elabora l'evento di riparazione e lo prepara per la pianificazione.

4. Pianificazione: la soluzione richiama la funzione di pianificazione di AWS Lambda per inserire l'evento di riparazione nella tabella di stato di Amazon DynamoDB.

5. Orchestrate: nell'account amministratore, Step Functions utilizza ruoli AWS Identity and Access Management (IAM) multiaccount. Step Functions richiama la correzione nell'account membro contenente la risorsa che ha prodotto il risultato di sicurezza.

6. Correzione: un documento AWS Systems Manager Automation nell'account membro esegue l'azione necessaria per correggere il risultato sulla risorsa di destinazione, come disabilitare l'accesso pubblico Lambda.

   Facoltativamente, puoi abilitare la funzionalità Action Log negli stack dei membri con il parametro Log. EnableCloudTrailFor ASRAction Questa funzionalità acquisisce le azioni intraprese dalla soluzione nei tuoi account Membro e le visualizza nella CloudWatch dashboard Amazon della soluzione.

7. (Facoltativo) Crea un ticket: se utilizzi il TicketGenFunctionNameparametro per abilitare il ticketing nello stack di amministrazione, la soluzione richiama la funzione Lambda del generatore di ticket fornita. Questa funzione Lambda crea un ticket nel servizio di biglietteria dopo che la riparazione è stata eseguita correttamente nell'account del membro. Forniamo stack per l'integrazione con Jira e. ServiceNow

8. Notifica e registra: il playbook registra i risultati in un gruppo di CloudWatch log, invia una notifica a un argomento di Amazon Simple Notification Service (Amazon SNS) e aggiorna i risultati del Security Hub. La soluzione mantiene una traccia di controllo delle azioni nelle note dei risultati.

Considerazioni sulla progettazione di AWS Well-Architected

Questa soluzione è stata progettata con le migliori pratiche di AWS Well-Architected Framework che aiutano i clienti a progettare e gestire carichi di lavoro affidabili, sicuri, efficienti ed economici nel cloud. Questa sezione descrive come sono stati applicati i principi di progettazione e le best practice del Well-Architected Framework durante la creazione di questa soluzione.

Eccellenza operativa

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'eccellenza operativa.

- Risorse definite come IaC utilizzando. CloudFormation
- Correzioni implementate con le seguenti caratteristiche, ove possibile:
  - Idempotenza
  - Gestione e segnalazione degli errori
  - Registrazione
  - Ripristino delle risorse a uno stato noto in caso di errore

Sicurezza

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro della sicurezza.

- IAM utilizzato per l'autenticazione e l'autorizzazione.
- L'ambito delle autorizzazioni di ruolo è stato progettato per essere il più ristretto possibile, sebbene in molti casi questa soluzione richieda autorizzazioni jolly per poter agire su qualsiasi risorsa.

Affidabilità

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'affidabilità.

- Security Hub continua a creare risultati se la causa alla base del risultato non viene risolta mediante la correzione.
- I servizi serverless consentono alla soluzione di scalare in base alle esigenze.

Efficienza delle prestazioni

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'efficienza delle prestazioni.

- Questa soluzione è stata progettata per essere una piattaforma da estendere senza dover implementare personalmente l'orchestrazione e le autorizzazioni.

Ottimizzazione dei costi

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro dell'ottimizzazione dei costi.

- I servizi serverless ti consentono di pagare solo ciò che utilizzi.
- Utilizza il livello gratuito per l'automazione SSM in ogni account

Sostenibilità

Questa sezione descrive come abbiamo progettato questa soluzione utilizzando i principi e le migliori pratiche del pilastro della sostenibilità.

- I servizi serverless consentono la scalabilità verso l'alto o verso il basso in base alle esigenze.

Dettagli dell'architettura

Questa sezione descrive i componenti e i servizi AWS che compongono questa soluzione e i dettagli dell'architettura su come questi componenti interagiscono.

Integrazione con AWS Security Hub

La distribuzione `automated-security-response-admin` dello stack crea l'integrazione con la funzionalità di azione personalizzata di AWS Security Hub. Quando gli utenti della console AWS Security Hub selezionano Findings for remediation, la soluzione indirizza il record di ricerca per la correzione utilizzando AWS Step Functions.

Le autorizzazioni per più account e i runbook di AWS Systems Manager devono essere distribuiti a tutti gli account AWS Security Hub (amministratore e membro) utilizzando i modelli and. `automated-security-response-member.template` `automated-security-response-member-roles.template` CloudFormation Per ulteriori informazioni, consulta Playbooks. Questo modello consente la riparazione automatica nell'account di destinazione.

Gli utenti possono avviare automaticamente riparazioni automatiche in base alla singola riparazione utilizzando le regole degli eventi di Amazon. CloudWatch Questa opzione attiva la correzione completamente automatica dei risultati non appena vengono segnalati ad AWS Security Hub. Per impostazione predefinita, le iniziazioni automatiche sono disattivate. Questa opzione può essere modificata in qualsiasi momento durante o dopo l'installazione del playbook attivando le regole CloudWatch degli eventi nell'account amministratore di AWS Security Hub.

Correzione tra account

Automated Security Response on AWS utilizza ruoli multiaccount per funzionare su account primari e secondari utilizzando ruoli multiaccount. Questi ruoli vengono distribuiti agli account dei membri durante l'installazione della soluzione. A ogni riparazione viene assegnato un ruolo individuale. Al processo di riparazione nell'account principale viene concessa l'autorizzazione ad assumere il ruolo di riparazione nell'account che richiede la riparazione. La riparazione viene eseguita dai runbook di AWS Systems Manager in esecuzione nell'account che richiede la riparazione.

Playbook

Una serie di rimedi è raggruppata in un pacchetto chiamato playbook. I playbook vengono installati, aggiornati e rimossi utilizzando i modelli di questa soluzione. Per informazioni sulle correzioni supportate in ogni playbook, consulta la Guida per gli sviluppatori → Playbook. Questa soluzione attualmente supporta i seguenti playbook:

- Security Control, un playbook allineato alla funzionalità Consolidated control results di AWS Security Hub, pubblicato il 23 febbraio 2023.

> **Important**
>
> Quando i risultati del controllo consolidato sono abilitati in Security Hub, questo è l'unico playbook che deve essere abilitato nella soluzione.

- Benchmark Amazon Web Services Foundations del Center for Internet Security (CIS), versione 1.2.0, pubblicati il 18 maggio 2018.
- Benchmark di Amazon Web Services Foundations del Center for Internet Security (CIS), versione 1.4.0, pubblicati il 9 novembre 2022.
- Benchmark Amazon Web Services Foundations del Center for Internet Security (CIS), versione 3.0.0, pubblicati il 13 maggio 2024.
- AWS Foundational Security Best Practices (FSBP) versione 1.0.0, pubblicata a marzo 2021.
- Payment Card Industry Data Security Standards (PCI-DSS) versione 3.2.1, pubblicata a maggio 2018.
- Versione 5.0.0 del National Institute of Standards and Technology (NIST), pubblicata a novembre 2023.

Registrazione centralizzata

Automated Security Response on AWS registra un singolo gruppo di CloudWatch log, SO0111-ASR. Questi log contengono registrazioni dettagliate della soluzione per la risoluzione dei problemi e la gestione della soluzione.

Notifiche

Questa soluzione utilizza un argomento Amazon Simple Notification Service (Amazon SNS) per pubblicare i risultati della correzione. Puoi utilizzare gli abbonamenti a questo argomento per estendere le funzionalità della soluzione. Ad esempio, è possibile inviare notifiche e-mail e aggiornare i ticket di assistenza.

- SO0111-ASR_topic — Utilizzato per inviare informazioni generali e messaggi di errore relativi alle riparazioni eseguite.
- SO0111-ASR_Alarm_topic — Utilizzato per notificare quando viene attivato uno degli allarmi della soluzione, a indicare che la soluzione non funziona come previsto.

Servizi AWS in questa soluzione

La soluzione utilizza i seguenti servizi. I servizi di base sono necessari per utilizzare la soluzione e i servizi di supporto collegano i servizi principali.

Servizio AWS	Descrizione
Amazon EventBridge	Core. Implementa eventi che avvieranno la funzione orchestator step quando viene corretto un risultato.
AWS IAM	Nucleo. Implementa molti ruoli per consentire riparazioni su risorse diverse.
AWS Lambda	Core. Implementa più funzioni lambda che verranno utilizzate dallo step function orchestat or per risolvere i problemi.
AWS Security Hub	Core. Fornisce ai clienti una visione completa dello stato di sicurezza di AWS.
AWS Step Functions	Core. Implementa un orchestratore che richiamerà i documenti di riparazione con chiamate API AWS Systems Manager.

Servizio AWS	Descrizione
AWS Systems Manager	Nucleo. Implementa i documenti di System Manager (collegamento al documento) che contengono la logica di riparazione che verrà eseguita.
AWS CloudTrail	Supporto. Registra le modifiche apportate dalla soluzione alle risorse AWS e le visualizza su un CloudWatch pannello di controllo.
Amazon CloudWatch	Supporto. Implementa gruppi di log che i diversi playbook utilizzeranno per registrare i risultati . Raccoglie metriche da visualizzare su una dashboard personalizzata con allarmi.
AWS DynamoDB	Supporto. Memorizza l'ultima correzione eseguita in ogni account e regione per ottimizza re la pianificazione delle riparazioni.
Amazon Simple Notification Service	Supporto. Implementa argomenti SNS che ricevono una notifica una volta completata una correzione.
AWS SQS	Supporto. Aiuta a pianificare le riparazioni in modo che la soluzione possa eseguire le riparazioni in parallelo.
AWS Key Management Service	Supporto. Utilizzato per crittografare i dati a scopo di riparazione.
AWS Config	Supporto. Registra tutte le risorse da utilizzare con AWS Security Hub.

Pianifica la tua implementazione

Questa sezione descrive i costi, la sicurezza della rete, le regioni AWS supportate, le quote e altre considerazioni prima di implementare la soluzione.

Costo

Sei responsabile del costo dei servizi AWS utilizzati per eseguire questa soluzione.

A partire da questa revisione, i costi mensili stimati sono:

- Implementazione su piccola scala (10 account, 1 regione: Stati Uniti) East/N. Virginia): Approximately $21.17 for 300 remediations/month
- Implementazione media (100 account, 1 regione: Stati Uniti) East/N. Virginia): Approximately $134.86 for 3,000 remediations/month
- Implementazione su larga scala (1.000 account, 10 regioni): circa 10.271,70 USD per 30.000 riparazioni al mese

> **Important**
>
> I prezzi sono soggetti a modifiche. Per tutti i dettagli, consulta la pagina dei prezzi di ogni servizio AWS utilizzato in questa soluzione.

> **Note**
>
> Molti servizi AWS includono un piano gratuito, una quantità di base del servizio che i clienti possono utilizzare gratuitamente. I costi effettivi possono essere superiori o inferiori agli esempi di prezzo forniti.

Ti consigliamo di creare un budget tramite AWS Cost Explorer per gestire i costi. I prezzi sono soggetti a modifiche. Per tutti i dettagli, consulta la pagina web dei prezzi per ogni servizio AWS utilizzato in questa soluzione.

Esempio di tabella dei costi

Il costo totale di esecuzione di questa soluzione dipende dai seguenti fattori:

- Il numero di account membri di AWS Security Hub
- Il numero di riparazioni attive richiamate automaticamente
- La frequenza delle riparazioni

Questa soluzione utilizza i seguenti componenti AWS, che comportano un costo in base alla configurazione. Vengono forniti esempi di prezzi per organizzazioni di piccole, medie e grandi dimensioni.

Servizio	Piano gratuito	Prezzi [USD]
AWS Systems Manager Automation - Step Count	100.000 passaggi per account al mese	Oltre al livello gratuito, per ogni passaggio base viene addebitato un costo di 0,002 USD per passaggio. Per le automazioni con più account, tutti i passaggi, inclusi quelli eseguiti in qualsiasi account per bambini, vengono conteggiati solo nell'account di origine.
AWS Systems Manager Automation - Durata della fase	5.000 secondi al mese	Oltre al piano gratuito, ogni fase di azione di AWS:ExecuteScript viene addebitata a 0,00003 USD al secondo dopo un livello gratuito di 5.000 secondi al mese.
AWS Systems Manager Automation - Archiviazione	Nessun livello gratuito	0,046 USD per GB al mese

Servizio	Piano gratuito	Prezzi [USD]
AWS Systems Manager Automation - Trasferimento dati	Nessun livello gratuito	0,900 USD per GB trasferito (per più account o) out-of-Region
AWS Security Hub - Controlli di sicurezza	Nessun piano gratuito	I primi 100.000 dollari checks/account/Region/month costano 0,0010 USD per assegno I successivi 400.000 dollari checks/account/Region/month costano 0,0008 USD per assegno Oltre 500.000 dollari checks/account/Region/month costano 0,0005 USD per assegno
AWS Security Hub - Ricerca degli eventi di importazione	I primi 10.000 sono events/account/Region/month gratuiti. Individuazione degli eventi di ingestione associati ai controlli di sicurezza di Security Hub.	Oltre 10.000 dollari events/account/Region/month costano 0,00003 dollari per evento

Servizio	Piano gratuito	Prezzi [USD]
Amazon CloudWatch - Metriche	Metriche di monitoraggio di base (con frequenza di 5 minuti) 10 metriche di monitoraggio dettagliate (con frequenza di 1 minuto) 1 milione di richieste API (non applicabile a e) GetMetricData GetMetricWidgetImage	I primi 10.000 parametri costano 0,30 dollari metrici al mese Le successive 240.000 metriche costano 0,10 USD metrici al mese I successivi 750.000 parametri costano 0,05 USD metrici al mese Oltre 1.000.000 di parametri costano 0,02 USD metrici al mese Le chiamate API costano 0,01 USD per 1.000 richieste
Amazon CloudWatch - Pannello di controllo	3 dashboard per un massimo di 50 metriche al mese	3,00 USD per dashboard al mese

Servizio	Piano gratuito	Prezzi [USD]
Amazon CloudWatch - Allarmi	10 parametri di allarme (non applicabile agli allarmi ad alta risoluzione)	La risoluzione standard (60 sec) costa 0,10 USD per metrica di allarme L'alta risoluzione (10 sec) costa 0,30 USD per metrica di allarme Il rilevamento delle anomalie a risoluzione standard costa 0,30 USD per allarme Il rilevamento delle anomalie ad alta risoluzione costa 0,90 USD per allarme Il materiale composito costa 0,50 USD per allarme
Amazon CloudWatch - Raccolta di registri	5 GB di dati (acquisizione, archiviazione e scansione dei dati mediante query di Logs Insights)	0,50 USD per GB
Amazon CloudWatch - Archiviazione dei log	5 GB di dati (acquisizione, archiviazione e scansione dei dati mediante query di Logs Insights)	0,005 USD per GB di dati scansionati
Amazon CloudWatch - Eventi	Sono inclusi tutti gli eventi tranne gli eventi personalizzati	1,00 USD per milione di eventi per eventi personalizzati 1,00 USD per milione di eventi per eventi tra più account
AWS Lambda - Richieste	1 milione di richieste gratuite al mese	0,20 USD per 1 milione di richieste

Servizio	Piano gratuito	Prezzi [USD]
AWS Lambda - Durata	400.000 GB di tempo di elaborazione al mese	0,0000166667 USD per ogni GB al secondo. Il prezzo di Duration dipende dalla quantità di memoria allocata alla funzione. È possibile allocare qualsiasi quantità di memoria alla funzione tra 128 MB e 10.240 MB, con incrementi di 1 MB.
AWS Step Functions - Transizioni di stato	4.000 transizioni di stato gratuite al mese	0,025 USD per 1.000 transizioni di stato successive
Amazon EventBridge	Tutti gli eventi di modifica dello stato pubblicati dai servizi AWS sono gratuiti	Gli eventi personalizzati costano 1,00 USD per milione di eventi personalizzati pubblicati Gli eventi di terze parti (SaaS) costano 1,00 USD per milione di eventi pubblicati Gli eventi su più account costano 1,00 USD per milione di eventi inviati su più account
Amazon SNS	Le prime 1 milione di richieste Amazon SNS al mese sono gratuite	0,50 USD per 1 milione di richieste successive
Amazon SQS	I primi 1 milione di richieste Amazon SQS al mese sono gratuite	0,40 USD per ogni milione - 100 miliardi di richieste successive

Servizio	Piano gratuito	Prezzi [USD]
Amazon DynamoDB	I primi 25 GB di spazio di archiviazione sono gratuiti	2,00 USD per 1 milione di letture e scritture coerenti successive
Prezzi di AWS Key Management Service	20.000 richieste/mese	1,00 USD per 1 chiave KMS. Per le chiavi KMS che ruotate automaticamente o su richiesta, la prima e la seconda rotazione della chiave aggiungono un costo di 1 dollaro al mese (ripartito proporzionalmente all'ora).

Esempi di prezzi (mensili)

Esempio 1:300 riparazioni al mese

- 10 account, 1 regione
- 30 riparazioni per account/Region/month
- Costo totale 21,17 USD al mese

Servizio	Presupposti	Spese mensili [USD]
AWS Systems Manager Automation	Passaggi: ~4 passaggi* 300 riparazioni* 0,002 USD = 2,40 USD Durata: 10 sec* 300 riparazioni * 0,00003 USD = 0,09 USD	2,49 USD
Centrale di sicurezza AWS	Nessun servizio fatturabile utilizzato	0 USD

Servizio	Presupposti	Spese mensili [USD]
CloudWatch Registri Amazon	300 riparazioni* 0,000002 USD = 0,0006 USD 0,0006 USD* 0,03 = 0,000018 USD	< 0,01 US$
AWS Lambda - Richieste	300 riparazioni* 6 richieste = 1.800 richieste 0,20 USD* 1.000.000 di richieste = 0,20 USD	0,20 US$
AWS Lambda - Durata	256 milioni: 1,875 GB al secondo * 300 riparazioni * 0,0000167 USD = 0,009375 USD	< 0,01 USD
AWS Step Functions	17 transizioni di stato * 300 riparazioni = 5.100 0,025 USD* (5.100/1.000) transizioni di stato = 0,15 USD	$0,15
EventBridge Regole di Amazon	Nessun costo per le regole	0 USD
AWS Key Management Service	1 chiave* 10 account* 1 regione* 1$ = 10$	$10,00
Amazon DynamoDB	2,00 USD* 1.000.000 di letture e scritture = 2,00 USD	$2,00
Amazon SQS	0,40 USD* 1.000.000 di richieste = 0,40 USD	0,40 USD
Amazon SNS	0,50 USD* 1.000.000 di notifiche = 0,50 USD	$0,50

Servizio	Presupposti	Spese mensili [USD]
Amazon CloudWatch - Metriche	0,30 USD* 7 metriche personalizzate = 2,10 USD 0,01 USD* (300 * 3/1.000) chiamate API put Metrics = 0,01 USD	2,11 USD
Amazon CloudWatch - Pannelli di controllo	3,00 USD* 1 dashboard = 3,00 USD	$3,00
Amazon CloudWatch - Allarmi	0,10 USD* 3 allarmi = 0,30 USD	0,30$
Totale		21,17$

Esempio 2:3.000 riparazioni al mese

- 100 account, 1 regione
- 30 riparazioni per account/Region/month
- Costo totale 134,86 USD al mese

Servizio	Presupposti	Spese mensili [USD]
AWS Systems Manager Automation	Fasi: ~4 passaggi* 3.000 riparazioni* 0,002 USD = 24,00 USD Durata: 10 sec* 3.000 riparazioni* 0,00003 USD = 0,90 USD	$24,90
Centrale di sicurezza AWS	Nessun servizio fatturabile utilizzato	0 USD

Servizio	Presupposti	Spese mensili [USD]
CloudWatch Registri Amazon	3.000 riparazioni* 0,000002 USD = 0,006 USD 0,006 USD* 0,03 = 0,00018 USD	< 0,01 US$
AWS Lambda - Richieste	3.000 riparazioni* 6 richieste = 18.000 richieste 0,20 USD* 1.000.000 di richieste = 0,20 USD	0,20 US$
AWS Lambda - Durata	256 milioni: 1,875 GB sec* 3.000 riparazioni* 0,000167 USD = 0,09375 USD	0,09 USD
AWS Step Functions	17 transizioni di stato * 3.000 riparazioni = 51.000 0,025 USD* (51.000/1.000) transizioni di stato = 1,275 USD	$1,28
EventBridge Regole di Amazon	Nessun costo per le regole	0 USD
AWS Key Management Service	1 chiave* 100 account* 1 regione* 1$ = 100$	$100
Amazon DynamoDB	2,00 USD* 1.000.000 di letture e scritture = 2,00 USD	$2,00
Amazon SQS	0,40 USD* 1.000.000 di richieste = 0,40 USD	0,40 USD
Amazon SNS	0,50 USD* 1.000.000 di notifiche = 0,50 USD	$0,50

Servizio	Presupposti	Spese mensili [USD]
Amazon CloudWatch - Metriche	0,30 USD* 7 metriche personalizzate = 2,10 USD 0,01 USD* (3000 * 3/1.000) chiamate API put metrics = 0,09 USD	2,19 USD
Amazon CloudWatch - Pannelli di controllo	3,00 USD* 1 dashboard = 3,00 USD	$3,00
Amazon CloudWatch - Allarmi	0,10 USD* 3 allarmi = 0,30 USD	0,30$
Totale		$134,86

Esempio 3:30.000 riparazioni al mese

- 1.000 account, 10 regioni
- 30 riparazioni per account/Region/month
- Costo totale 1.271,70 USD al mese

Servizio	Presupposti	Spese mensili [USD]
AWS Systems Manager Automation	Fasi: ~4 passaggi* 30.000 riparazioni* 0,002 USD = 240,00 USD Durata: 10 sec* 30.000 riparazioni* 0,00003 USD = 9,00 USD	249,00$
Centrale di sicurezza AWS	Nessun servizio fatturabile utilizzato	0 USD

Servizio	Presupposti	Spese mensili [USD]
CloudWatch Registri Amazon	30.000 riparazioni* 0,000002 USD = 0,06 USD 0,06 USD* 0,03 = 0,0018 USD	< 0,01 US$
AWS Lambda - Richieste	30.000 riparazioni* 6 richieste = 180.000 richieste 0,20 USD* 1.000.000 di richieste = 0,20 USD	0,20 US$
AWS Lambda - Durata	256 milioni: 1,875 GB sec* 30.000 riparazioni* 0,000167 USD = 0,9375 USD	0,94 USD
AWS Step Functions	17 transizioni di stato* 30.000 riparazioni = 510.000 0,025 USD* (510.000/1.000) transizioni di stato = 12,75 USD	$12,75
EventBridge Regole di Amazon	Nessun costo per le regole	0 USD
AWS Key Management Service	(1 chiave) 1 USD* 1.000 account * 10 regioni = 10.000 USD	10.000$
Amazon DynamoDB	0,000002 USD* 1.000.000 di letture e scritture = 2,00 USD	$2,00
Amazon SQS	0,000004 USD* 1.000.000 di richieste = 0,40 USD	0,40 US$
Amazon SNS	0,000005 USD * 1.000.000 di notifiche = 0,50 USD	0,50 USD

Servizio	Presupposti	Spese mensili [USD]
Amazon CloudWatch - Metriche	0,30 USD* 6 metriche personalizzate = 1,80 USD 0,01 USD* (30.000 * 3/1.000) chiamate API put metrics = 0,90 USD	2,70$
Amazon CloudWatch - Pannelli di controllo	3,00 USD* 1 dashboard = 3,00 USD	$3,00
Amazon CloudWatch - Allarmi	0,10 USD* 2 allarmi = 0,20 USD	0,20$
Totale		$10.271,70

> **Important**
>
> Costi di rotazione delle chiavi KMS AWS Key Management Service (KMS) ruota automaticamente le chiavi gestite dal cliente una volta all'anno quando la rotazione è abilitata. Ogni rotazione comporta un costo di 1,00 USD per chiave all'anno. Ad esempio, con 1000 account in una singola regione, ciò comporta un costo aggiuntivo di 1000 USD all'anno (1 rotazione × 1000 chiavi × 1,00 USD).

Costo aggiuntivo per funzionalità opzionali

Questa sezione identifica i costi aggiuntivi associati alle funzionalità opzionali di questa soluzione.

Metriche avanzate CloudWatch

Se si seleziona `yes` il EnableEnhancedCloudWatchMetricsparametro durante la distribuzione dello stack di amministrazione, la soluzione crea due metriche personalizzate e un allarme per ogni ID di controllo. Il costo dipende dal numero di controlli da IDs correggere. Nella tabella seguente, si presume che si stiano ripristinando tutti i 96 diversi controlli IDs al mese, per determinare il limite massimo dei costi.

Servizio	Ipotesi 96 IDs controllo* 2 = 192 metriche personalizzate	Spese mensili [USD]
Amazon CloudWatch - Metriche	0,30 USD* 192 metriche personalizzate = 57,60 USD	57,60$
Amazon CloudWatch - Allarmi	0,10 USD* 96 allarmi = 9,60 USD	9,60$
Totale		$67,20

CloudTrail Registro delle azioni

In ogni account membro per cui abiliti la funzionalità Action Log, le soluzioni creano una CloudTrail traccia per registrare tutti gli eventi di gestione delle scritture. Una funzione Lambda filtra gli eventi non correlati alla soluzione. Ciò significa che il costo è correlato al numero totale di eventi di gestione nell'account, poiché gli eventi non correlati alla soluzione vengono comunque acquisiti dal trail ed elaborati dalla funzione Lambda.

Per la tabella seguente, ipotizziamo 150.000 eventi di gestione al mese nell'account. Il costo effettivo dipende dall'effettiva attività degli eventi di gestione nell'account.

Servizio	Presupposti	Spese mensili [USD]
AWS CloudTrail	150.000 USD* 2,00/100.000 USD = 3,00 USD	$3,00
Lambda	150.000 * 0,2 * 0,125 = 3.750 GB/secondi 3.750 USD* 0,0000166667 = 0,0625 USD di costo del tempo di elaborazione 0,15 USD* 0,20 USD = 0,03 USD per il costo della richiesta	0,0925 USD

Servizio	Presupposti	Spese mensili [USD]
	0,0625 USD + 0,03 USD = 0,0952 USD di costo totale Lambda	
Totale		3,09$ per account membro

Sicurezza

Quando crei sistemi sull'infrastruttura AWS, le responsabilità di sicurezza vengono condivise tra te e AWS. Questo modello condiviso riduce il carico operativo perché AWS gestisce, gestisce e controlla i componenti, tra cui il sistema operativo host, il livello di virtualizzazione e la sicurezza fisica delle strutture in cui operano i servizi. Per ulteriori informazioni sulla sicurezza di AWS, visita la pagina AWS Cloud Security.

Ruoli IAM

I ruoli di AWS Identity and Access Management (IAM) consentono ai clienti di assegnare policy e autorizzazioni di accesso granulari a servizi e utenti nel cloud AWS. Questa soluzione crea ruoli IAM che garantiscono alle funzioni automatizzate della soluzione l'accesso per eseguire azioni di riparazione entro un ambito ristretto di autorizzazioni specifiche per ciascuna riparazione.

La Step Function dell'account di amministrazione è assegnata al ruolo SO0111-. ASR-Orchestrator-Admin Solo questo ruolo può assumere il membro SO0111-Orchestrator in ogni account membro. Il ruolo membro è autorizzato da ciascun ruolo di riparazione a trasferirlo al servizio AWS Systems Manager per eseguire runbook di riparazione specifici. I nomi dei ruoli di riparazione iniziano con SO0111, seguiti da una descrizione che corrisponde al nome del runbook di riparazione. Ad esempio, SO0111-Remove è il ruolo del runbook di correzione ASR-Remove VPCDefaultSecurityGroupRules . VPCDefault SecurityGroupRules

Regioni AWS supportate

Nome della Regione	Codice regione
Stati Uniti orientali (Ohio)	us-east-2

Nome della Regione	Codice regione
US East (N. Virginia)	us-east-1
Stati Uniti occidentali (California settentrionale)	us-west-1
US West (Oregon)	us-west-2
Africa (Cape Town)	af-south-1
Asia Pacifico (Hong Kong)	ap-east-1
Asia Pacific (Hyderabad)	ap-south-2
Asia Pacifico (Giacarta)	ap-southeast-3
Asia Pacifico (Melbourne)	ap-southeast-4
Asia Pacific (Mumbai)	ap-south-1
Asia Pacifico (Osaka-Locale)	ap-northeast-3
Asia Pacifico (Seoul)	ap-northeast-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Canada (Central)	ca-central-1
Europa (Francoforte)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europa (Milano)	eu-south-1
Europe (Paris)	eu-west-3

Nome della Regione	Codice regione
Europa (Spagna)	eu-south-2
Europa (Stoccolma)	eu-north-1
Europa (Zurigo)	eu-central-2
Medio Oriente (Bahrein)	me-south-1
Medio Oriente (Emirati Arabi Uniti)	me-central-1
Sud America (San Paolo)	sa-east-1
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1
China (Beijing)	cn-north-1
China (Ningxia)	cn-northwest-1
Israele (Tel Aviv)	il-central-1
Canada occidentale (Calgary)	ca-west-1
Messico (Città del Messico)	mx-central-1
Asia Pacifico (Tailandia)	ap-southeast-7

> **Note**
>
> Tutte le nuove regioni AWS non elencate possono essere supportate tramite distribuzione locale ma non tramite distribuzione con un clic.

Quote

Le quote di servizio, anche denominate limiti, rappresentano il numero massimo di risorse di servizio o operazioni per l'account AWS.

Quote per i servizi AWS in questa soluzione

Assicurati di disporre di una quota sufficiente per ciascuno dei servizi implementati in questa soluzione. Per ulteriori informazioni, consulta le quote dei servizi AWS.

Utilizza i seguenti link per accedere alla pagina relativa al servizio. Per visualizzare le Service Quotas per tutti i servizi AWS nella documentazione senza cambiare pagina, visualizza invece le informazioni nella pagina Service endpoints and quotas nel PDF.

CloudFormation Quote AWS

Il tuo account AWS ha CloudFormation quote AWS di cui dovresti essere a conoscenza quando avvii lo stack di questa soluzione. Comprendendo queste quote, puoi evitare errori di limitazione che potrebbero impedirti di implementare questa soluzione con successo. Per ulteriori informazioni, consulta le CloudFormation quote AWS nella AWS CloudFormation User Guide.

CloudWatch Quote AWS

Il tuo account AWS ha CloudWatch quote AWS legate alle CloudWatch Resource Policies, che consentono solo 10 policy di risorse per regione per account e questo non può essere richiesto per un aumento della quota, consulta AWS CloudWatch Logs Quotas nella CloudWatch AWS User Guide. Prima della distribuzione, controlla l'utilizzo attuale per assicurarti di non superare questa soglia durante la distribuzione della soluzione.

Amazon EventBridge regola le quote

Il tuo account AWS prevede EventBridge delle quote di regole Amazon di cui dovresti essere a conoscenza quando selezioni i playbook da distribuire con la soluzione. Ogni playbook creerà una EventBridge regola per ogni controllo a cui può porre rimedio. Quando si distribuiscono più playbook, è possibile raggiungere la quota di regole. Per ulteriori informazioni, consulta le EventBridge quote Amazon nella Amazon EventBridge User Guide.

Implementazione di AWS Security Hub

La distribuzione e la configurazione di AWS Security Hub sono un prerequisito per questa soluzione. Per ulteriori informazioni sulla configurazione di AWS Security Hub, consulta la sezione Configurazione di AWS Security Hub nella AWS Security Hub User Guide.

Come minimo, devi avere un Security Hub funzionante configurato nel tuo account principale. Puoi distribuire questa soluzione nello stesso account (e nella stessa regione AWS) dell'account primario di Security Hub. In ogni account primario e secondario di Security Hub, devi anche distribuire il modello membro che consente AssumeRole le autorizzazioni ad AWS Step Functions della soluzione per eseguire i runbook di correzione nell'account.

Stack e distribuzione StackSets

Un set di stack consente di creare stack negli account AWS in tutte le regioni AWS utilizzando un singolo modello CloudFormation AWS. A partire dalla versione 1.4, questa soluzione supporta la distribuzione di stack set suddividendo le risorse in base a dove e come vengono distribuite. I clienti con più account, in particolare quelli che utilizzano AWS Organizations, possono trarre vantaggio dall'utilizzo di set di stack per la distribuzione su più account. Riduce lo sforzo necessario per installare e mantenere la soluzione. Per ulteriori informazioni StackSets, consulta Using AWS CloudFormation StackSets.

Implementa la soluzione

> **Important**
>
> Se la funzionalità dei risultati del controllo consolidato è attivata in Security Hub (impostazione predefinita nelle nuove distribuzioni), abilita il playbook Security Control (CS) solo quando distribuisci questa soluzione. Se la funzione non è attivata, abilita solo i playbook per gli standard di sicurezza abilitati in Security Hub. L'attivazione di playbook aggiuntivi può comportare il raggiungimento della quota per EventBridge le regole.

Questa soluzione utilizza CloudFormation modelli e stack AWS per automatizzarne l'implementazione. I CloudFormation modelli specificano le risorse AWS incluse in questa soluzione e le relative proprietà. Lo CloudFormation stack fornisce le risorse descritte nei modelli.

Affinché la soluzione funzioni, è necessario implementare tre modelli. Innanzitutto, decidi dove distribuire i modelli, quindi decidi come distribuirli.

Questa panoramica descriverà i modelli e come decidere dove e come distribuirli. Le sezioni successive conterranno istruzioni più dettagliate per distribuire ogni stack come stack o. StackSet

Decidere dove distribuire ogni stack

I tre modelli verranno denominati con i seguenti nomi e conterranno le seguenti risorse:

- Admin stack: funzione Orchestrator Step, regole degli eventi e azione personalizzata del Security Hub.
- Member stack: documenti di correzione SSM Automation.
- Stack di ruoli dei membri: ruoli IAM per le riparazioni.

Lo stack di amministrazione deve essere distribuito una sola volta, in un unico account e in un'unica regione. Deve essere distribuito nell'account e nella regione che hai configurato come destinazione di aggregazione per i risultati del Security Hub per la tua organizzazione. Se desideri utilizzare la funzionalità Action Log per monitorare gli eventi di gestione, devi distribuire lo stack di amministrazione nell'account di gestione dell'organizzazione o in un account amministratore delegato.

La soluzione funziona sui risultati di Security Hub, quindi non sarà in grado di operare sui risultati di un account e di una regione particolari se tale account o regione non è stato configurato per aggregare i risultati nell'account amministratore e nella regione di Security Hub.

Ad esempio, un'organizzazione ha account che operano nelle regioni `us-east-1` e`us-west-2`, con account `111111111111` come amministratore delegato del Security Hub, nella regione`us-east-1`. Account `222222222222` e `333333333333` devono essere account membri del Security Hub per l'account `111111111111` amministratore delegato. Tutti e tre gli account devono essere configurati per aggregare i risultati dal `us-west-2` al. `us-east-1` Lo stack di amministrazione deve essere distribuito sull'account in. `111111111111` `us-east-1`

Per maggiori dettagli sulla ricerca dell'aggregazione, consulta la documentazione per gli account amministratore delegato di Security Hub e l'aggregazione tra regioni.

Lo stack di amministrazione deve completare la distribuzione prima di distribuire gli stack dei membri in modo da poter creare una relazione di fiducia tra gli account dei membri e l'account hub.

Lo stack di membri deve essere distribuito in ogni account e regione in cui desideri correggere i risultati. Questo può includere l'account amministratore delegato di Security Hub in cui è stato precedentemente distribuito lo stack di amministrazione ASR. I documenti di automazione devono essere eseguiti negli account dei membri per poter utilizzare il livello gratuito per l'automazione SSM.

Utilizzando l'esempio precedente, se si desidera correggere i risultati di tutti gli account e le regioni, lo stack di membri deve essere distribuito su tutti e tre gli account (`111111111111`, `222222222222` e) e su entrambe le regioni (e). `333333333333` `us-east-1` `us-west-2`

Lo stack di ruoli dei membri deve essere distribuito su ogni account, ma contiene risorse globali (ruoli IAM) che possono essere distribuite solo una volta per account. Non importa in quale regione distribuisci lo stack di ruoli dei membri, quindi per semplicità ti consigliamo di distribuirlo nella stessa regione in cui viene distribuito lo stack di amministrazione.

Utilizzando l'esempio precedente, suggeriamo di distribuire lo stack di ruoli dei membri su tutti e tre gli account (, e) in. `111111111111` `222222222222` `333333333333` `us-east-1`

Decidere come distribuire ogni stack

Le opzioni per la distribuzione di uno stack sono

- CloudFormation StackSet (autorizzazioni autogestite)

- CloudFormation StackSet (autorizzazioni gestite dal servizio)
- CloudFormation Pila

StackSets con autorizzazioni gestite dal servizio sono le più comode perché non richiedono l'implementazione di ruoli propri e possono essere implementate automaticamente su nuovi account dell'organizzazione. Sfortunatamente, questo metodo non supporta gli stack annidati, che utilizziamo sia nello stack di amministrazione che nello stack dei membri. L'unico stack che può essere distribuito in questo modo è lo stack dei ruoli dei membri.

Tieni presente che durante la distribuzione all'intera organizzazione, l'account di gestione dell'organizzazione non è incluso, quindi se desideri correggere i risultati nell'account di gestione dell'organizzazione, devi distribuirlo su questo account separatamente.

Lo stack di membri deve essere distribuito su ogni account e regione, ma non può essere distribuito utilizzando autorizzazioni gestite dal servizio perché contiene stack StackSets annidati. Pertanto, suggeriamo di distribuire questo stack con autorizzazioni gestite automaticamente. StackSets

Lo stack di amministrazione viene distribuito una sola volta, quindi può essere distribuito come CloudFormation stack semplice o come uno StackSet con autorizzazioni autogestite in un unico account e regione.

Risultati di controllo consolidati

Gli account dell'organizzazione possono essere configurati con la funzionalità di controllo consolidato dei risultati del controllo di Security Hub attivata o disattivata. Consulta i risultati del controllo consolidato nella Guida per l'utente di AWS Security Hub.

> **Important**
>
> Se abilitata, devi usare la versione 2.0.0 della soluzione o successiva. Inoltre, è necessario distribuire gli stack annidati Admin e Member per gli standard «SC» o «security control». In questo modo vengono implementati i documenti e EventBridge le regole di automazione da utilizzare con il controllo consolidato IDs generato quando questa funzionalità è attivata. Non è necessario distribuire gli stack annidati Admin o Member per standard specifici (ad esempio AWS FSBP) quando si utilizza questa funzionalità.

CloudFormation Modelli AWS

View template

automa

security-response-admin.template: utilizza questo modello per avviare la soluzione Automated Security Response on AWS. Il modello installa i componenti principali della soluzione, uno stack annidato per i log di AWS Step Functions e uno stack nidificato per ogni standard di sicurezza che scegli di attivare.

I servizi utilizzati includono Amazon Simple Notification Service, AWS Key Management Service, AWS Identity and Access Management, AWS Lambda, AWS Step Functions, Amazon CloudWatch Logs, Amazon S3 e AWS Systems Manager.

Supporto per account amministrativi

I seguenti modelli vengono installati nell'account amministratore di AWS Security Hub per attivare gli standard di sicurezza che desideri supportare. Puoi scegliere quale dei seguenti modelli installare durante l'installazione di`automated-security-response-admin.template`.

automated-security-response-orchestrator-log.template - Crea un gruppo di CloudWatch log per la funzione Orchestrator Step.

AFSBPStack.template - Regole AWS Foundational Security Best Practices v1.0.0.

CIS120Stack.template - Benchmark CIS Amazon Web Services Foundations, regole v1.2.0.

CIS140Stack.template - Benchmark CIS Amazon Web Services Foundations, regole v1.4.0.

CIS300Stack.template - Benchmark CIS Amazon Web Services Foundations, regole v3.0.0.

PCI321Stack.template - Regole PCI-DSS v3.2.1.

NISTStack.template - Regole del National Institute of Standards and Technology (NIST), v5.0.0.

SCStack.template - Regole Security Controls v2.0.0.

Ruoli dei membri

View template

automa

security-response-member-roles.template: definisce i ruoli di riparazione necessari in ogni account membro di AWS Security Hub.

Account membri

View template

automa

security-response-member.template: utilizza questo modello dopo aver configurato la soluzione principale per installare i runbook di automazione e le autorizzazioni di AWS Systems Manager in ciascuno degli account membro di AWS Security Hub (incluso l'account amministratore). Questo modello ti consente di scegliere quali playbook standard di sicurezza installare.

`automated-security-response-member.template`Installa i seguenti modelli in base alle tue selezioni:

automated-security-response-remediation-runbooks.template - Codice di correzione comune utilizzato da uno o più standard di sicurezza.

AFSBPMemberStack.template - Impostazioni, autorizzazioni e runbook di correzione di AWS Foundational Security Best Practices v1.0.0.

CIS120 MemberStack .template - Benchmark CIS di Amazon Web Services Foundations, impostazioni, autorizzazioni e runbook di correzione della versione 1.2.0.

CIS140 MemberStack .template - Benchmark CIS di Amazon Web Services Foundations, impostazioni, autorizzazioni e runbook di correzione della versione 1.4.0.

CIS300 MemberStack .template - Benchmark CIS di Amazon Web Services Foundations, impostazioni, autorizzazioni e runbook di correzione della versione 3.0.0.

PCI321MemberStack.template - Impostazioni, autorizzazioni e runbook di correzione PCI-DSS v3.2.1.

NISTMemberStack.template - Impostazioni, autorizzazioni e runbook di correzione del National Institute of Standards and Technology (NIST), v5.0.0.

SCMemberStack.template - Impostazioni, autorizzazioni e runbook di correzione del controllo di sicurezza.

automated-security-response-member-cloudtrail.template: utilizzato nella funzione Action Log per tracciare e controllare l'attività di assistenza.

Integrazione del sistema di ticket

Utilizza uno dei seguenti modelli per l'integrazione con il tuo sistema di biglietteria.

View template

JiraBlu

esegui l'implementazione se usi Jira come sistema di ticketing.

View template

Service

implementalo se lo utilizzi come sistema di ticketing. ServiceNow

Se desideri integrare un sistema di ticketing esterno diverso, puoi utilizzare uno di questi stack come modello per capire come implementare la tua integrazione personalizzata.

Implementazione automatizzata - StackSets

> **Note**
>
> Ti consigliamo di eseguire la distribuzione con. StackSets Tuttavia, per le implementazioni con account singolo o per scopi di test o valutazione, prendi in considerazione l'opzione di distribuzione in stack.

Prima di avviare la soluzione, esaminate l'architettura, i componenti della soluzione, la sicurezza e le considerazioni sulla progettazione discusse in questa guida. Segui le step-by-step istruzioni in questa sezione per configurare e distribuire la soluzione nelle tue AWS Organizations.

Tempo di implementazione: circa 30 minuti per account, a seconda StackSet dei parametri.

Prerequisiti

AWS Organizations ti aiuta a gestire e governare centralmente l'ambiente e le risorse AWS multi-account. StackSets funzionano al meglio con AWS Organizations.

Se hai già distribuito la versione 1.3.x o una versione precedente di questa soluzione, devi disinstallare la soluzione esistente. Per ulteriori informazioni, consulta Aggiornare la soluzione.

Prima di distribuire questa soluzione, esamina la distribuzione di AWS Security Hub:

- Nella tua AWS Organization deve essere presente un account amministratore delegato di Security Hub.
- Security Hub deve essere configurato per aggregare i risultati tra le regioni. Per ulteriori informazioni, consulta la sezione Aggregazione dei risultati tra le regioni nella AWS Security Hub User Guide.
- Devi attivare Security Hub per la tua organizzazione in ogni regione in cui utilizzi AWS.

Questa procedura presuppone che tu disponga di più account che utilizzano AWS Organizations e che tu abbia delegato un account amministratore AWS Organizations e un account amministratore AWS Security Hub.

Panoramica della distribuzione

> **Note**
>
> StackSets l'implementazione di questa soluzione utilizza una combinazione di gestione dei servizi e gestione automatica. StackSets La modalità Self-Managed StackSets deve essere utilizzata attualmente in quanto utilizza sistemi annidati StackSets, che non sono ancora supportati con Service-Managed. StackSets

Distribuiscili StackSets da un account amministratore delegato nel tuo AWS Organizations.

Pianificazione

Utilizza il seguente modulo per aiutarti con StackSets la distribuzione. Prepara i dati, quindi copia e incolla i valori durante la distribuzione.

```
AWS Organizations admin account ID: ______________
Security Hub admin account ID: ______________
CloudTrail Logs Group: ______________________________
Member account IDs (comma-separated list):
____________________,
____________________,
```

```
____________________,
____________________,
____________________
AWS Organizations OUs (comma-separated list):
____________________,
____________________,
____________________,
____________________,
____________________
```

(Facoltativo) Fase 0: Implementazione dello stack di integrazione dei ticket

- Se intendi utilizzare la funzione di ticketing, implementa prima lo stack di integrazione dei ticket nel tuo account amministratore di Security Hub.
- Copia il nome della funzione Lambda da questo stack e forniscilo come input allo stack di amministrazione (vedi Passaggio 1).

Passaggio 1: avviare lo stack di amministrazione nell'account amministratore delegato di Security Hub

- Utilizzando un modello autogestito StackSet, avvia il CloudFormation modello `automated-security-response-admin.template` AWS nel tuo account amministratore AWS Security Hub nella stessa regione dell'amministratore di Security Hub. Questo modello utilizza pile annidate.
- Scegli quali standard di sicurezza installare. Per impostazione predefinita, è selezionato solo SC (consigliato).
- Scegliete un gruppo di log di Orchestrator esistente da utilizzare. Seleziona `Yes` se esiste `SO0111-ASR- Orchestrator` già da un'installazione precedente.

Per ulteriori informazioni sulla gestione automatica StackSets, consulta Grant self-managed permissions nella CloudFormation AWS User Guide.

Fase 2: installa i ruoli di riparazione in ogni account membro di AWS Security Hub

Attendi il passaggio 1 per completare la distribuzione, poiché il modello nella fase 2 fa riferimento ai ruoli IAM creati dalla fase 1.

- Utilizzando un servizio gestito StackSet, avvia il CloudFormation modello `automated-security-response-member-roles.template` AWS in una singola regione in ogni account delle tue AWS Organizations.

- Scegli di installare questo modello automaticamente quando un nuovo account si unisce all'organizzazione.
- Inserisci l'ID dell'account amministratore di AWS Security Hub.

Fase 3: Avvia lo stack di membri in ogni account membro e regione di AWS Security Hub

- Utilizzando la gestione automatica StackSets, avvia il CloudFormation modello `automated-security-response-member.template` AWS in tutte le regioni in cui hai risorse AWS in ogni account della tua AWS Organization gestite dallo stesso amministratore di Security Hub.

> **Note**
>
> Fino a quando il StackSets supporto gestito dal servizio non sarà annidato, devi eseguire questo passaggio per tutti i nuovi account che entrano a far parte dell'organizzazione.

- Scegliete quali playbook Security Standard installare.
- Fornisci il nome di un gruppo di CloudTrail log (utilizzato per alcune soluzioni correttive).
- Inserisci l'ID dell'account amministratore di AWS Security Hub.

(Facoltativo) Fase 0: Avvia uno stack di integrazione del sistema di ticket

1. Se intendi utilizzare la funzione di ticketing, avvia prima il rispettivo stack di integrazione.
2. Scegli gli stack di integrazione forniti per Jira oppure ServiceNow usali come modello per implementare la tua integrazione personalizzata.

   Per distribuire lo stack Jira:

   a. Inserisci un nome per lo stack.

   b. Fornisci l'URI alla tua istanza Jira.

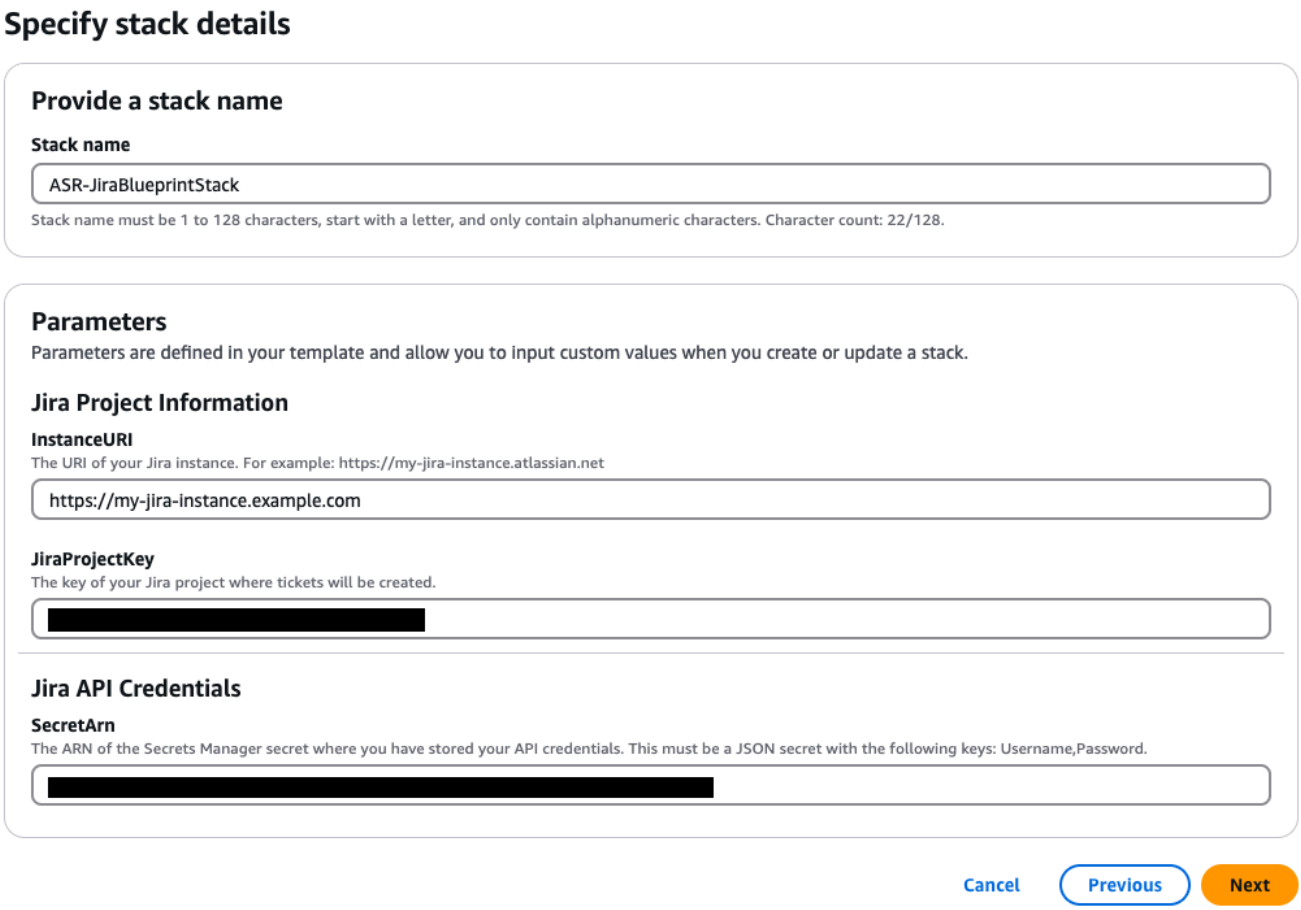
   c. Fornisci la chiave del progetto Jira a cui desideri inviare i ticket.

   d. Crea un nuovo segreto chiave-valore in Secrets Manager che contenga `Username` Jira e. `Password`

> **Note**
>
> Puoi scegliere di utilizzare una chiave API Jira al posto della password fornendo il tuo nome utente come `Username` e la tua chiave API come. `Password`

e. Aggiungi l'ARN di questo segreto come input allo stack.

   Fornisci il nome dello stack, le informazioni sul progetto Jira e le credenziali dell'API Jira.



   Per distribuire lo stack: ServiceNow

f. Inserisci un nome per lo stack.

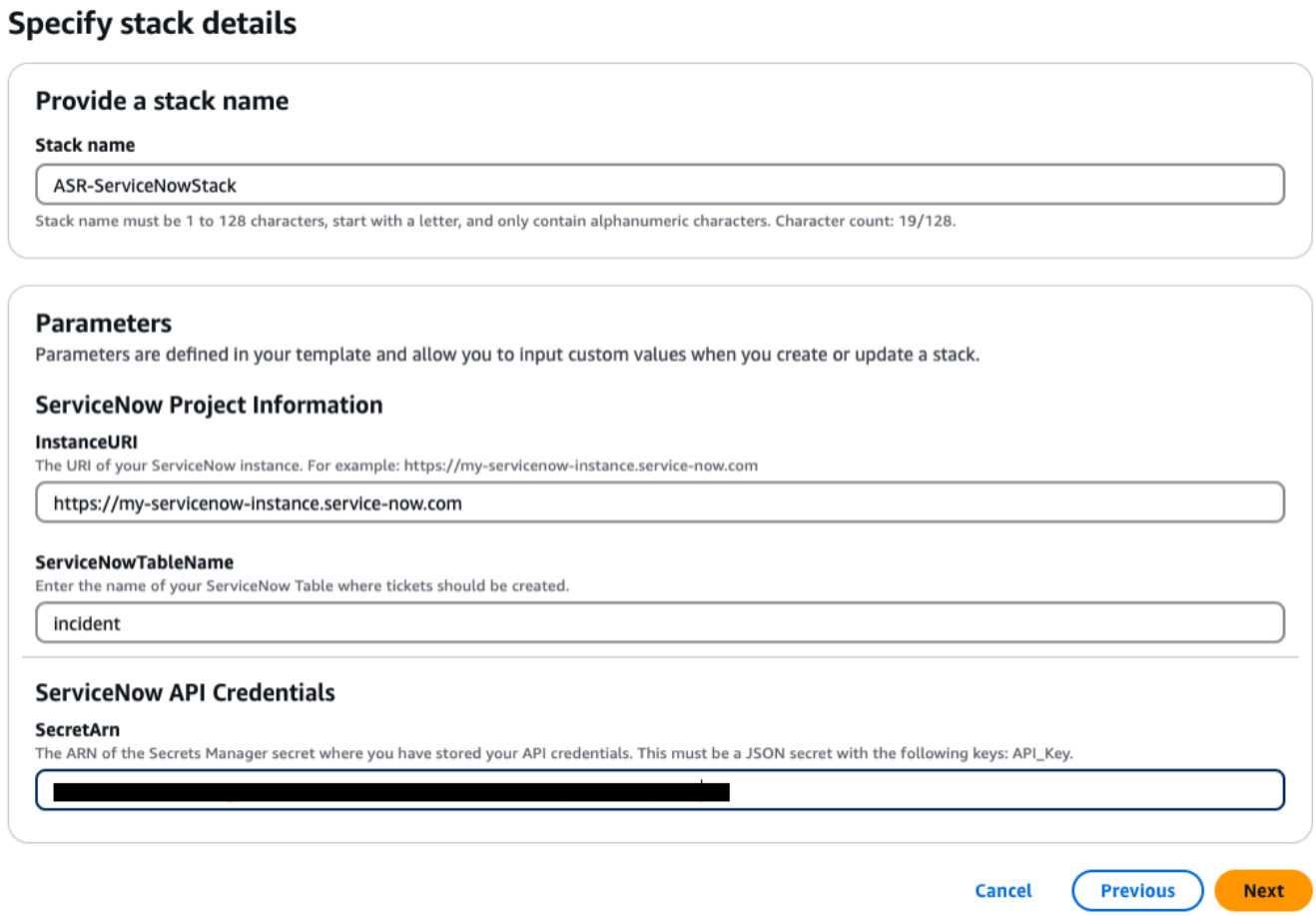
g. Fornisci l'URI della tua ServiceNow istanza.

h. Fornisci il nome della ServiceNow tabella.

i. Crea una chiave API ServiceNow con l'autorizzazione a modificare la tabella su cui intendi scrivere.

j. Crea un segreto in Secrets Manager con la chiave `API_Key` e fornisci l'ARN segreto come input per lo stack.

   Fornisci un nome di stack, informazioni sul ServiceNow progetto e ServiceNow credenziali API.



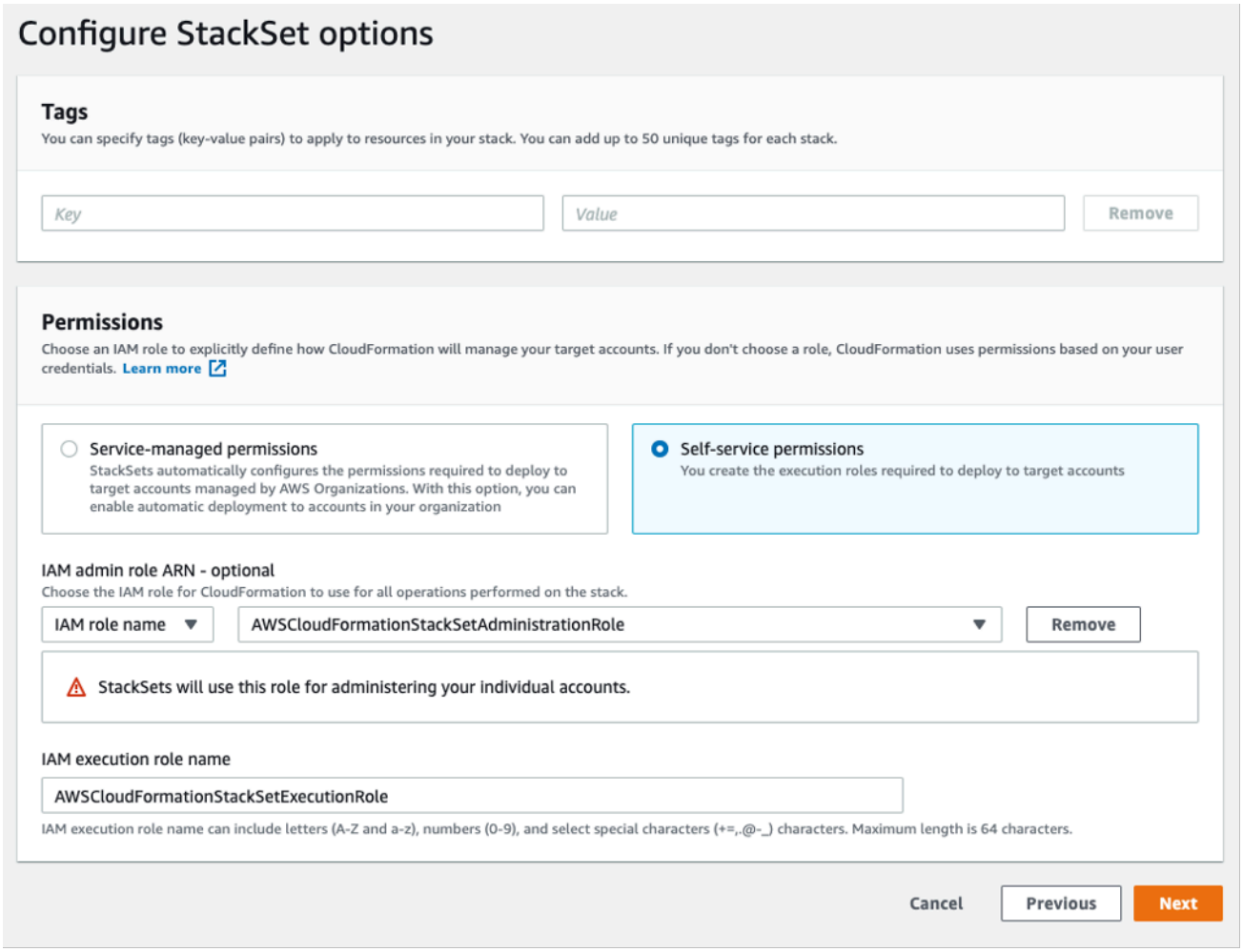
   Per creare uno stack di integrazione personalizzato: includi una funzione Lambda che l'orchestratore di soluzioni Step Functions può chiamare per ogni correzione. La funzione Lambda dovrebbe prendere l'input fornito da Step Functions, costruire un payload in base ai requisiti del sistema di ticketing ed effettuare una richiesta al sistema per creare il ticket.

Passaggio 1: avviare lo stack di amministrazione nell'account amministratore delegato di Security Hub

1. Avvia lo stack di amministrazione con `automated-security-response-admin.template` il tuo account amministratore di Security Hub. In genere, uno per organizzazione in una singola

regione. Poiché questo stack utilizza stack annidati, è necessario distribuire questo modello come sistema autogestito. StackSet

Configura le opzioni StackSet



2. Per il parametro Account numbers, inserisci l'ID account dell'account amministratore di AWS Security Hub.
3. Per il parametro Specificare le regioni, selezionare solo la regione in cui è attivato l'amministratore di Security Hub. Attendi il completamento di questo passaggio prima di passare al Passaggio 2.

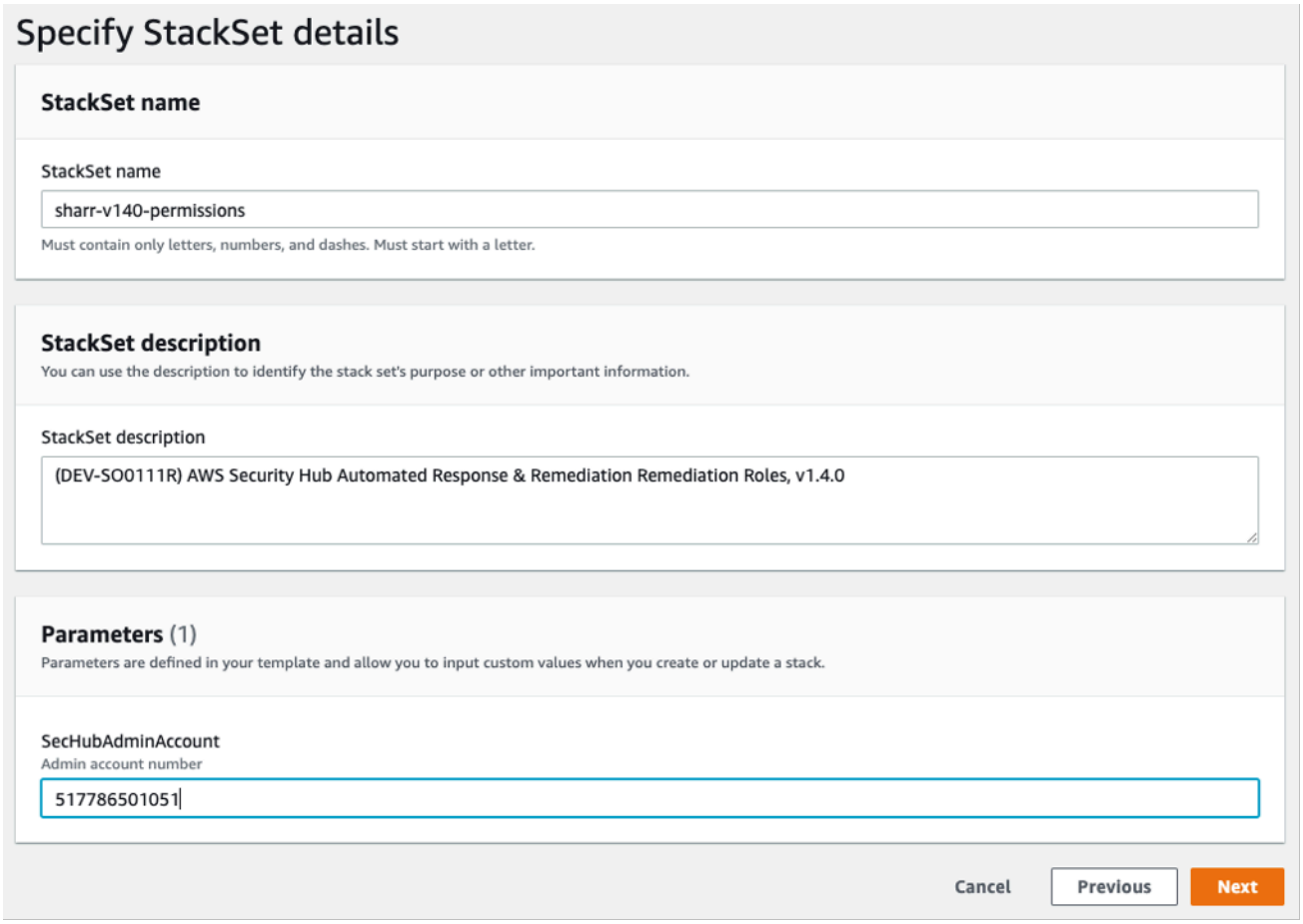
Fase 2: installa i ruoli di riparazione in ogni account membro di AWS Security Hub

Utilizza un servizio gestito StackSets per distribuire il modello dei ruoli dei membri,. `automated-security-response-member-roles.template` Questo StackSet deve essere distribuito in una

regione per account membro. Definisce i ruoli globali che consentono le chiamate API tra account dalla funzione step di ASR Orchestrator.

1. Effettua la distribuzione all'intera organizzazione (tipica) o alle unità organizzative, in base alle politiche dell'organizzazione.
2. Attiva la distribuzione automatica in modo che i nuovi account in AWS Organizations ricevano queste autorizzazioni.
3. Per il parametro Specificare le regioni, seleziona una singola regione. I ruoli IAM sono globali. Puoi continuare con la Fase 3 durante la StackSet distribuzione.

   Specificare i dettagli StackSet



Fase 3: Avvia lo stack di membri in ogni account membro e regione di AWS Security Hub

Poiché lo stack di membri utilizza stack annidati, devi distribuirlo come sistema autogestito. StackSet Ciò non supporta la distribuzione automatica su nuovi account nell'AWS Organization.

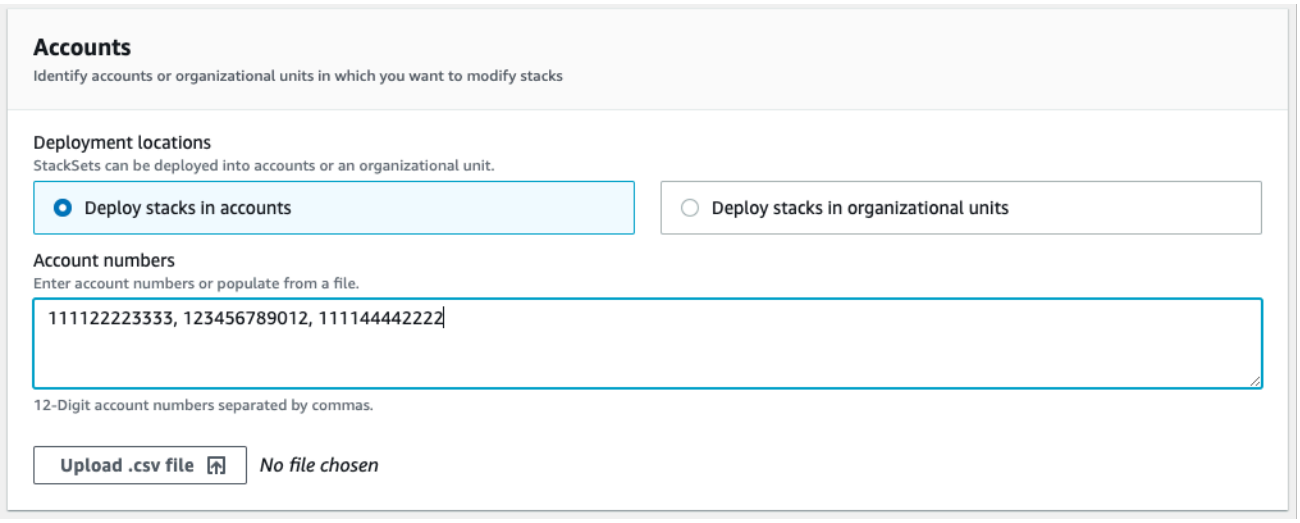
Parametri

LogGroup Configurazione: scegli il gruppo di log che riceve CloudTrail i log. Se non ne esiste nessuno o se il gruppo di log è diverso per ogni account, scegli un valore conveniente. Gli amministratori degli account devono aggiornare il parametro Systems Manager - Parameter Store/Solutions/SO0111/Metrics_ LogGroupName dopo aver creato un gruppo di CloudWatch log per CloudTrail i registri. Questo è necessario per le riparazioni che creano allarmi metrici sulle chiamate API.

Standard: scegli gli standard da caricare nell'account del membro. Questo installa solo i runbook di AWS Systems Manager e non abilita il Security Standard.

SecHubAdminAccount: Inserisci l'ID dell'account AWS Security Hub Admin in cui hai installato il modello di amministrazione della soluzione.

Account



Luoghi di distribuzione: puoi specificare un elenco di numeri di account o unità organizzative.

Specificare le regioni: seleziona tutte le regioni in cui desideri correggere i risultati. È possibile modificare le opzioni di distribuzione in base al numero di account e regioni. La concorrenza regionale può essere parallela.

Distribuzione automatizzata - Stacks

> **Note**
>
> Per i clienti con più account, consigliamo vivamente di implementare con. StackSets

Prima di lanciare la soluzione, esamina l'architettura, i componenti della soluzione, la sicurezza e le considerazioni sulla progettazione discusse in questa guida. Segui le step-by-step istruzioni in questa sezione per configurare e distribuire la soluzione nel tuo account.

Tempo di implementazione: circa 30 minuti

Prerequisiti

Prima di distribuire questa soluzione, assicurati che AWS Security Hub si trovi nella stessa regione AWS degli account primari e secondari. Se hai già distribuito questa soluzione, devi disinstallare la soluzione esistente. Per ulteriori informazioni, consulta Aggiornare la soluzione.

Panoramica della distribuzione

Utilizza i seguenti passaggi per distribuire questa soluzione su AWS.

(Facoltativo) Fase 0: Avvio di uno stack di integrazione del sistema di ticket

- Se intendi utilizzare la funzione di ticketing, implementa prima lo stack di integrazione dei ticket nel tuo account amministratore di Security Hub.
- Copia il nome della funzione Lambda da questo stack e forniscilo come input allo stack di amministrazione (vedi Passaggio 1).

Passaggio 1: avvia lo stack di amministrazione

- Avvia il CloudFormation modello `automated-security-response-admin.template` AWS nel tuo account amministratore di AWS Security Hub.
- Scegli quali standard di sicurezza installare.
- Scegli un gruppo di log di Orchestrator esistente da utilizzare (seleziona `Yes` se esiste `SO0111-ASR-Orchestrator` già da un'installazione precedente).

Fase 2: installa i ruoli di riparazione in ogni account membro di AWS Security Hub

- Avvia il CloudFormation modello `automated-security-response-member-roles.template` AWS in una regione per account membro.
- Inserisci l'account IG a 12 cifre per l'account amministratore di AWS Security Hub.

Fase 3: Avvia lo stack di membri

- Specificate il nome del gruppo CloudWatch Logs da utilizzare con le riparazioni CIS 3.1-3.14. Deve essere il nome di un gruppo di log Logs che riceve CloudWatch i log. CloudTrail
- Scegli se installare i ruoli di riparazione. Installa questi ruoli solo una volta per account.
- Seleziona i playbook da installare.
- Inserisci l'ID dell'account amministratore di AWS Security Hub.

Fase 4: (Facoltativo) Modifica le correzioni disponibili

- Rimuovi eventuali rimedi in base all'account di ciascun membro. Questa fase è facoltativa.

(Facoltativo) Fase 0: Avvio di uno stack di integrazione del sistema di ticket

1. Se intendi utilizzare la funzione di ticketing, avvia prima il rispettivo stack di integrazione.
2. Scegli gli stack di integrazione forniti per Jira oppure ServiceNow usali come modello per implementare la tua integrazione personalizzata.

   Per distribuire lo stack Jira:

   a. Inserisci un nome per lo stack.

   b. Fornisci l'URI alla tua istanza Jira.

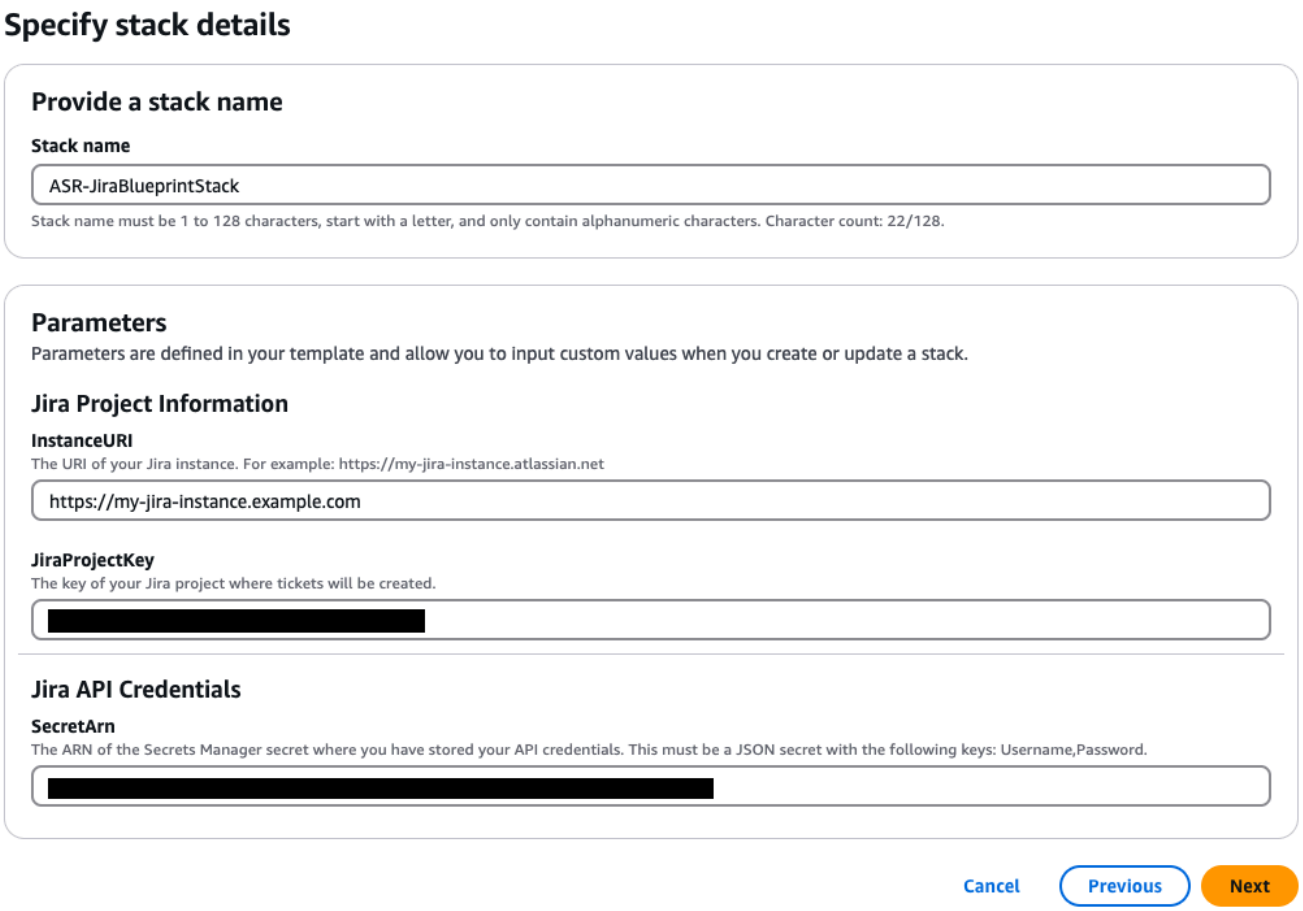
   c. Fornisci la chiave del progetto Jira a cui desideri inviare i ticket.

   d. Crea un nuovo segreto chiave-valore in Secrets Manager che contenga `Username` Jira e. `Password`

   > **Note**
   >
   > Puoi scegliere di utilizzare una chiave API Jira al posto della password fornendo il tuo nome utente come `Username` e la tua chiave API come. `Password`

e. Aggiungi l'ARN di questo segreto come input allo stack.

«Fornisci un nome di stack, informazioni sul progetto Jira e credenziali dell'API Jira.



Per distribuire lo stack: ServiceNow

f. Inserisci un nome per lo stack.

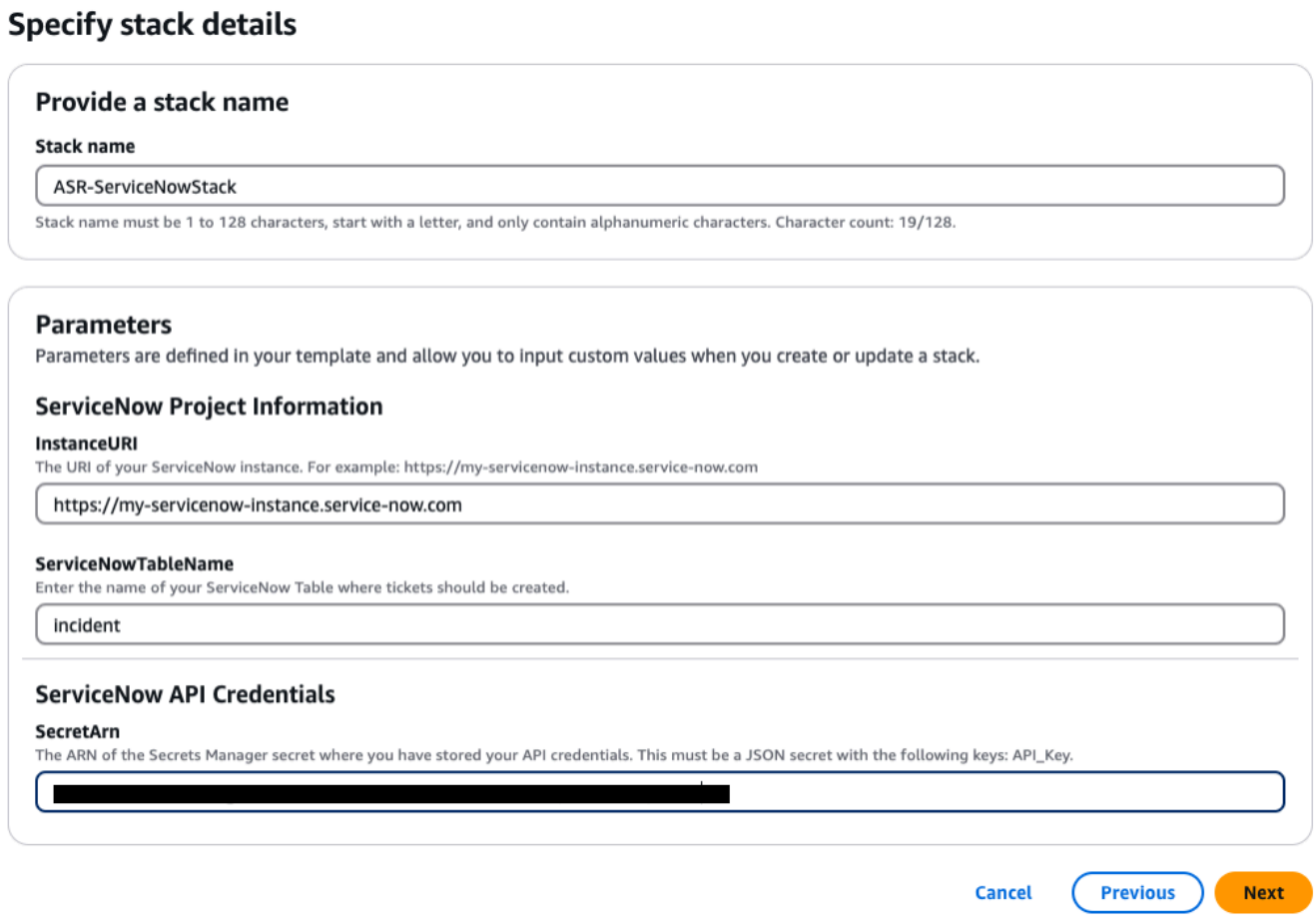
g. Fornisci l'URI della tua ServiceNow istanza.

h. Fornisci il nome della ServiceNow tabella.

i. Crea una chiave API ServiceNow con l'autorizzazione a modificare la tabella su cui intendi scrivere.

j. Crea un segreto in Secrets Manager con la chiave `API_Key` e fornisci l'ARN segreto come input per lo stack.

Fornisci un nome di stack, informazioni sul ServiceNow progetto e ServiceNow credenziali API.



Per creare uno stack di integrazione personalizzato: includi una funzione Lambda che l'orchestratore di soluzioni Step Functions può chiamare per ogni correzione. La funzione Lambda dovrebbe prendere l'input fornito da Step Functions, costruire un payload in base ai requisiti del sistema di ticketing ed effettuare una richiesta al sistema per creare il ticket.

Fase 1: Avvia lo stack di amministrazione

> **Important**
>
> Questa soluzione include un'opzione per inviare metriche operative anonime ad AWS. Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. AWS possiede i dati raccolti tramite questo sondaggio. La raccolta dei dati è soggetta all'Informativa sulla privacy di AWS.
> Per disattivare questa funzionalità, scarica il modello, modifica la sezione di CloudFormation mappatura AWS, quindi utilizza la CloudFormation console AWS per caricare il modello e

distribuire la soluzione. Per ulteriori informazioni, consulta la sezione Raccolta di dati anonimi di questa guida.

Questo CloudFormation modello AWS automatizzato distribuisce la soluzione Automated Security Response on AWS nel cloud AWS. Prima di avviare lo stack, è necessario abilitare Security Hub e completare i prerequisiti.

> **Note**
>
> Sei responsabile del costo dei servizi AWS utilizzati durante l'esecuzione di questa soluzione. Per maggiori dettagli, visita la sezione Costi di questa guida e consulta la pagina web dei prezzi per ogni servizio AWS utilizzato in questa soluzione.

1. Accedi alla Console di gestione AWS dall'account in cui è attualmente configurato AWS Security Hub e utilizza il pulsante in basso per avviare il CloudFormation modello `automated-security-response-admin.template` AWS.

   Launch solution

   Puoi anche scaricare il modello come punto di partenza per un'implementazione personalizzata.
2. Per impostazione predefinita, il modello viene lanciato nella regione Stati Uniti orientali (Virginia settentrionale). Per avviare questa soluzione in un'altra regione AWS, utilizza il selettore di regione nella barra di navigazione della Console di gestione AWS.

   > **Note**
   >
   > Questa soluzione utilizza AWS Systems Manager, attualmente disponibile solo in regioni AWS specifiche. La soluzione funziona in tutte le regioni che supportano questo servizio. Per la disponibilità più aggiornata per regione, consulta l'AWS Regional Services List.
3. Nella pagina Create stack, verifica che l'URL del modello corretto sia nella casella di testo URL Amazon S3, quindi scegli Avanti.
4. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack di soluzioni. Per informazioni sulle limitazioni dei caratteri di denominazione, consulta i limiti di IAM e STS nella AWS Identity and Access Management User Guide.

5. Nella pagina Parametri, scegli Avanti.

Parametro	Predefinito	Descrizione
Carica SC Admin Stack	`yes`	Specificate se installare i componenti di amministr azione per la riparazione automatica dei controlli SC.
Carica AFSBP Admin Stack	`no`	Specificate se installare i componenti di amministr azione per la riparazione automatica dei controlli FSBP.
Carica 0 Admin Stack CIS12	`no`	Specificate se installare i componenti di amministr azione per la riparazio ne automatica di CIS12 0 controlli.
Carica CIS14 0 Admin Stack	`no`	Specificate se installare i componenti di amministr azione per la riparazio ne automatica di CIS14 0 controlli.
Carica CIS3 00 Admin Stack	`no`	Specificare se installare i componenti di amministr azione per la riparazione automatica dei controlli CIS3 00.
Carica PC1321 Admin Stack	`no`	Specificate se installare i componenti di amministr azione per la riparazione automatica dei PC1321 controlli.

Parametro	Predefinito	Descrizione
Carica NIST Admin Stack	no	Specificate se installare i componenti di amministr azione per la riparazione automatica dei controlli NIST.
Riutilizza il gruppo di log di Orchestrator	no	Seleziona se riutilizzare o meno un gruppo di log esistente. `SO0111-ASR-Orchestrator` CloudWatc h Ciò semplifica la reinstall azione e gli aggiornam enti senza perdere i dati di registro di una versione precedente. Riutilizza `Orchestrator Log Group` quello esistente scegli `yes` se esiste `Orchestra tor Log Group` ancora da una distribuzione precedent e in questo account, altriment i. no Se stai eseguendo un aggiornamento dello stack da una versione precedente alla v2.3.0, scegli no
Usa le metriche CloudWatch	`yes`	Specificate se abilitare le CloudWatch metriche per il monitoraggio della soluzione. Questo creerà una CloudWatch dashboard per la visualizzazione delle metriche.

Parametro	Predefinito	Descrizione
Usa CloudWatch Metrics & Alarms	`yes`	Specificare se abilitare CloudWatch Metrics Alarms per la soluzione. Questo creerà allarmi per determina te metriche raccolte dalla soluzione.
RemediationFailure AlarmThreshold	5	Specificate la soglia per la percentuale di errori di riparazione per ID di controllo . Ad esempio, se si inserisce 5, si riceve un allarme se un ID di controllo fallisce per più del 5% delle riparazioni in un determinato giorno. Questo parametro funziona solo se vengono creati allarmi (vedi il parametro Use CloudWatch Metrics Alarms).
EnableEnhancedClou dWatchMetrics	no	If`yes`, crea CloudWatch metriche aggiuntive per tenere traccia di tutti i controlli IDs singolarmente sulla CloudWatch dashboard e come allarmi. CloudWatch Consulta la sezione Costo per comprendere i costi aggiuntivi che ciò comporta.

Parametro	Predefinito	Descrizione
TicketGenFunctionName	(Inserimento opzionale)	Facoltativo. Lascia vuoto se non desideri integrare un sistema di biglietteria. Altrimenti, fornisci il nome della funzione Lambda dall'output dello stack dello Step 0, ad esempio:. `S00111-ASR-ServiceNow-TicketGenerator`
TargetAccountIDs	`ALL`	Un elenco di account AWS IDs per controllare l'ambito della riparazione automatizzata. Usa «ALL» per indirizzare tutti gli account dell'organizzazione. Oppure fornisci un elenco separato da virgole di account AWS a 12 cifre. IDs Esempio: «123456789012,098765432109"

Parametro	Predefinito	Descrizione
TargetAccountIDsStrategia	`INCLUDE`	Definisce in che modo la soluzione applica le riparazioni automatiche in base all'elenco. TargetAccount IDs INCLUDE: Esegui riparazioni automatiche solo per gli account elencati. ESCLUDI: esegui riparazioni automatiche per tutti gli account tranne quelli elencati.

> **Note**
> È necessario abilitare manualmente le riparazioni automatiche nell'account Admin dopo aver distribuito o aggiornato gli stack della soluzione. CloudFormation

1. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
2. Nella pagina Rivedi, verifica e conferma le impostazioni. Seleziona la casella per confermare che il modello creerà risorse AWS Identity and Access Management (IAM).
3. Seleziona Create (Crea) per implementare lo stack.

Puoi visualizzare lo stato dello stack nella CloudFormation console AWS nella colonna Status. Dovresti ricevere lo status CREATE_COMPLETE in circa 15 minuti.

Fase 2: installa i ruoli di riparazione in ogni account membro di AWS Security Hub

`automated-security-response-member-roles.template` StackSet Devono essere distribuiti in una sola regione per account membro. Definisce i ruoli globali che consentono le chiamate API tra account dalla funzione step di ASR Orchestrator.

1. Accedi alla Console di gestione AWS per ogni account membro di AWS Security Hub (incluso l'account amministratore, che è anche membro). Seleziona il pulsante per avviare il CloudFormation modello `automated-security-response-member-roles.template` AWS. Puoi anche scaricare il modello come punto di partenza per un'implementazione personalizzata.

   Launch solution

2. Per impostazione predefinita, il modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). Per avviare questa soluzione in un'altra regione AWS, utilizza il selettore di regione nella barra di navigazione della Console di gestione AWS.
3. Nella pagina Create stack, verifica che l'URL del modello corretto sia nella casella di testo URL Amazon S3, quindi scegli Avanti.
4. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack di soluzioni. Per informazioni sulle limitazioni dei caratteri di denominazione, consulta i limiti di IAM e STS nella AWS Identity and Access Management User Guide.
5. Nella pagina Parametri, specifica i seguenti parametri e scegli Avanti.

Parametro	Predefinito	Descrizione
Spazio dei nomi	*<Requires input>*	Immettete una stringa composta da un massimo di 9 caratteri alfanumer ici minuscoli. Namespace univoco da aggiungere come suffisso ai nomi dei ruoli IAM di riparazione. Lo stesso spazio dei nomi deve essere utilizzato negli stack Member Roles e Member. Questa stringa deve essere unica per ogni implement azione della soluzione, ma non deve essere modificat a durante gli aggiornamenti dello stack. Non è necessario che il valore dello spazio dei

Parametro	Predefinito	Descrizione
		nomi sia univoco per account membro.
Amministratore dell'account Sec Hub	`<Requires input>`	Inserisci l'ID dell'account a 12 cifre per l'account amministratore di AWS Security Hub. Questo valore concede le autorizzazioni per il ruolo di soluzione dell'account amministratore.

6. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
7. Nella pagina Rivedi, verifica e conferma le impostazioni. Seleziona la casella per confermare che il modello creerà risorse AWS Identity and Access Management (IAM).
8. Seleziona Create (Crea) per implementare lo stack.

   Puoi visualizzare lo stato dello stack nella CloudFormation console AWS nella colonna Status. Dovresti ricevere lo status CREATE_COMPLETE in circa 5 minuti. Puoi continuare con il passaggio successivo durante il caricamento di questo stack.

Passaggio 3: Avvia lo stack dei membri

> **Important**
>
> Questa soluzione include un'opzione per inviare metriche operative anonime ad AWS. Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. AWS possiede i dati raccolti tramite questo sondaggio. La raccolta dei dati è soggetta alla politica sulla privacy di AWS.
> Per disattivare questa funzionalità, scarica il modello, modifica la sezione di CloudFormation mappatura AWS, quindi utilizza la CloudFormation console AWS per caricare il modello e distribuire la soluzione. Per ulteriori informazioni, consulta la sezione Raccolta di metriche operative di questa guida.

Lo `automated-security-response-member` stack deve essere installato in ogni account membro del Security Hub. Questo stack definisce i runbook per la riparazione automatica. L'amministratore di ogni account membro può controllare quali rimedi sono disponibili tramite questo stack.

1. Accedi alla Console di gestione AWS per ogni account membro di AWS Security Hub (incluso l'account amministratore, che è anche membro). Seleziona il pulsante per avviare il CloudFormation modello `automated-security-response-member.template` AWS.

   Launch solution

Puoi anche scaricare il modello come punto di partenza per la tua implementazione. Per impostazione predefinita, il modello viene avviato nella regione Stati Uniti orientali (Virginia settentrionale). Per avviare questa soluzione in un'altra regione AWS, utilizza il selettore di regione nella barra di navigazione della Console di gestione AWS.

+

> **Note**
>
> Questa soluzione utilizza AWS Systems Manager, attualmente disponibile nella maggior parte delle regioni AWS. La soluzione funziona in tutte le regioni che supportano questi servizi. Per la disponibilità più aggiornata per regione, consulta l'AWS Regional Services List.

1. Nella pagina Create stack, verifica che l'URL del modello corretto sia nella casella di testo URL Amazon S3, quindi scegli Avanti.
2. Nella pagina Specificare i dettagli dello stack, assegna un nome allo stack di soluzioni. Per informazioni sulle limitazioni dei caratteri di denominazione, consulta i limiti di IAM e STS nella AWS Identity and Access Management User Guide.
3. Nella pagina Parametri, specifica i seguenti parametri e scegli Avanti.

Parametro	Predefinito	Descrizione
Fornisci il nome LogGroup da utilizzare per creare filtri e allarmi metrici	`<Requires input>`	Specificare il nome di un gruppo CloudWatch Logs in cui CloudTrail registra le chiamate API. Viene utilizzat o per le riparazioni CIS 3.1-3.14.
Carica SC Member Stack	`yes`	Specificare se installare i componenti dei membri per la riparazione automatica dei controlli SC.
Carica lo stack di membri AFSBP	`no`	Specificare se installare i componenti dei membri per la riparazione automatica dei controlli FSBP.
Carica 0 CIS12 Member Stack	`no`	Specificare se installare i componenti membri per la riparazione automatica di CIS12 0 controlli.
Carica lo stack di CIS14 0 membri	`no`	Specificare se installare i componenti membri per la riparazione automatica di CIS14 0 controlli.
Carica uno stack di CIS3 100 membri	`no`	Specificare se installare i componenti membri per la riparazione automatica dei controlli CIS3 00.

Parametro	Predefinito	Descrizione
Carica lo stack PC1321 dei membri	no	Specificare se installare i componenti membri per la riparazione automatica dei PC1321 controlli.
Carica lo stack dei membri NIST	no	Specificare se installare i componenti membri per la riparazione automatica dei controlli NIST.
Crea un bucket S3 per la registrazione di audit di Redshift	no	Seleziona `yes` se il bucket S3 deve essere creato per la riparazione di FSBP 1.4. RedShift Per i dettagli sul bucket S3 e sulla correzion e, consulta la correzion e Redshift.4 nella AWS Security Hub User Guide.
Account amministratore Sec Hub	*`<Requires input>`*	Inserisci l'ID dell'account a 12 cifre per l'account amministr atore di AWS Security Hub.

Parametro	Predefinito	Descrizione
Spazio dei nomi	*<Requires input>*	Inserisci una stringa composta da un massimo di 9 caratteri alfanumerici minuscoli. Questa stringa diventa parte dei nomi dei ruoli IAM e del bucket Action Log S3. Usa lo stesso valore per la distribuzione dello stack dei membri e la distribuzione dello stack dei ruoli dei membri. La stringa deve essere unica per ogni implementazione della soluzione, ma non deve essere modificata durante gli aggiornamenti dello stack.
EnableCloudTrailFo rASRActionLog	no	Seleziona `yes` se desideri monitorare gli eventi di gestione condotti dalla soluzione sulla CloudWatc h dashboard. La soluzione crea una CloudTrail traccia in ogni account membro selezionato`yes`. È necessari o distribuire la soluzione in un'organizzazione AWS per abilitare questa funzionalità. Consulta la sezione Costo per comprendere i costi aggiuntivi che ciò comporta.

4. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).
5. Nella pagina Rivedi, verifica e conferma le impostazioni. Seleziona la casella per confermare che il modello creerà risorse AWS Identity and Access Management (IAM).

6. Seleziona Create (Crea) per implementare lo stack.

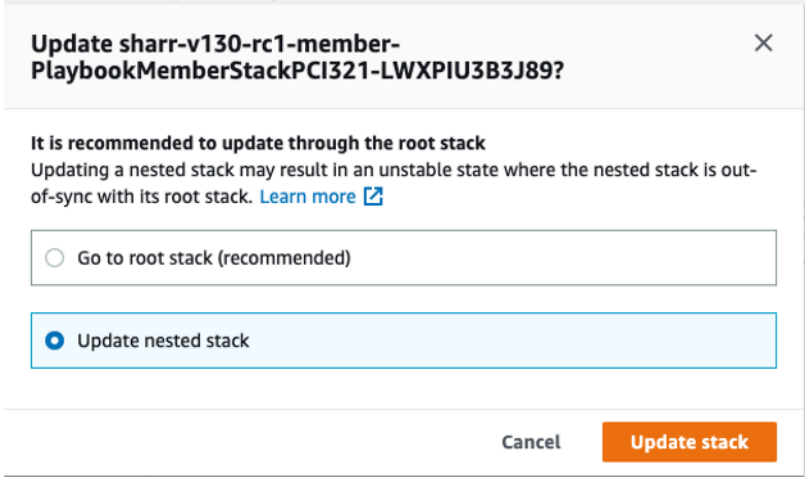
Puoi visualizzare lo stato dello stack nella CloudFormation console AWS nella colonna Status. Dovresti ricevere lo status CREATE_COMPLETE in circa 15 minuti.

Fase 4: (Facoltativo) Modifica le correzioni disponibili

Se desideri rimuovere rimedi specifici da un account membro, puoi farlo aggiornando lo stack annidato per lo standard di sicurezza. Per semplicità, le opzioni dello stack annidato non vengono propagate allo stack principale.

1. Accedi alla CloudFormation console AWS e seleziona lo stack annidato.
2. Scegli Aggiorna.
3. Seleziona Update nested stack e scegli Update stack.

   Aggiorna lo stack annidato



4. Seleziona Usa il modello corrente e scegli Avanti.
5. Modifica le correzioni disponibili. Cambia i valori per i controlli desiderati `Available` e i controlli indesiderati in. `Not available`

   > **Note**
   >
   > La disattivazione di una correzione rimuove il runbook di correzione delle soluzioni per lo standard e il controllo di sicurezza.

6. Nella pagina Configure stack options (Configura opzioni pila), scegliere Next (Successivo).

7. Nella pagina Rivedi, verifica e conferma le impostazioni. Seleziona la casella per confermare che il modello creerà risorse AWS Identity and Access Management (IAM).
8. Scegli Aggiorna stack.

Puoi visualizzare lo stato dello stack nella CloudFormation console AWS nella colonna Status. Dovresti ricevere lo status CREATE_COMPLETE in circa 15 minuti.

Implementazione di Control Tower (CT)

La guida Customizations for AWS Control Tower (cFCT) è rivolta ad amministratori, DevOps professionisti, fornitori di software indipendenti, architetti di infrastrutture IT e integratori di sistemi che desiderano personalizzare ed estendere i propri ambienti AWS Control Tower per la propria azienda e i propri clienti. Fornisce informazioni sulla personalizzazione e l'estensione dell'ambiente AWS Control Tower con il pacchetto di personalizzazione cFCT.

Tempo di implementazione: circa 30 minuti

Prerequisiti

Prima di distribuire questa soluzione, assicurati che sia destinata agli amministratori di AWS Control Tower.

Quando sei pronto per configurare la tua landing zone utilizzando la console AWS Control Tower APIs, oppure segui questi passaggi:

Per iniziare a usare AWS Control Tower, consulta: Getting Started with AWS Control Tower

Per informazioni su come personalizzare la tua landing zone, consulta: Personalizzazione della tua landing zone

Per lanciare e dispiegare la tua landing zone, consulta: Landing Zone Deployment Guide

Panoramica sulla distribuzione

Utilizza i seguenti passaggi per distribuire questa soluzione su AWS.

Fase 1: Crea e distribuisci un bucket S3

> **Note**
>
> Configurazione del bucket S3: solo per amministratori. Si tratta di un passaggio di configurazione che si effettua una sola volta e non deve essere ripetuto dagli utenti finali. I bucket S3 memorizzano il pacchetto di distribuzione, incluso il CloudFormation modello AWS e il codice Lambda necessari per l'esecuzione di ASR. Queste risorse vengono distribuite utilizzando o. CfCt StackSet

1. Configura il bucket S3

Configura il bucket S3 che verrà utilizzato per archiviare e servire i pacchetti di distribuzione.

2. Configurazione dell'ambiente

Prepara le variabili di ambiente, le credenziali e gli strumenti necessari per il processo di creazione e distribuzione.

3. Configura le politiche dei bucket S3

Definisci e applica le policy bucket appropriate per controllare l'accesso e le autorizzazioni.

4. Prepara la build

Compila, impacchetta o prepara in altro modo l'applicazione o le risorse per la distribuzione.

5. Distribuisci pacchetti su S3

Carica gli artefatti di build preparati nel bucket S3 designato.

Fase 2: distribuzione di Stacks su AWS Control Tower

1. Crea Build Manifest per i componenti ASR

Definisci un manifesto di compilazione che elenchi tutti i componenti ASR, le relative versioni, dipendenze e istruzioni di compilazione.

2. Aggiorna il CodePipeline

Modifica la CodePipeline configurazione AWS per includere i nuovi passaggi di build, artefatti o fasi necessari per la distribuzione dei componenti ASR.

Fase 1: Crea e distribuisci nel bucket S3

Le soluzioni AWS utilizzano due bucket: un bucket per l'accesso globale ai modelli, a cui si accede tramite HTTPS, e un bucket regionale per l'accesso agli asset all'interno della regione, come il codice Lambda.

1. Configura il bucket S3

Scegli un nome univoco per il bucket, ad esempio asr-staging. Imposta due variabili di ambiente sul tuo terminale, una dovrebbe essere il nome del bucket di base con -reference come suffisso, l'altra con la regione di distribuzione desiderata come suffisso:

```
export BASE_BUCKET_NAME=asr-staging-$(date +%s)
export TEMPLATE_BUCKET_NAME=$BASE_BUCKET_NAME-reference
export REGION=us-east-1
export ASSET_BUCKET_NAME=$BASE_BUCKET_NAME-$REGION
```

2. Configurazione dell'ambiente

Nel tuo account AWS, crea due bucket con questi nomi, ad esempio asr-staging-reference e asr-staging-us-east -1. (Il bucket di riferimento conterrà i CloudFormation modelli, il bucket regionale conterrà tutte le altre risorse come il bundle di codice lambda.) I bucket devono essere crittografati e impedire l'accesso pubblico

```
aws s3 mb s3://$TEMPLATE_BUCKET_NAME/
aws s3 mb s3://$ASSET_BUCKET_NAME/
```

> **Note**
>
> Quando crei i bucket, assicurati che non siano accessibili al pubblico. Usa nomi casuali per i bucket. Disabilita l'accesso pubblico. Usa la crittografia KMS. E verifica la proprietà del bucket prima di caricarlo.

3. Configurazione della politica dei bucket S3

Aggiorna la policy del bucket S3 di $TEMPLATE_BUCKET_NAME per includere le autorizzazioni per l'ID dell'account di esecuzione. PutObject Assegna questa autorizzazione a un ruolo IAM all'interno dell'account di esecuzione che è autorizzato a scrivere nel bucket. Questa configurazione consente di evitare di creare il bucket nell'account di gestione.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::<template bucket name>/*",
                "arn:aws:s3:::<template bucket name>"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "<org id>"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
                "arn:aws:s3:::<template bucket name>/*",
                "arn:aws:s3:::<template bucket name>"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::<execute_account_id>:role/
<iam_role_name>"
                }
            }
        }
    ]
}
```

Modifica la policy del bucket S3 dell'asset per includere le autorizzazioni. Assegna questa autorizzazione a un ruolo IAM all'interno dell'account di esecuzione che è autorizzato a scrivere nel bucket. Ripeti questa configurazione per ogni bucket di asset regionale (ad esempio, asr-staging-us-east -1, asr-staging-eu-west -1, ecc.), consentendo le distribuzioni in più regioni senza la necessità di creare i bucket nell'account di gestione.

```
{
```

```
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:GetObject",
            "Resource": [
                "arn:aws:s3:::<asset bucket name>-<region>/*",
                "arn:aws:s3:::<asset bucket name>-<region>"
            ],
            "Condition": {
                "StringEquals": {
                    "aws:PrincipalOrgID": "<org id>"
                }
            }
        },
        {
            "Effect": "Allow",
            "Principal": "*",
            "Action": "s3:PutObject",
            "Resource": [
            "arn:aws:s3:::<asset bucket name>-<region>/*",
                "arn:aws:s3:::<asset bucket name>-<region>"
            ],
            "Condition": {
                "ArnLike": {
                    "aws:PrincipalArn": "arn:aws:iam::<execute_account_id>:role/
<iam_role_name>"
                }
            }
        }
    ]
}
```

4. Preparazione alla costruzione

- Prerequisiti:
  - CLI AWS v2
  - Python 3.11+ con pip
  - CDK AWS 2.171,1 E VERSIONI SUCCESSIVE
  - Node.js 20+ con npm

- Poetry v2 con plugin per l'esportazione
- Git clone https://github.com/aws-solutions/ automated-security-response-on -aws.git

Per prima cosa assicurati di aver eseguito npm install nella cartella dei sorgenti.

Successivamente, dalla cartella di distribuzione nel repository clonato, esegui build-s3-dist.sh, passando il nome root del bucket (es. mybucket) e la versione che stai creando (es. v1.0.0). Ti consigliamo di utilizzare una versione semver basata sulla versione scaricata da (es. GitHub GitHub: v1.0.0, la tua build: v1.0.0.mybuild)

```
chmod +x build-s3-dist.sh
export SOLUTION_NAME=automated-security-response-on-aws
export SOLUTION_VERSION=v1.0.0.mybuild
./build-s3-dist.sh -b $BASE_BUCKET_NAME -v $SOLUTION_VERSION
```

5. Distribuisci pacchetti su S3

```
cd deployment
aws s3 cp global-s3-assets/  s3://$TEMPLATE_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
aws s3 cp regional-s3-assets/  s3://$ASSET_BUCKET_NAME/$SOLUTION_NAME/
$SOLUTION_VERSION/ --recursive --acl bucket-owner-full-control
```

Fase 2: distribuzione di Stacks su AWS Control Tower

1. Crea un manifesto per i componenti ASR

Dopo aver distribuito gli artefatti ASR nei bucket S3, aggiorna il manifesto della pipeline Control Tower in modo che faccia riferimento alla nuova versione, quindi attiva l'esecuzione della pipeline, consulta: distribuzione controltower

> **Important**
>
> Per garantire la corretta implementazione della soluzione ASR, consulta la documentazione ufficiale di AWS per informazioni dettagliate sulla panoramica dei CloudFormation modelli e sulla descrizione dei parametri. Link informativi di seguito: Panoramica dei CloudFormation modelli, Guida ai parametri

Il manifesto per i componenti ASR ha il seguente aspetto:

```
region: us-east-1 #<HOME_REGION_NAME>
version: 2021-03-15

# Control Tower Custom CloudFormation Resources
resources:
  - name: <ADMIN STACK NAME>
    resource_file: s3://<ADMIN TEMPLATE BUCKET path>
    parameters:
      - parameter_key: UseCloudWatchMetricsAlarms
        parameter_value: "yes"
      - parameter_key: TicketGenFunctionName
        parameter_value: ""
      - parameter_key: LoadSCAdminStack
        parameter_value: "yes"
      - parameter_key: LoadCIS120AdminStack
        parameter_value: "no"
      - parameter_key: TargetAccountIDsStrategy
        parameter_value: "INCLUDE"
      - parameter_key: LoadCIS300AdminStack
        parameter_value: "no"
      - parameter_key: UseCloudWatchMetrics
        parameter_value: "yes"
      - parameter_key: LoadNIST80053AdminStack
        parameter_value: "no"
      - parameter_key: LoadCIS140AdminStack
        parameter_value: "no"
      - parameter_key: ReuseOrchestratorLogGroup
        parameter_value: "yes"
      - parameter_key: LoadPCI321AdminStack
        parameter_value: "no"
      - parameter_key: RemediationFailureAlarmThreshold
        parameter_value: "5"
      - parameter_key: LoadAFSBPAdminStack
        parameter_value: "no"
      - parameter_key: TargetAccountIDs
        parameter_value: "ALL"
      - parameter_key: EnableEnhancedCloudWatchMetrics
        parameter_value: "no"
    deploy_method: stack_set
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
```

```
        - <ACCOUNT_NUMBER>
    regions:
      - <REGION_NAME>

  - name:  <ROLE MEMBER STACK NAME>
    resource_file: s3://<ROLE MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
    deploy_method: stack_set
    deployment_targets:
      organizational_units:
        - <ORG UNIT>

  - name:  <MEMBER STACK NAME>
    resource_file: s3://<MEMBER TEMPLATE BUCKET path>
    parameters:
      - parameter_key: SecHubAdminAccount
        parameter_value: <ADMIN_ACCOUNT_NAME>
      - parameter_key: LoadCIS120MemberStack
        parameter_value: "no"
      - parameter_key: LoadNIST80053MemberStack
        parameter_value: "no"
      - parameter_key: Namespace
        parameter_value: <NAMESPACE>
      - parameter_key: CreateS3BucketForRedshiftAuditLogging
        parameter_value: "no"
      - parameter_key: LoadAFSBPMemberStack
        parameter_value: "no"
      - parameter_key: LoadSCMemberStack
        parameter_value: "yes"
      - parameter_key: LoadPCI321MemberStack
        parameter_value: "no"
      - parameter_key: LoadCIS140MemberStack
        parameter_value: "no"
      - parameter_key: EnableCloudTrailForASRActionLog
        parameter_value: "no"
      - parameter_key: LogGroupName
        parameter_value: <LOG_GROUP_NAME>
      - parameter_key: LoadCIS300MemberStack
        parameter_value: "no"
    deploy_method: stack_set
```

```
    deployment_targets:
     accounts: # :type: list
        - <ACCOUNT_NAME> # and/or
        - <ACCOUNT_NUMBER>
    organizational_units:
      - <ORG UNIT>
    regions: # :type: list
      - <REGION_NAME>
```

2. Aggiornamento della pipeline del codice

Aggiungi un file manifest a un custom-control-tower-configuration file.zip ed esegui un file CodePipeline, consulta: code pipeline overview

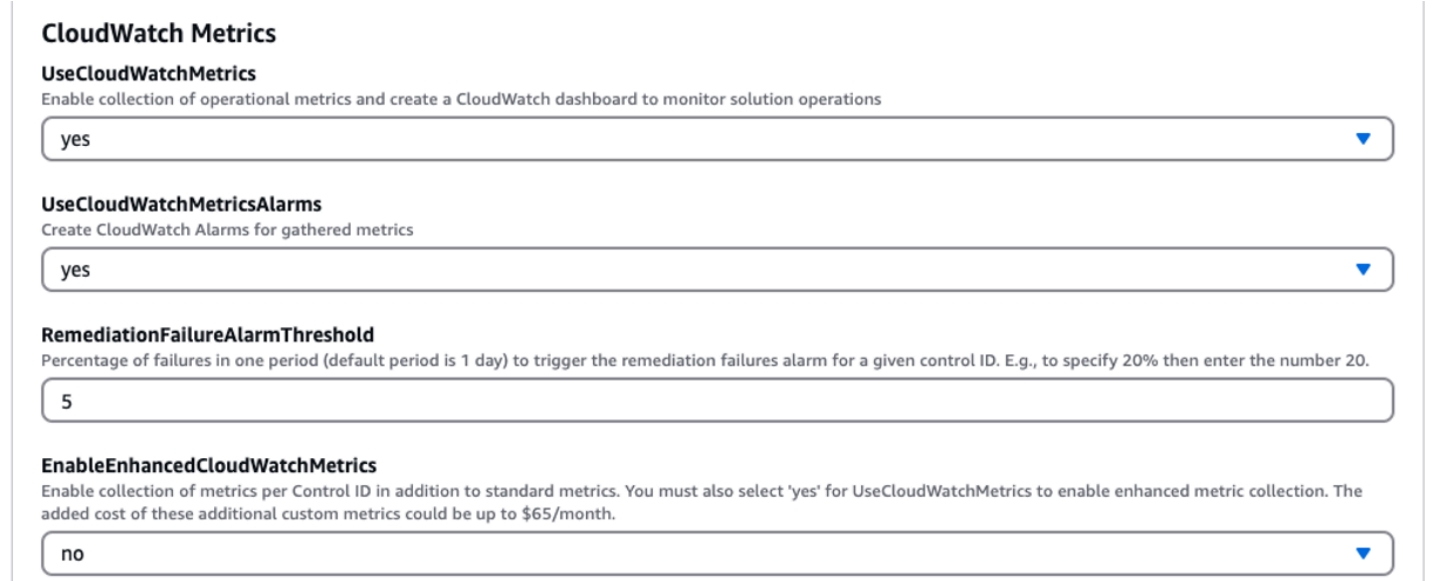
Monitora le operazioni della soluzione con una CloudWatch dashboard di Amazon

Questa soluzione include metriche e allarmi personalizzati visualizzati su una dashboard di Amazon CloudWatch .

La CloudWatch dashboard e gli allarmi monitorano le operazioni della soluzione e avvisano quando c'è un potenziale problema.

Abilitazione di CloudWatch metriche, allarmi e dashboard

Esistono quattro parametri del CloudFormation modello per la CloudWatch funzionalità.



1. UseCloudWatchMetrics- Questa impostazione `yes` consente la raccolta di metriche operative e crea una CloudWatch dashboard per visualizzare tali metriche.
2. UseCloudWatchAlarms- Impostazione per `yes` abilitare gli allarmi predefiniti della soluzione.
3. RemediationFailureAlarmThreshold- La percentuale di riparazioni non riuscite in un periodo in cui è stato generato un allarme.
4. EnableEnhancedCloudWatchMetrics- Imposta questo parametro per `yes` raccogliere metriche individuali per ID di controllo. Per impostazione predefinita, questo parametro è impostato suno, in modo che vengano raccolte solo le metriche relative al numero totale di correzioni relative a tutto il controllo IDs . Le metriche e gli allarmi individuali per ID di controllo comportano costi aggiuntivi.

Utilizzo della dashboard CloudWatch

Per visualizzare la dashboard:

1. Vai su Amazon CloudWatch e poi su Dashboards.
2. Seleziona la dashboard denominata «ASR-Remediation-Metrics-Dashboard».

CloudWatch La dashboard contiene le seguenti sezioni:

1. Rimediazioni totali riuscite: fornisce informazioni sul numero di risultati del Security Hub che sono stati risolti con successo dalla soluzione.
2. Risoluzioni non riuscite: mostra quante riparazioni hanno avuto esito negativo, sia in totale che in percentuale, e la causa dell'errore. Un numero elevato di errori può suggerire la presenza di un problema tecnico relativo alla soluzione che potrebbe essere necessario esaminare in modo più dettagliato.
3. Riparazione successa/fallimento per Control ID: se hai abilitato Enhanced Metrics al momento della distribuzione, questa sezione elenca i risultati della correzione per ID di controllo. Quando la sezione Errori di riparazione mostra un tasso di errore elevato in generale, in questa sezione viene indicato se gli errori sono distribuiti su più controlli o se solo alcuni controlli IDs falliscono. IDs
4. Runbook Assume Role Failures: mostra il numero di errori che si sono verificati a causa di tentativi di riparazione in account in cui non è installato il ruolo Solution Member. I ripetuti errori dovuti ai tentativi di riparazione automatici dovuti alla mancanza di ruoli causano costi inutili. Attenua questo problema installando lo stack di ruoli Member negli account interessati, disabilitando tutte le EventBridge regole create dalla soluzione o dissociando l'account in Security Hub.
5. Cloud Trail Management Actions by ASR: elenca le azioni di gestione della soluzione su tutti gli account membri in cui hai abilitato Action Logs con il parametro Log al momento dell'implementazione. EnableCloudTrailFor ASRAction Quando osservi cambiamenti imprevisti delle risorse in uno qualsiasi dei tuoi account AWS, questo widget può aiutarti a capire se le risorse sono state modificate dalla soluzione.

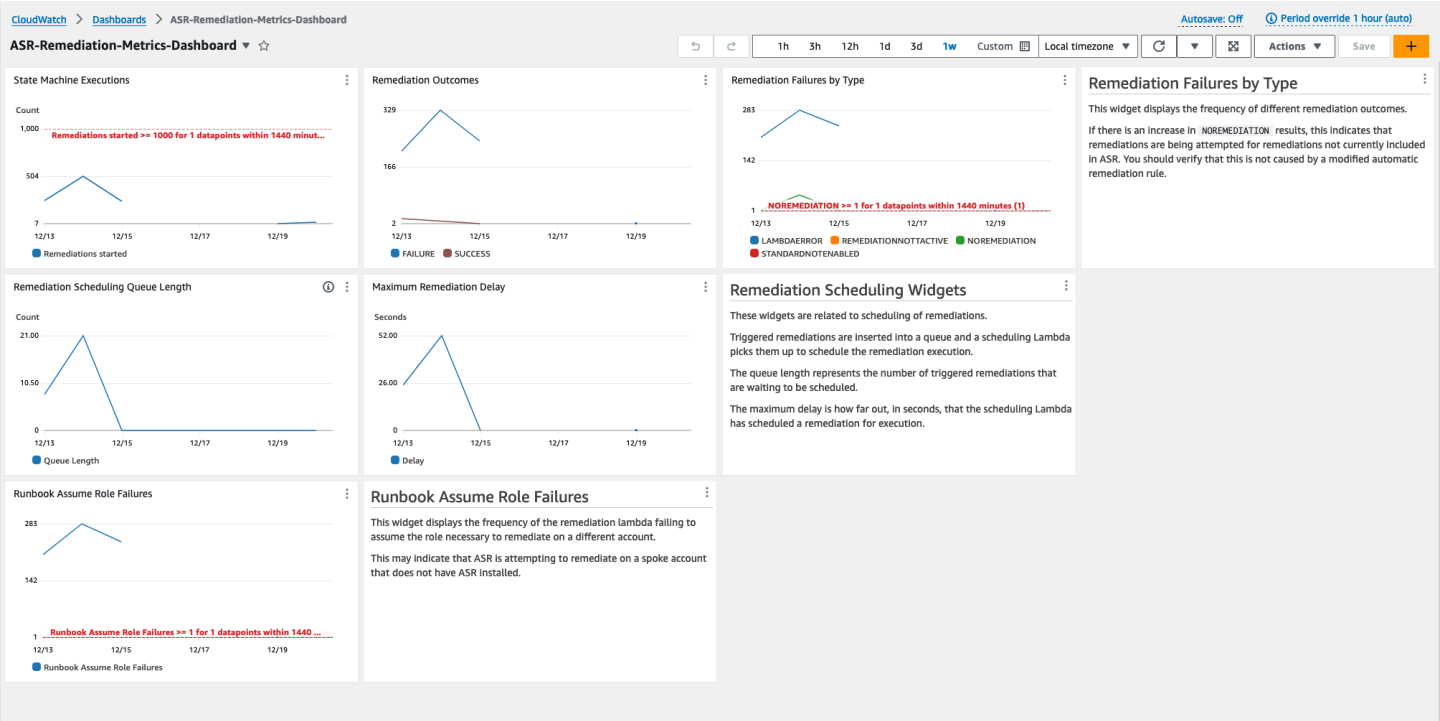
La CloudWatch dashboard è inoltre dotata di allarmi predefiniti che segnalano errori operativi comuni.

1. Esecuzioni di State Machine > 1000 in un periodo di 24 ore.
   a. Un forte picco nelle esecuzioni di riparazione potrebbe indicare che una regola di evento viene avviata più spesso del previsto.

   b. La soglia può essere modificata utilizzando il parametro. CloudFormation

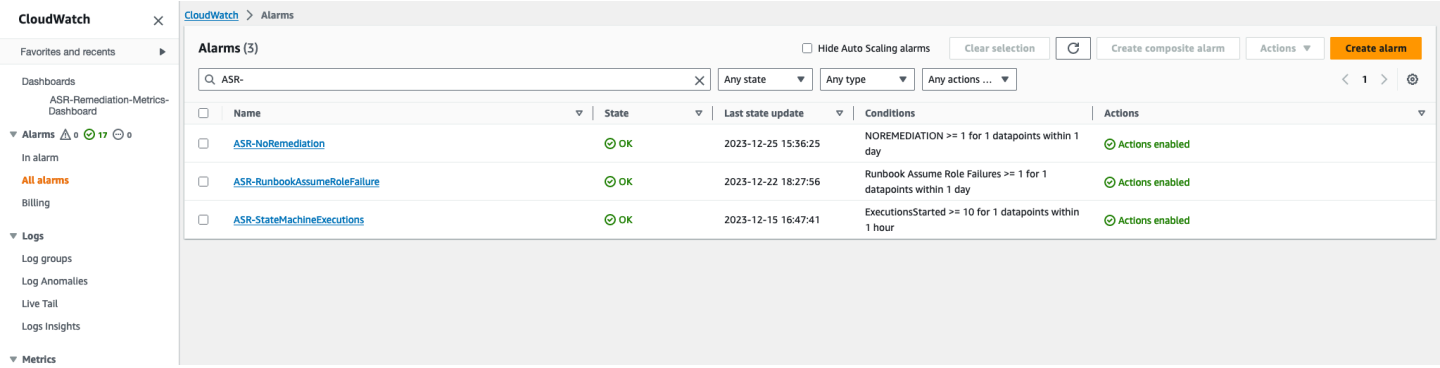
2. Errori di riparazione per tipo = NOREMEDIATION > 0
   a. Sono in corso tentativi di riparazione per riparazioni non incluse in ASR. Ciò potrebbe indicare che una regola relativa all'evento è stata modificata in modo da includere più riparazioni rispetto a quelle previste.
3. Runbook Assume errori di ruolo > 0
   a. Si stanno tentando di porre rimedio agli account o alle regioni in cui la soluzione non è stata distribuita correttamente. Ciò potrebbe indicare che una regola relativa all'evento è stata modificata per includere più account del previsto.

Tutte le soglie di allarme possono essere modificate per soddisfare le esigenze di implementazione individuali.

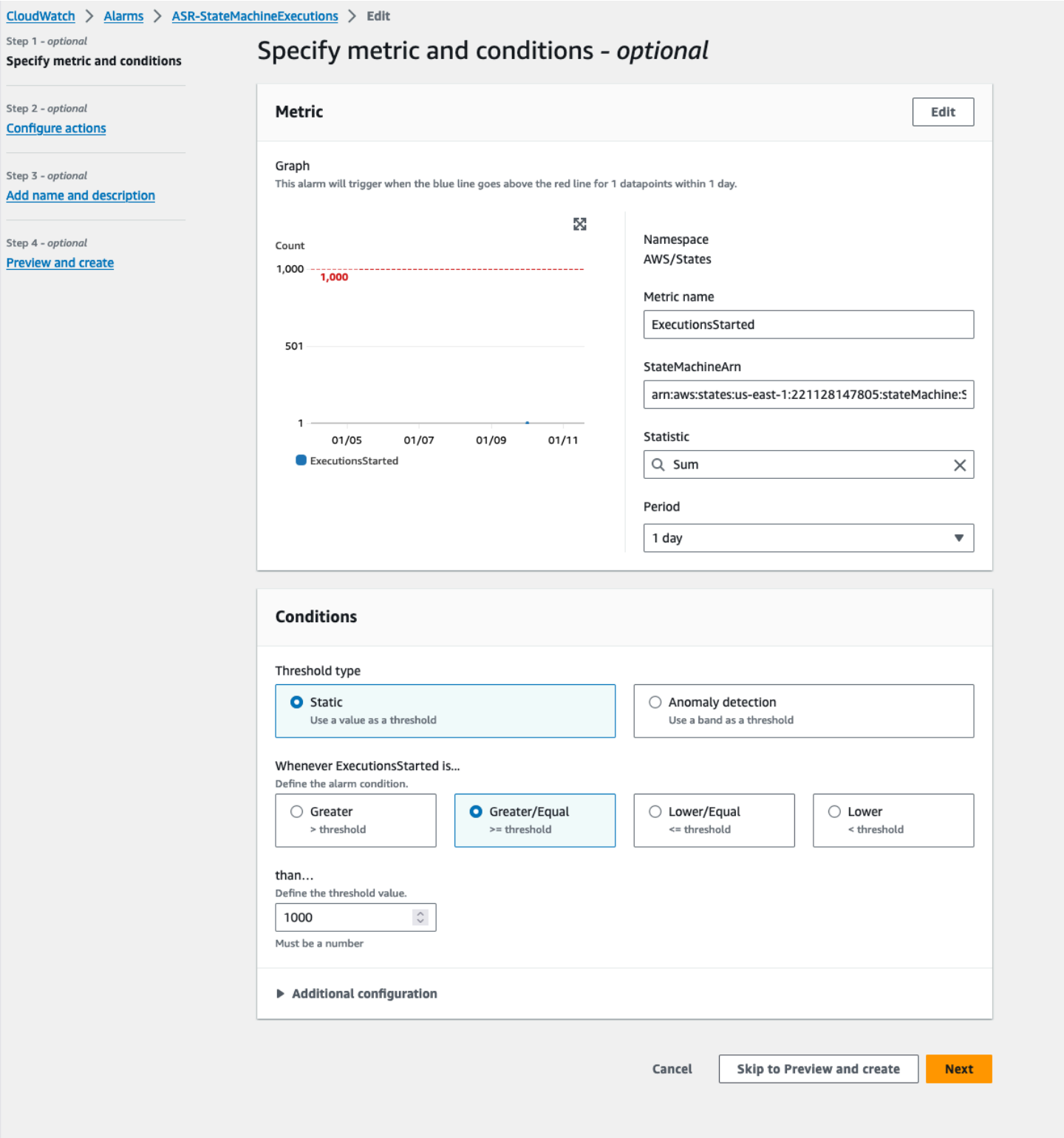


Modifica delle soglie di allarme

1. Vai su Amazon CloudWatch → Allarmi → Tutti gli allarmi.
2. Scegli l'allarme che desideri modificare, quindi seleziona Azioni → Modifica.



1. Cambia la soglia con il valore desiderato e salva.

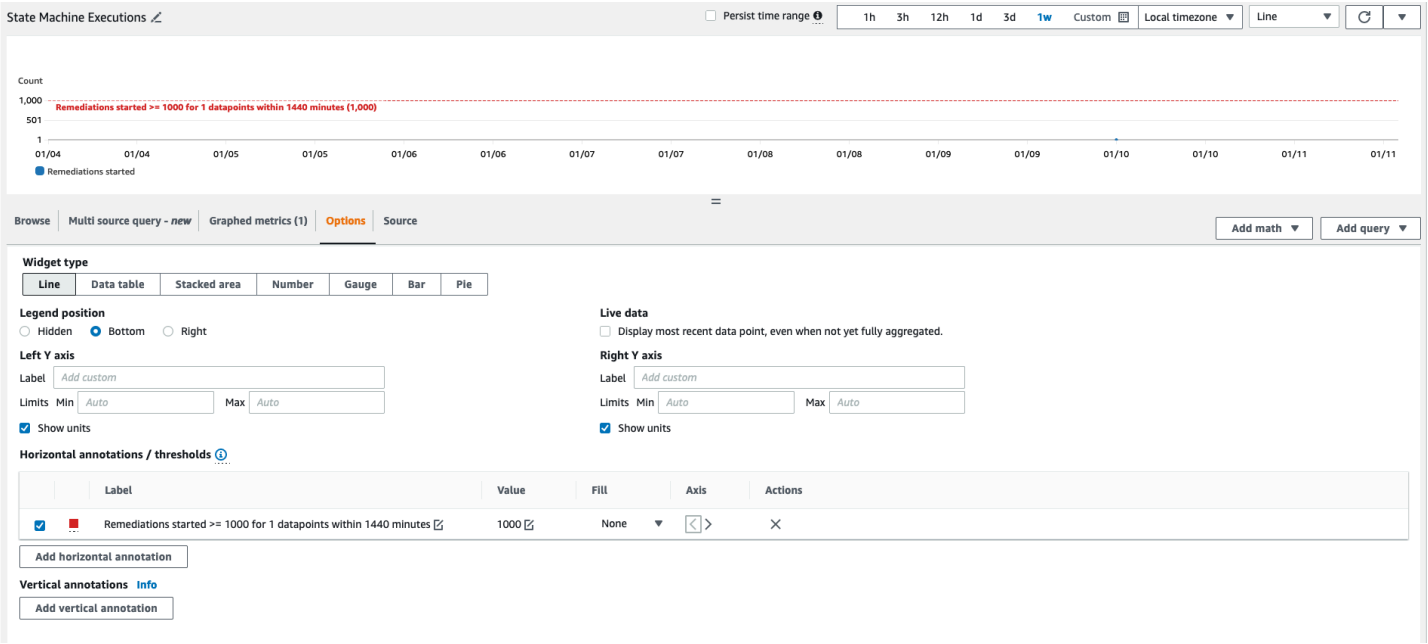


1. Vai alla CloudWatch dashboard per modificare i grafici in modo che corrispondano alle nuove impostazioni.
   a. Seleziona i puntini di sospensione in alto a destra del widget corrispondente.

b. Seleziona Edit (Modifica).

c. Passate alla scheda Opzioni.

d. Modifica l'annotazione dell'allarme in modo che corrisponda alle nuove impostazioni.



Iscrizione alle notifiche di allarme

Nell'account amministratore, iscriviti all'argomento Amazon SNS creato dallo stack di amministrazione, SO0111-ASR_alarm_topic. Questo ti avviserà quando un allarme entra nello stato ALARM.

Aggiorna la soluzione

Aggiornamento da versioni precedenti alla v1.4

Se hai già distribuito la soluzione prima della versione 1.4.x, disinstallala e installa la versione più recente:

1. Disinstalla la soluzione precedentemente distribuita. Fare riferimento a Disinstallare la soluzione.
2. Avvia il modello più recente. Fare riferimento a Implementare la soluzione.

> **Note**
>
> Se stai effettuando l'aggiornamento dalla v1.2.1 o precedente alla v1.3.0 o successiva, imposta Use existing Orchestrator Log Group su. No Se stai reinstallando la versione 1.3.0 o successiva, puoi selezionare questa opzione. `Yes` Questa opzione consente di continuare a accedere allo stesso gruppo di log per Orchestrator Step Functions.

Aggiornamento dalla v1.4 e versioni successive

Se stai eseguendo l'aggiornamento dalla v1.4.x, aggiorna tutti gli stack o come segue: StackSets

1. Aggiorna lo stack nell'account amministratore di Security Hub utilizzando il modello più recente.
2. In ogni account membro, aggiorna le autorizzazioni dal modello più recente.
3. In ogni account membro in tutte le regioni in cui è attualmente distribuito, aggiorna lo stack di membri utilizzando il modello più recente.

Aggiornamento dalla v2.0.x

Se stai effettuando l'aggiornamento dalla v2.0.x, esegui l'aggiornamento alla versione 2.1.2 o successiva. L'aggiornamento alla v2.1.0 - v2.1.1 avrà esito negativo. CloudFormation

Note

- Durante l'aggiornamento della soluzione, potrebbe essere necessario riattivare manualmente le regole di correzione automatica nell'account Admin. Fai riferimento a Abilitare riparazioni completamente automatizzate.
- Se utilizzate il `Reuse Orchestrator Log Group` parametro per conservare i log, assicuratevi che sia impostato correttamente durante l'aggiornamento dello stack per evitare la ricreazione dei gruppi di log o la perdita delle impostazioni di conservazione dei log. Fare riferimento a Implementare la soluzione. Se stai eseguendo un aggiornamento dello stack alla v2.3.0+ da una versione precedente, scegli «no»

Risoluzione dei problemi

La risoluzione di problemi noti fornisce istruzioni per mitigare gli errori noti. Se queste istruzioni non risolvono il problema, Contatta AWS Support fornisce istruzioni per aprire un caso AWS Support per questa soluzione.

Log delle soluzioni

Questa sezione include informazioni sulla risoluzione dei problemi per questa soluzione, consulta la navigazione a sinistra per gli argomenti.

Questa soluzione raccoglie l'output dai runbook di correzione, eseguiti in AWS Systems Manager, e registra il risultato nel gruppo Logs nell'account amministratore di CloudWatch AWS `SO0111-ASR` Security Hub. Esiste un flusso per controllo al giorno.

Orchestrator Step Functions registra tutte le transizioni di passaggio nel gruppo `SO0111-ASR-Orchestrator` CloudWatch Logs nell'account amministratore di AWS Security Hub. Questo registro è una traccia di controllo per registrare le transizioni di stato per ogni istanza di Step Functions. Esiste un flusso di log per ogni esecuzione di Step Functions.

Entrambi i gruppi di log sono crittografati utilizzando una chiave AWS KMS Customer-Manager (CMK).

Le seguenti informazioni per la risoluzione dei problemi utilizzano il gruppo di log. `SO0111-ASR` Utilizza questo registro, oltre alla console AWS Systems Manager Automation, ai log di Automation Executions, alla console Step Function e ai log Lambda per risolvere i problemi.

Se una riparazione fallisce, un messaggio simile al seguente verrà registrato `SO0111-ASR` nel flusso di log per lo standard, il controllo e la data. Ad esempio: CIS-2.9-2021-08-12

```
ERROR: a4cbb9bb-24cc-492b-a30f-1123b407a6253: Remediation failed for CIS control
 2.9 in account 123412341234: See Automation Execution output for details (AwsEc2Vpc
 vpc-0e92bbe911cf08acb)
```

I seguenti messaggi forniscono ulteriori dettagli. Questo output proviene dal runbook ASR per lo standard di sicurezza e il controllo. Ad esempio: ASR-CIS_1.2.0_2.9

```
Step fails when it is Execution complete: verified. Failed to run automation with
 executionId: eecdef79-9111-4532-921a-e098549f5259 Failed :
```

```
{Status=[Failed], Output=[No output available yet because the step is not successfully
 executed], ExecutionId=[eecdef79-9111-4532-921a-e098549f5259]}. Please refer to
 Automation Service Troubleshooting Guide for more diagnosis details.
```

Queste informazioni indicano l'errore, che in questo caso era un'automazione secondaria in esecuzione nell'account del membro. Per risolvere questo problema, devi accedere alla Console di gestione AWS nell'account del membro (dal messaggio sopra), andare su AWS Systems Manager, accedere ad Automation ed esaminare l'output del log per l'ID di esecuzione. `eecdef79-9111-4532-921a-e098549f525`

Risoluzione di problemi noti

- Problema: l'implementazione della soluzione non riesce a causa di un errore che indica che le risorse sono già disponibili in Amazon CloudWatch.

  Risoluzione: verifica la presenza di un messaggio di errore nella sezione CloudFormation risorse/eventi che indica che i gruppi di log esistono già. I modelli di distribuzione ASR consentono il riutilizzo dei gruppi di log esistenti. Verifica di aver selezionato il riutilizzo.
- Problema: la soluzione non viene distribuita con un errore in uno stack annidato di playbook in cui non viene creata una regola EventBridge

  Risoluzione: probabilmente hai raggiunto la quota di EventBridge regole con il numero di playbook distribuiti. Puoi evitarlo utilizzando i risultati del controllo consolidato in Security Hub abbinati al playbook SC di questa soluzione, implementando solo i playbook per gli standard utilizzati o richiedendo un aumento della quota di regole. EventBridge
- Problema: eseguo Security Hub in più regioni con lo stesso account. Voglio implementare questa soluzione in più regioni.

  Soluzione: distribuisci lo stack di amministrazione nello stesso account e nella stessa regione dell'amministratore del Security Hub. Installa il modello di membro in ogni account e regione in cui è configurato un membro del Security Hub. Abilita l'aggregazione nel Security Hub.
- Problema: subito dopo la distribuzione, SO0111-ASR-Orchestrator non funziona nello stato del documento Get Automation con un errore 502: «`Lambda non è riuscita a decrittografare le variabili di ambiente perché l'accesso al KMS è stato negato. Controlla le impostazioni dei tasti KMS della funzione. Eccezione KMS: messaggio UnrecognizedClientException KMS: il token di sicurezza incluso nella richiesta non è valido. (Servizio: AWSLambda; Codice di stato: 502; Codice di errore:; ID richiesta: KMSAccessDeniedException... `»

Risoluzione: attendere circa 10 minuti per stabilizzare la soluzione prima di eseguire le riparazioni. Se il problema persiste, apri un ticket o GitHub un problema di assistenza.

- Problema: ho tentato di porre rimedio a un problema ma non è successo nulla.

  Risoluzione: controlla le note del risultato per scoprire i motivi per cui non è stato posto rimedio. Una causa comune è che non è prevista alcuna correzione automatica del problema. Al momento non è possibile fornire un feedback diretto all'utente se non esiste alcuna soluzione se non tramite le note. Esamina i log della soluzione. Apri CloudWatch Logs nella console. Trova il gruppo CloudWatch SO0111-ASR Logs. Ordina l'elenco in modo che gli stream aggiornati più di recente vengano visualizzati per primi. Seleziona il flusso di registro per il risultato che hai tentato di eseguire. Dovresti trovare eventuali errori lì. Alcune ragioni dell'errore potrebbero essere: mancata corrispondenza tra Finding Control e Correation Control, risoluzione tra account diversi (non ancora supportata) o il fatto che il risultato sia già stato risolto. Se non riesci a determinare il motivo dell'errore, raccogli i log e apri un ticket di assistenza.
- Problema: dopo aver avviato una riparazione, lo stato nella console Security Hub non è stato aggiornato.

  Risoluzione: la console Security Hub non si aggiorna automaticamente. Aggiorna la visualizzazione corrente. Lo stato del risultato dovrebbe essere aggiornato. Potrebbero essere necessarie diverse ore prima che il risultato passi da Failed a Passed. I risultati vengono creati dai dati degli eventi inviati da altri servizi, come AWS Config, ad AWS Security Hub. Il tempo prima che una regola venga rivalutata dipende dal servizio sottostante. Se ciò non risolve il problema, fate riferimento alla risoluzione precedente per «`Ho provato a correggere un problema ma non è successo niente. `»
- Problema: la funzione step di Orchestrator non funziona in Get Automation Document State: si è verificato un errore (AccessDenied) durante la chiamata dell'operazione. AssumeRole

  Risoluzione: il modello di membro non è stato installato nell'account membro in cui ASR sta tentando di correggere un risultato. Segui le istruzioni per la distribuzione del modello di membro.
- Problema: il runbook Config.1 non funziona perché il registratore o il canale di distribuzione esistono già.

  Risoluzione: ispeziona attentamente le impostazioni di AWS Config per assicurarti che Config sia configurato correttamente. In alcuni casi, la riparazione automatica non è in grado di correggere le impostazioni AWS Config esistenti.
- Problema: la riparazione ha esito positivo ma restituisce il messaggio `"No output available yet because the step is not successfully executed."`

Risoluzione: si tratta di un problema noto in questa versione a causa del quale alcuni runbook di correzione non restituiscono una risposta. I runbook di correzione falliranno correttamente e segnaleranno la soluzione se non funzionano.

- Problema: la risoluzione non è riuscita e ha inviato una traccia dello stack.

  Risoluzione: a volte perdiamo l'opportunità di gestire una condizione di errore che genera una traccia dello stack anziché un messaggio di errore. Tentativo di risolvere il problema utilizzando i dati di traccia. Apri un ticket di supporto se hai bisogno di assistenza.

- Problema: la rimozione dello stack v1.3.0 non è riuscita sulla risorsa Custom Action.

  Risoluzione: la rimozione del modello di amministrazione potrebbe non riuscire a seguito della rimozione dell'azione personalizzata. Si tratta di un problema noto che verrà risolto nella prossima versione. Se ciò si verifica:

  a. Accedi alla console di gestione AWS Security Hub.
  b. Nell'account amministratore, vai a Impostazioni.
  c. Seleziona la scheda Azioni personalizzate
  d. Eliminare manualmente la voce Remediate with ASR.
  e. Elimina nuovamente lo stack.

- Problema: dopo aver ridistribuito lo stack di amministrazione, la funzione Step non funziona. `AssumeRole`

  Soluzione: la ridistribuzione dello stack di amministrazione interrompe la connessione di fiducia tra il ruolo di amministratore nell'account amministratore e il ruolo di membro negli account dei membri. È necessario ridistribuire lo stack dei ruoli dei membri in tutti gli account dei membri.

- Problema: le riparazioni di CIS 3.x non vengono visualizzate `PASSED` dopo più di 24 ore.

  Soluzione: si tratta di un evento comune se non si dispone di abbonamenti all'argomento `S00111-ASR_LocalAlarmNotification` SNS nell'account del membro.

Problemi relativi a correzioni specifiche

Set SSLBucket Policy fallisce con AccessDenied errore

Controlli associati: AWS FSBP v1.0.0 S3.5, PCI v3.2.1 PCI.S3.5, CIS v1.4.0 2.1.2, SC v2.0.0 S3.5

SSLBucketProblema: la Set AccessDenied Policy fallisce con un errore:

Si è verificato un errore (AccessDenied) durante la chiamata all' PutBucketPolicy operazione: Accesso negato

Se l'impostazione Block Public Access è stata abilitata per un bucket, i tentativi di inserire una policy bucket che includa istruzioni che consentono l'accesso pubblico falliscono con questo errore. Questo stato può essere raggiunto inserendo una policy bucket che contenga tali istruzioni e quindi abilitando il blocco dell'accesso pubblico per quel bucket.

La correzione ConfigureS3 BucketPublicAccessBlock (controlli associati: AWS FSBP v1.0.0 S3.2, PCI v3.2.1 PCI.S3.2, CIS v1.4.0 2.1.5.2, SC v2.0.0 S3.2) può anche mettere un bucket in questo stato perché imposta l'impostazione del blocco di accesso pubblico senza modificare la politica del bucket.

La Set SSLBucket Policy aggiunge una dichiarazione alla policy bucket per rifiutare le richieste che non utilizzano SSL. Non modifica le altre istruzioni della policy, quindi se ci sono istruzioni che consentono l'accesso pubblico, la correzione fallirà nel tentativo di inserire la policy bucket modificata che include ancora tali istruzioni.

Risoluzione: modifica la policy del bucket per rimuovere le dichiarazioni che consentono l'accesso pubblico in conflitto con l'impostazione di blocco dell'accesso pubblico nel bucket.

PutS3 fallisce BucketPolicyDeny

Controlli associati: AWS FSBP v1.0.0 S3.6, (1), NIST.800-53.r5 CM-2 NIST.800-53.r5 CA-9

Problema: il BucketPolicyDeny PUTs3 con il seguente errore:

```
Unable to create an explicit deny statement for {bucket_name}.
```

Se i principi per tutte le politiche nel bucket di destinazione sono «*», la soluzione non può aggiungere la politica di negazione al bucket di destinazione poiché bloccherebbe tutte le azioni del bucket per tutti i principali.

Risoluzione: modifica la policy del bucket per consentire azioni a account specifici anziché utilizzare i principi «*» e limita le azioni negate.

Come disattivare la soluzione

In caso di incidente, potrebbe essere necessario disabilitare la soluzione senza rimuovere alcuna infrastruttura. Questi scenari descrivono in dettaglio come disabilitare diversi componenti della soluzione.

Scenario 1: disabilita la riparazione automatica per un singolo controllo.

1. EventBridge Accedi alla CloudFormation console AWS.
2. Seleziona Regole nella barra laterale.
3. Seleziona il bus degli eventi predefinito e cerca il controllo che desideri disabilitare.
4. Seleziona la regola e seleziona il pulsante Disabilita.

Scenario 2: disabilita la riparazione automatica per tutti i controlli.

1. Accedere EventBridge alla console.
2. Seleziona Regole nella barra laterale.
3. Seleziona il bus degli eventi «predefinito» e seleziona tutte le regole di seguito.
4. Seleziona il pulsante «Disabilita». Tieni presente che potresti dover eseguire questa operazione per più pagine di regole.

Scenario 3: disabilita la riparazione manuale per un account

1. Vai a EventBridge nella console.
2. Seleziona Regole nella barra laterale.
3. Seleziona il bus degli eventi «predefinito» e cerca «CustomActionRemediate_with_ASR_»
4. Seleziona la regola e seleziona il pulsante «Disabilita».

Contattare Support.

Se disponi di AWS Developer Support, AWS Business Support o AWS Enterprise Support, puoi utilizzare il Support Center per ottenere l'assistenza di esperti su questa soluzione. Le istruzioni per eseguire tali operazioni sono fornite nelle sezioni seguenti.

Crea un caso

1. Accedi al Support Center.
2. Scegli Crea caso.

Come possiamo aiutarti?

1. Scegli Tecnico.
2. Per Assistenza, seleziona Soluzioni.
3. Per Categoria, seleziona Altre soluzioni.
4. Per Severità, seleziona l'opzione più adatta al tuo caso d'uso.
5. Quando si inseriscono i campi Servizio, Categoria e Severità, l'interfaccia compila i collegamenti alle domande più comuni per la risoluzione dei problemi. Se non riesci a risolvere la tua domanda con questi link, scegli Passaggio successivo: Informazioni aggiuntive.

Informazioni aggiuntive

1. In Oggetto, inserisci il testo che riassume la domanda o il problema.
2. Per Descrizione, descrivi il problema in dettaglio.
3. Scegli Allega file.
4. Allega le informazioni necessarie a Support per elaborare la richiesta.

Aiutaci a risolvere il tuo caso più velocemente

1. Inserisci le informazioni richieste.
2. Scegli Passaggio successivo: risolvi ora o contattaci.

Risolvi subito o contattaci

1. Rivedi le soluzioni Solve now.
2. Se non riesci a risolvere il problema con queste soluzioni, scegli Contattaci, inserisci le informazioni richieste e scegli Invia.

Disinstalla la soluzione

Utilizza la seguente procedura per disinstallare la soluzione con la Console di gestione AWS.

V1.0.0-V1.2.1

Per le versioni da v1.0.0 a v1.2.1, utilizzare Service Catalog per disinstallare i playbook CIS FSBP. and/or Con la v1.3.0 Service Catalog non viene più utilizzato.

1. Accedi alla CloudFormation console AWS e accedi all'account primario di Security Hub.
2. Scegli Service Catalog per chiudere tutti i playbook forniti, rimuovere gruppi, ruoli o utenti di sicurezza.
3. Rimuovi il `CISPermissions.template` modello spoke dagli account dei membri del Security Hub.
4. Rimuovi il `AFSBPMemberStack.template` modello spoke dagli account amministratore e membro di Security Hub.
5. Passa all'account principale di Security Hub, seleziona lo stack di installazione della soluzione, quindi scegli Elimina.

> **Note**
>
> CloudWatch Registri I registri di gruppo vengono conservati. Si consiglia di conservare questi registri come richiesto dalla politica di conservazione dei log dell'organizzazione.

V1.3.x

1. Rimuovi il `automated-security-response-member.template` da ogni account membro.
2. Rimuovi il `automated-security-response-admin.template` dall'account amministratore.

> **Note**
>
> La rimozione del modello di amministrazione nella v1.3.0 probabilmente fallirà con la rimozione dell'azione personalizzata. Si tratta di un problema noto che verrà risolto nella prossima versione. Utilizza le seguenti istruzioni per risolvere il problema:

1. Accedi alla console di gestione AWS Security Hub.
2. Nell'account amministratore, vai a Impostazioni.
3. Seleziona la scheda Azioni personalizzate.
4. Eliminare manualmente la voce Remediate with ASR.
5. Elimina nuovamente lo stack.

V1.4.0 e versioni successive

Implementazione dello stack

1. Rimuovi il `automated-security-response-member.template` da ogni account membro.
2. Rimuovi il `automated-security-response-admin.template` dall'account amministratore.

StackSet distribuzione

Per ciascuna di esse StackSet, rimuovi le pile, quindi rimuovile StackSet nell'ordine inverso rispetto alla distribuzione.

Tieni presente che i ruoli IAM di `automated-security-response-member-roles.template` vengono mantenuti anche se il modello viene rimosso. In questo modo le riparazioni che utilizzano questi ruoli continueranno a funzionare. Questi ruoli SO0111-* possono essere rimossi manualmente dopo aver verificato che non siano più utilizzati mediante correzioni attive, ad esempio alla registrazione o CloudTrail al CloudWatch monitoraggio avanzato RDS.

Guida per gli amministratori

Abilitazione e disabilitazione di parti della soluzione

In qualità di amministratore della soluzione, hai i seguenti controlli su quali funzionalità della soluzione sono abilitate.

Dove vengono distribuiti gli stack dei membri e dei ruoli dei membri:

- Lo stack di amministrazione sarà in grado di avviare correzioni (tramite azioni personalizzate o EventBridge regole completamente automatizzate) solo negli account in cui gli stack di ruoli dei membri e dei membri sono stati distribuiti con il numero di account amministratore fornito come valore del parametro.
- Per esonerare completamente gli account o le regioni dal controllo della soluzione, non distribuite gli stack di ruoli dei membri o dei membri su tali account o regioni.

Configurazione dell'aggregazione di ricerca dell'account e della regione in Security Hub:

- Lo stack di amministrazione sarà in grado di avviare correzioni (tramite azioni personalizzate o EventBridge regole completamente automatizzate) solo per i risultati che arrivano nell'account di amministrazione e nella regione.
- Per esonerare completamente gli account o le regioni dal controllo della soluzione, non includere tali account o regioni per inviare i risultati allo stesso account amministratore e alla stessa regione in cui è distribuito lo stack di amministrazione.

Quali stack annidati standard vengono implementati:

- Lo stack di amministrazione sarà in grado di avviare correzioni (tramite azioni personalizzate o EventBridge regole completamente automatizzate) solo per i controlli che hanno un runbook di controllo distribuito nell'account membro e nella regione di destinazione. Questi vengono implementati dallo stack di membri per ogni standard.
- Lo stack di amministrazione sarà in grado di avviare riparazioni completamente automatizzate solo utilizzando EventBridge regole per i controlli che hanno le regole implementate dallo stack di amministrazione per quello standard. Queste vengono distribuite all'account amministratore.
- Per semplicità, ti consigliamo di implementare gli standard in modo coerente tra gli account amministratore e membro. Se ti interessano AWS FSBP e CIS v1.2.0, distribuisci questi due stack

di amministrazione annidati sull'account amministratore e distribuisci questi due stack di membri nidificati su ciascun account membro e regione.

Quali runbook di controllo vengono distribuiti in ogni stack di membri annidato:

- Lo stack di amministrazione sarà in grado di avviare correzioni (tramite azioni personalizzate o EventBridge regole completamente automatizzate) solo per i controlli che hanno un runbook di controllo distribuito nell'account membro e nella regione di destinazione dallo stack membro per ogni standard.
- Per esercitare un controllo più preciso sui controlli abilitati per un particolare standard, ogni stack annidato per uno standard contiene parametri per i quali vengono distribuiti i control runbook. Imposta il parametro per un controllo sul valore «NOT Available» per annullare la distribuzione del runbook di controllo.

Parametri SSM per abilitare e disabilitare gli standard:

- Lo stack di amministrazione sarà in grado di avviare riparazioni (tramite azioni personalizzate o EventBridge regole completamente automatizzate) solo per gli standard abilitati tramite il parametro SSM distribuito dallo stack di amministrazione standard.
- <standard_name><standard_version>Per disabilitare uno standard, imposta il valore del parametro SSM con il percorso «/Solutions/SO0111///status" su «No».

Esempio di notifiche SNS

Quando viene avviata una riparazione

```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation queued for SC control
 RDS.13 in account 111111111111",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
```

```
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Quando una riparazione ha esito positivo

```
{
 "severity": "INFO",
 "message": "00000000-0000-0000-0000-000000000000: Remediation succeeded for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Quando una riparazione fallisce

```
{
 "severity": "ERROR",
 "message": "00000000-0000-0000-0000-000000000000: Remediation failed for SC
 control RDS.13 in account 111111111111: See Automation Execution output for details
 (AwsRdsDbInstance arn:aws:rds:us-east-1:111111111111:db:database-1)",
 "finding": {
 "finding_id": "22222222-2222-2222-2222-222222222222",
 "finding_description": "This control checks if automatic minor version upgrades are
 enabled for the Amazon RDS database instance.",
 "standard_name": "security-control",
 "standard_version": "2.0.0",
 "standard_control": "RDS.13",
```

```
 "title": "RDS automatic minor version upgrades should be enabled",
 "region": "us-east-1",
 "account": "111111111111",
 "finding_arn": "arn:aws:securityhub:us-east-1:111111111111:security-control/RDS.13/
finding/22222222-2222-2222-2222-222222222222"
 }
}
```

Usa la soluzione

Questo è un tutorial che ti guiderà nella prima implementazione di ASR. Inizierà con i prerequisiti per l'implementazione della soluzione e terminerà con la correzione di esempi trovati in un account membro.

Tutorial: Guida introduttiva a Automated Security Response su AWS

Questo è un tutorial che ti guiderà nella prima implementazione. Inizierà con i prerequisiti per l'implementazione della soluzione e terminerà con la correzione degli esempi trovati in un account membro.

Prepara i conti

Per dimostrare le funzionalità di riparazione tra account e aree geografiche della soluzione, questo tutorial utilizzerà due account. Puoi anche distribuire la soluzione su un singolo account.

Negli esempi seguenti vengono utilizzati gli account `111111111111` e `222222222222` viene illustrata la soluzione. `111111111111`sarà l'account amministratore e `222222222222` sarà l'account membro. Definiremo la soluzione per correggere i problemi relativi alle risorse nelle Regioni `us-east-1` e`us-west-2`.

La tabella seguente è un esempio per illustrare le azioni che intraprenderemo per ogni fase in ciascun account e regione.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
`111111111111`	Admin	Nessuno	Nessuno
`222222222222`	Membro	Nessuno	Nessuno

L'account amministratore è l'account che eseguirà le azioni amministrative della soluzione, ovvero l'avvio manuale delle riparazioni o l'abilitazione della riparazione completamente automatizzata con regole. EventBridge Questo account deve anche essere l'account amministratore delegato di Security

Hub per tutti gli account in cui desideri correggere i risultati, ma non è necessario né deve essere l'account amministratore di AWS Organizations per l'organizzazione AWS a cui appartengono i tuoi account.

Abilitazione di AWS Config

Consulta la seguente documentazione:

- Documentazione AWS Config
- Prezzi di AWS Config
- Abilitazione di AWS Config

Abilita AWS Config in entrambi gli account e in entrambe le regioni. Ciò comporterà dei costi.

> **Important**
>
> Assicurati di selezionare l'opzione «Includi risorse globali (ad esempio, risorse AWS IAM)». Se non selezioni questa opzione quando abiliti AWS Config, non vedrai i risultati relativi alle risorse globali (ad esempio le risorse AWS IAM)

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Abilitazione di AWS Config	Abilitazione di AWS Config
222222222222	Membro	Abilitazione di AWS Config	Abilitazione di AWS Config

Abilita l'hub di sicurezza AWS

Consulta la seguente documentazione:

- Documentazione di AWS Security Hub
- Prezzi di AWS Security Hub
- Abilitazione di AWS Security Hub

Abilita AWS Security Hub in entrambi gli account e in entrambe le regioni. Ciò comporterà dei costi.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
`111111111111`	Admin	Abilita AWS Security Hub	Abilita AWS Security Hub
`222222222222`	Membro	Abilita AWS Security Hub	Abilita AWS Security Hub

Abilita risultati di controllo consolidati

Consulta la seguente documentazione:

- Generazione e aggiornamento dei risultati del controllo

Ai fini di questo tutorial, dimostreremo l'utilizzo della soluzione con la funzionalità di controllo consolidato dei risultati di controllo di AWS Security Hub abilitata, che è la configurazione consigliata. Nelle partizioni che non supportano questa funzionalità al momento della scrittura, sarà necessario distribuire i playbook specifici dello standard anziché SC (Security Control).

Abilita risultati di controllo consolidati in entrambi gli account e in entrambe le regioni.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
`111111111111`	Admin	Abilita risultati di controllo consolidati	Abilita risultati di controllo consolidati
`222222222222`	Membro	Abilita risultati di controllo consolidati	Abilita risultati di controllo consolidati

La generazione dei risultati con la nuova funzionalità potrebbe richiedere del tempo. Puoi procedere con il tutorial, ma non potrai correggere i risultati generati senza la nuova funzionalità. I risultati generati con la nuova funzionalità possono essere identificati dal valore `security-control/<control_id>` del `GeneratorId` campo.

Configura l'aggregazione dei risultati tra regioni

Consulta la seguente documentazione:

- Aggregazione tra regioni
- Abilitazione dell'aggregazione tra regioni

Configura l'aggregazione dei risultati da us-west-2 a us-east-1 in entrambi gli account.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Configurare l'aggregazione da us-west-2	Nessuno
222222222222	Membro	Configurare l'aggregazione da us-west-2	Nessuno

La propagazione dei risultati nella regione di aggregazione potrebbe richiedere del tempo. Puoi procedere con il tutorial, ma non potrai correggere i risultati di altre regioni finché non inizieranno a comparire nella regione di aggregazione.

Designare un account amministratore del Security Hub

Consulta la seguente documentazione:

- Gestione degli account in AWS Security Hub
- Gestione degli account dei membri dell'organizzazione
- Gestione degli account dei membri tramite invito

Nell'esempio seguente, utilizzeremo il metodo di invito manuale. Per un set di account di produzione, consigliamo di gestire l'amministrazione delegata di Security Hub tramite AWS Organizations.

Dalla console AWS Security Hub nell'account amministratore (111111111111), invita l'account membro (222222222222) ad accettare l'account amministratore come amministratore delegato di Security Hub. Dall'account membro, accetta l'invito.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Invita l'account del membro	Nessuno
222222222222	Membro	Accetta l'invito	Nessuno

La propagazione dei risultati all'account amministratore potrebbe richiedere del tempo. Puoi procedere con il tutorial, ma non potrai correggere i risultati degli account dei membri finché non inizieranno a comparire nell'account amministratore.

Crea i ruoli per le autorizzazioni StackSets autogestite

Consulta la seguente documentazione:

- AWS CloudFormation StackSets
- Concedi autorizzazioni autogestite

Distribuiremo gli CloudFormation stack su più account, quindi li useremo. StackSets Non possiamo utilizzare le autorizzazioni gestite dal servizio perché lo stack di amministrazione e lo stack dei membri hanno stack annidati, che non sono supportati dal servizio, quindi dobbiamo utilizzare autorizzazioni autogestite.

Distribuisci gli stack per le autorizzazioni di base per le operazioni. StackSet Per gli account di produzione, potresti voler restringere le autorizzazioni in base alla documentazione sulle «opzioni di autorizzazione avanzate».

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Implementa lo stack di ruoli di amministratore StackSet Distribuisci lo stack di ruoli di esecuzione StackSet	Nessuno

Account	Scopo	Azione in us-east-1	Azione in us-west-2
222222222222	Membro	Implementa lo stack di ruoli di esecuzione StackSet	Nessuno

Crea le risorse non sicure che genereranno risultati di esempio

Consulta la seguente documentazione:

- Riferimento ai controlli del Security Hub
- Controlli AWS Lambda

Il seguente esempio di risorsa con una configurazione non sicura per dimostrare una correzione. Il controllo di esempio è Lambda.1: le politiche delle funzioni Lambda dovrebbero vietare l'accesso pubblico.

> **Important**
>
> Creeremo intenzionalmente una risorsa con una configurazione non sicura. Esamina la natura del controllo e valuta personalmente il rischio di creare una risorsa di questo tipo nel tuo ambiente. Siate consapevoli degli strumenti a disposizione della vostra organizzazione per rilevare e segnalare tali risorse e richiedete un'eccezione, se del caso. Se il controllo di esempio che abbiamo selezionato non è appropriato per te, seleziona un altro controllo supportato dalla soluzione.

Nella seconda regione dell'account membro, accedi alla console AWS Lambda e crea una funzione nell'ultimo runtime di Python. In Configurazione → Autorizzazioni, aggiungi una dichiarazione politica per consentire di richiamare la funzione dall'URL senza autenticazione.

Conferma nella pagina della console che la funzione consenta l'accesso pubblico. Dopo che la soluzione ha risolto il problema, confronta le autorizzazioni per confermare che l'accesso pubblico è stato revocato.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Nessuno	Nessuno
222222222222	Membro	Nessuno	Creare una funzione Lambda con una configurazione non sicura

AWS Config potrebbe impiegare del tempo per rilevare la configurazione non sicura. Puoi procedere con il tutorial, ma non sarai in grado di correggere il risultato finché Config non lo rileverà.

Crea gruppi di CloudWatch log per i controlli correlati

Consulta la seguente documentazione:

- Monitoraggio dei file di CloudTrail registro con Amazon CloudWatch Logs
- CloudTrail controlli

Vari CloudTrail controlli supportati dalla soluzione richiedono che sia presente un gruppo di CloudWatch log che sia la destinazione di una multiregione CloudTrail. Nell'esempio seguente, creeremo un gruppo di log segnaposto. Per gli account di produzione, è necessario configurare correttamente CloudTrail l'integrazione con CloudWatch Logs.

Crea un gruppo di log in ogni account e regione con lo stesso nome, ad esempio:`asr-log-group`.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Creazione di un gruppo di log	Creazione di un gruppo di log
222222222222	Membro	Creazione di un gruppo di log	Creazione di un gruppo di log

Implementa la soluzione negli account tutorial

Raccogli i tre Amazon S3 URLs per lo stack dei ruoli di amministratore, membro e membro.

Implementa lo stack di amministrazione

View template

automa

security-response-admin.modello

Nell'account amministratore, accedi alla CloudFormation console e distribuisci lo stack di amministrazione nella regione di aggregazione dei risultati di Security Hub.

Scegli No il valore di tutti i parametri per caricare gli stack di amministrazione annidati ad eccezione dello stack «SC» o «Security Control». Questo stack contiene le risorse per i risultati del controllo consolidato che abbiamo configurato nei nostri account.

Scegliete No di riutilizzare il gruppo di log di Orchestrator a meno che non abbiate già implementato questa soluzione in questo account e nella regione.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Implementa lo stack di amministrazione	Nessuno
222222222222	Membro	Nessuno	Nessuno

Attendi che lo stack di amministrazione completi la distribuzione prima di continuare in modo da poter creare una relazione di fiducia tra gli account membro e l'account amministratore.

Distribuisci lo stack dei membri

View template

automa

security-response-member.modello

Nell'account amministratore, accedi alla CloudFormation StackSets console e distribuisci lo stack di membri a ciascun account e regione. Usa i ruoli di StackSets amministratore ed esecuzione creati in questo tutorial.

Immettete il nome del gruppo di log che avete creato come valore per il parametro per il nome del gruppo di log.

Scegli No il valore di tutti i parametri per caricare gli stack di membri annidati ad eccezione dello stack «SC» o «security control». Questo stack contiene le risorse per i risultati del controllo consolidato che abbiamo configurato nei nostri account.

Inserisci l'ID dell'account amministratore come valore per il parametro per il numero dell'account amministratore. Nel nostro esempio, questo è`111111111111`.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
`111111111111`	Admin	Distribuisci il StackSet membro/Conferma lo stack di membri distribuito	Conferma lo stack di membri distribuito
`222222222222`	Membro	Conferma lo stack di membri distribuito	Conferma lo stack di membri distribuito

Implementa lo stack di ruoli dei membri

automated-security-response-memberpulsante modello -roles.template -roles.template automated-security-response-member

Nell'account amministratore, accedi alla CloudFormation StackSets console e distribuisci lo stack di membri su ciascun account. Usa i ruoli di StackSets amministratore ed esecuzione creati in questo tutorial. Inserisci l'ID dell'account amministratore come valore per il parametro per il numero dell'account amministratore. Nel nostro esempio, questo è`111111111111`.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
`111111111111`	Admin	Distribuisci il StackSet membro/Conferma lo stack di membri distribuito	Nessuno

Account	Scopo	Azione in us-east-1	Azione in us-west-2
222222222222	Membro	Conferma lo stack di membri distribuito	Nessuno

Puoi procedere, ma non potrai correggere i risultati fino CloudFormation StackSets al termine della distribuzione.

Iscriviti all'argomento SNS

Aggiornamenti di bonifica

Argomento - {https---us-east-1-console-aws-amazon-com-sns-v3- home-region-us-east -1— -US-East-1-221128147805-so0111-asr-argomento} [topic-arn-aws-snsSO0111-ASR_topic]

Nell'account amministratore, iscriviti all'argomento Amazon SNS creato dallo stack di amministrazione. Questo ti avviserà quando verranno avviate le riparazioni e quando avranno esito positivo o negativo.

Allarmi

Argomento - {https---us-east-1-console-aws-amazon-com-sns-v3- home-region-us-east -1— topic-arn-aws-sns -US-East-1-221128147805-so0111-asr-alarm-topic} [SO0111-Argomento_allarme]

Nell'account amministratore, iscriviti all'argomento Amazon SNS creato dallo stack di amministrazione. Questo ti avviserà quando inizieranno gli allarmi metrici.

Correggi i risultati degli esempi

Nell'account amministratore, accedi alla console Security Hub e individua il risultato della risorsa con una configurazione non sicura che hai creato come parte di questo tutorial.

Questa operazione può essere eseguita in diversi modi:

1. Nelle partizioni che supportano la funzionalità dei risultati dei controlli consolidati, una pagina denominata «Controlli» consente di individuare il risultato in base all'ID di controllo consolidato.
2. Nella pagina «Standard di sicurezza», è possibile individuare il controllo in base allo standard a cui appartiene.
3. Puoi visualizzare tutti i risultati nella pagina «Risultati» ed eseguire la ricerca per attributo.

L'ID di controllo consolidato per la funzione Lambda pubblica che abbiamo creato è Lambda.1.

Avvia la riparazione

Seleziona la casella di controllo a sinistra del risultato relativo alla risorsa che abbiamo creato. Nel menu a discesa «Azioni», seleziona «Ripara con ASR». Verrà visualizzata una notifica che indica che il risultato è stato inviato ad Amazon EventBridge.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Avviare la riparazione	Nessuno
222222222222	Membro	Nessuno	Nessuno

Conferma che la riparazione ha risolto il problema

Dovresti ricevere due notifiche SNS. La prima indicherà che è stata avviata una riparazione e la seconda indicherà che la riparazione è riuscita. Dopo aver ricevuto la seconda notifica, accedi alla console Lambda nell'account membro e conferma che l'accesso pubblico è stato revocato.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Nessuno	Nessuno
222222222222	Membro	Nessuno	Conferma che la riparazione è riuscita

Traccia l'esecuzione della riparazione

Per comprendere meglio come funziona la soluzione, è possibile tracciare l'esecuzione della riparazione.

EventBridge regola

Nell'account amministratore, individua una EventBridge regola denominata CustomActionRemediate_with_ASR_. Questa regola corrisponde al risultato inviato da Security Hub e lo invia a Orchestrator Step Functions.

Esecuzione di Step Functions

Nell'account amministratore, individua AWS Step Functions denominato "SO0111-ASR-Orchestrator». Questa funzione di fase richiama il documento SSM Automation nell'account e nella regione di destinazione. Puoi tracciare l'esecuzione della correzione nella cronologia di esecuzione di questo AWS Step Functions.

Automazione SSM

Nell'account membro, accedi alla console SSM Automation. Troverai due esecuzioni di un documento denominato «ASR-SC_2.0.0_Lambda.1" e un'esecuzione di un documento denominato «ASR-». RemoveLambdaPublicAccess

La prima esecuzione avviene dalla funzione orchestrator step nell'account di destinazione. La seconda esecuzione avviene nella regione di destinazione, che potrebbe non essere la regione da cui ha avuto origine il risultato. L'esecuzione finale è la correzione che revoca la politica di accesso pubblico alla funzione Lambda.

CloudWatch Gruppo di log

Nell'account amministratore, accedi alla console CloudWatch Logs e individua un gruppo di log denominato "SO0111-ASR». Questo gruppo di log è la destinazione dei log di alto livello di Orchestrator Step Functions.

Abilita riparazioni completamente automatizzate

L'altra modalità operativa della soluzione consiste nel correggere automaticamente i risultati non appena arrivano in Security Hub.

Conferma di non disporre di risorse a cui questo risultato potrebbe essere applicato accidentalmente

L'abilitazione delle riparazioni automatiche avvierà le riparazioni su tutte le risorse corrispondenti al controllo abilitato (Lambda.1).

> **Important**
>
> Conferma che desideri che questa autorizzazione venga revocata a tutte le funzioni Lambda pubbliche incluse nell'ambito della soluzione. Le riparazioni completamente automatizzate

non saranno limitate alla funzione che avete creato. La soluzione correggerà questo controllo se viene rilevato in uno qualsiasi degli account e delle regioni in cui è installato.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Conferma nessuna funzione pubblica desiderata	Conferma nessuna funzione pubblica desiderata
222222222222	Membro	Conferma nessuna funzione pubblica desiderata	Conferma nessuna funzione pubblica desiderata

Abilita la regola

Nell'account Admin, individua una EventBridge regola denominata AutoTriggerSC_2.0.0_Lambda.1_ e abilitala.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Abilita le regole di riparazione automatiz zate	Nessuno
222222222222	Membro	Nessuno	Nessuno

Configura la risorsa

Nell'account membro, riconfigura la funzione Lambda per consentire l'accesso pubblico.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Nessuno	Nessuno

Account	Scopo	Azione in us-east-1	Azione in us-west-2
222222222222	Membro	Nessuno	Configurare la funzione Lambda per consentire l'accesso pubblico

Conferma che la correzione ha risolto il problema

Config potrebbe impiegare del tempo per rilevare nuovamente la configurazione non sicura. Dovresti ricevere due notifiche SNS. La prima indicherà che è stata avviata una riparazione. Il secondo indicherà che la riparazione è riuscita. Dopo aver ricevuto la seconda notifica, accedi alla console Lambda nell'account membro e conferma che l'accesso pubblico è stato revocato.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Abilita le regole di riparazione automatiz zate	Nessuno
222222222222	Membro	Nessuno	Conferma che la riparazione è riuscita

Eliminazione

Eliminate le risorse di esempio

Nell'account membro, elimina la funzione Lambda di esempio che hai creato.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Nessuno	Nessuno
222222222222	Membro	Nessuno	Eliminare la funzione Lambda di esempio

Elimina lo stack di amministrazione

Nell'account amministratore, elimina lo stack di amministrazione.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Elimina lo stack di amministrazione	Nessuno
222222222222	Membro	Nessuno	Nessuno

Elimina lo stack di membri

Nell'account amministratore, elimina il membro StackSet.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Eliminare il membro StackSet Conferma l'elimina zione dello stack di membri	Conferma l'elimina zione dello stack di membri
222222222222	Membro	Conferma l'elimina zione dello stack di membri	Conferma l'elimina zione dello stack di membri

Elimina lo stack dei ruoli dei membri

Nell'account Amministratore, elimina i ruoli StackSet dei membri.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Eliminare i ruoli dei membri StackSet	Nessuno

Account	Scopo	Azione in us-east-1	Azione in us-west-2
		Conferma l'elimina zione dello stack di ruoli di ricordo	
222222222222	Membro	Conferma l'elimina zione dello stack di ruoli dei membri	Nessuno

Eliminare i ruoli mantenuti

In ogni account, elimina i ruoli IAM mantenuti.

Importante: questi ruoli vengono mantenuti per le riparazioni che richiedono un ruolo per continuare a funzionare (ad esempio la registrazione del flusso VPC). Verifica di non aver bisogno del funzionamento continuo di nessuno di questi ruoli prima di eliminarli.

Eliminare tutti i ruoli con il prefisso SO0111 -.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Eliminare i ruoli mantenuti	Nessuno
222222222222	Membro	Eliminare i ruoli mantenuti	Nessuno

Pianifica l'eliminazione delle chiavi KMS conservate

Gli stack di amministratori e membri creano e conservano una chiave KMS. Se conservi queste chiavi ti verranno addebitati dei costi.

Queste chiavi vengono conservate per consentire l'accesso a tutte le risorse crittografate dalla soluzione. Conferma di non averle necessarie prima di programmarne l'eliminazione.

Identifica le chiavi distribuite dalla soluzione utilizzando gli alias creati dalla soluzione o dalla cronologia. CloudFormation Pianificale per l'eliminazione.

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Identifica e pianifica l'eliminazione della chiave di amministr azione Identifica e pianifica l'eliminazione della chiave membro	Identifica e pianifica l'eliminazione della chiave membro
222222222222	Membro	Identifica e pianifica l'eliminazione della chiave membro	Identifica e pianifica l'eliminazione della chiave membro

Elimina gli stack per le autorizzazioni StackSets autogestite

Elimina gli stack creati per consentire le autorizzazioni autogestite StackSets

Account	Scopo	Azione in us-east-1	Azione in us-west-2
111111111111	Admin	Elimina lo stack di ruoli di StackSet amministratore	Nessuno
222222222222	Membro	Eliminare lo stack di ruoli di StackSet esecuzione	Nessuno

Guida per sviluppatori

Questa sezione fornisce il codice sorgente per la soluzione e personalizzazioni aggiuntive.

Codice sorgente

Visita il nostro GitHub repository per scaricare i modelli e gli script per questa soluzione e per condividere le tue personalizzazioni con altri.

Playbook

Questa soluzione include le soluzioni playbook per gli standard di sicurezza definiti come parte del Center for Internet Security (CIS) AWS Foundations Benchmark v1.2.0, CIS AWS Foundations Benchmark v1.4.0, CIS AWS Foundations Benchmark v3.0.0, AWS Foundational Security Best Practices (FSBP) v.1.0.0, Payment Card Industry Data Security Standard (PCI-DSS) v3.2.1 e National Institute of Standards e tecnologia (NIST).

Se hai abilitato i risultati dei controlli consolidati, tali controlli sono supportati in tutti gli standard. Se questa funzionalità è abilitata, è necessario implementare solo il playbook SC. In caso contrario, i playbook sono supportati per gli standard elencati in precedenza.

> **Important**
>
> Implementa i playbook solo per gli standard abilitati per evitare di raggiungere le quote di servizio.

Per i dettagli su una soluzione specifica, consulta il documento di automazione Systems Manager con il nome distribuito dalla soluzione nel tuo account. Vai alla console AWS Systems Manager, quindi nel pannello di navigazione scegli Documenti.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Rimediazioni totali	63	34	29	33	65	19	90
ASR-VerificaEnableAutoScalingGroupELBHealth I gruppi di Auto Scaling associati a un sistema di bilanciamento del carico devono utilizzare i controlli dello stato del sistema di bilanciamento del carico	Scalabilità automatica.1		Scalabilità automatica.1		Scalabilità automatica.1		Scalabilità automatica.1

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-ConfigureAutoScalingLaunchConfigToRequireIMDSv2 Le configurazioni di avvio del gruppo Auto Scaling devono configurare le EC2 istanze in modo da richiedere Instance Metadata Service versione 2 () IMDSv2					Scalabilità automatica.3		Scalabilità automatica.3

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateCloudTrailMultiRegionTrail CloudTrail deve essere attivato e configurato con almeno un percorso multiregionale	CloudTrail1.	2.1	CloudTrail2.	3.1	CloudTrail1.	3.1	CloudTrail1.
ASR-EnableEncryption CloudTrail dovrebbe avere la crittografia a riposo attivata	CloudTrail2.	2.7	CloudTrail1.	3.7	CloudTrail2.	3.5	CloudTrail2.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-EnableLogFileValidation Assicurati che la convalida dei file di CloudTrail registro sia attivata	CloudTrail4.	2.2	CloudTrail3.	3.2	CloudTrail4.		CloudTrail4.
ASR-EnableCloudTrailToCloudWatchLogging Assicurati che i CloudTrail percorsi siano integrati con Amazon CloudWatch Logs	CloudTrail5.	2.4	CloudTrail4.	3.4	CloudTrail5.		CloudTrail5.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR configura S3 BucketLogging Assicurati che la registrazione degli accessi al bucket S3 sia abilitata sul bucket S3 CloudTrail		2.6		3.6		3.4	CloudTrail7.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
A.S.R. ReplaceCodeBuildClearTextCredentials CodeBuild le variabili di ambiente del progetto non devono contenere credenziali di testo non crittografato	CodeBuild 2.		CodeBuild 2.		CodeBuild 2.		CodeBuild 2.
Attivazione ASR AWSConfig Assicurati che AWS Config sia attivato	Config.1	2.5	Config.1	3.5	Config.1	3.3	Config.1

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
EBSSnapshotsASR-Make Private Le istantanee di Amazon EBS non devono essere ripristinabili pubblicamente	EC21.		EC21.		EC21.		EC21.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR - Rimuovi VPCDefault SecurityGroupRules Il gruppo di sicurezza predefinito VPC dovrebbe vietare il traffico in entrata e in uscita	EC22.	4.3	EC22.	5.3	EC22.	5.4	EC22.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Registri di abilitazione ASR VPCFlow La registrazione del flusso VPC deve essere abilitata in tutti VPCs	EC26.	2.9	EC26.	3.9	EC26.	3.7	EC26.
A.S.R. EnableEbsEncryptionByDefault La crittografia predefinita di EBS deve essere attivata	EC27.	2.2.1			EC27.	2.2.1	EC27.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
A.S.R. RevokeUnrotatedKeys Le chiavi di accesso degli utenti devono essere ruotate ogni 90 giorni o meno	IAM.3	1.4		1.14	IAM.3	1.14	IAM.3
Politica ASR-Set IAMPassword Politica di password predefinita IAM	IAM.7	1.5-1,11	IAM.8	1.8	IAM.7	1.8	IAM.7

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Credenziali ASR-RevokeUnused IAMUser Le credenziali utente devono essere disattivate se non utilizzate entro 90 giorni	IAM.8	1.3	IAM.7		IAM.8		IAM.8

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Credenziali ASR-RevokeUnused IAMUser Le credenziali utente devono essere disattivate se non utilizzate entro 45 giorni				1.12		1.12	IO HO 22 ANNI
ASR-RemoveLambdaPublicAccess Le funzioni Lambda dovrebbero vietare l'accesso pubblico	Lambda.1		Lambda.1		Lambda.1		Lambda.1

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-Make Private RDSSnapshot Le istantanee RDS dovrebbero vietare l'accesso pubblico	RDS.1		RDS.1		RDS.1		RDS.1
ASR-DisablePublicAccessTo RDSInstance Le istanze DB RDS dovrebbero vietare l'accesso pubblico	RDS.2		RDS.2		RDS.2	2.3.3	RDS.2

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Crittografia ASR RDSSnapshot Le istantanee del cluster RDS e le istantanee del database devono essere crittografate quando sono inattive	RDS.4				RDS.4		RDS.4

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-EnableMulti AZOn RDSInstance Le istanze DB RDS devono essere configurate con più zone di disponibilità	RDS.5				RDS.5		RDS.5

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-EnableEnhancedMonitoringOnRDSInstance È necessario configurare un monitoraggio avanzato per le istanze e i cluster DB RDS	RDS.6				RDS.6		RDS.6

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Abilita ASR RDSCluster DeletionProtection Nei cluster RDS dovrebbe essere attivata la protezione da eliminazione	RDS.7				RDS.7		RDS.7

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Abilitazione ASR RDSInstance DeletionProtection Le istanze DB RDS devono avere la protezione da eliminazione attivata	RDS.8				RDS.8		RDS.8

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-EnableMinorVersionUpgradeOnRDSDBInstance Gli aggiornamenti automatici delle versioni secondarie di RDS devono essere attivati	RDS.13				RDS.13	2.3.2	RDS.13

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-EnableCopyTagsToSnapshotOnRDSCluster I cluster RDS DB devono essere configurati per copiare i tag nelle istantanee	RDS.16				RDS.16		RDS.16
ASR-DisablePublicAccessToRedshiftCluster I cluster Amazon Redshift dovrebbero vietare l'accesso pubblico	Redshift.1		Redshift.1		Redshift.1		Redshift.1

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-EnableAutomaticSnapshotsOnRedshiftCluster I cluster Amazon Redshift devono avere snapshot automatici attivati	Redshift.3				Redshift.3		Redshift.3
ASR-EnableRedshiftClusterAuditLogging I cluster Amazon Redshift devono avere la registrazione di controllo attivata	Redshift.4				Redshift.4		Redshift.4

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-EnableAutomaticVersionUpgradeOnRedshiftCluster Amazon Redshift dovrebbe avere gli upgrade automatici alle versioni principali attivati	Redshift.6				Redshift.6		Redshift.6
ASR configura S3 PublicAccessBlock L'impostazione S3 Block Public Access deve essere attivata	S3.1	2.3	S3.6	2.1.5.1	S3.1	2.1.4	S3.1

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR configura S3 BucketPublicAccessBlock I bucket S3 dovrebbero vietare l'accesso pubblico in lettura	S3.2		S3.2	2.1.5.2	S3.2		S3.2
ASR configura S3 BucketPublicAccessBlock I bucket S3 dovrebbero vietare l'accesso pubblico in scrittura		S3.3					S3.3

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-S3 EnableDefaultEncryption I bucket S3 devono avere la crittografia lato server attivata	S3.4		S3.4	2.1.1	S3.4		S3.4
SSLBucketPolicyASR-Set I bucket S3 dovrebbero richiedere richieste di utilizzo del protocollo SSL	S3.5		S3.5	2.1.2	S3.5	2.1.1	S3.5

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-S3 BlockDenylist Le autorizzazioni di Amazon S3 concesse ad altri account AWS nell'ambito delle policy bucket devono essere limitate	S3.6				S3.6		S3.6
L'impostazione S3 Block Public Access deve essere attivata a livello di bucket	S3.8				S3.8		S3.8

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR configura S3 BucketPublicAccessBlock Assicurati che i log del CloudTrail bucket S3 non siano accessibili pubblicamente		2.3					CloudTrail6.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
A.S.R. CreateAccessLoggingBucket Assicurati che la registrazione degli accessi al bucket S3 sia attivata sul bucket S3 CloudTrail		2.6					CloudTrail7.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
A.S.R. EnableKeyRotation Assicurati che la rotazione per quella creata dal cliente CMKs sia attivata		2.8	KMS.1	3.8	KMS.4	3.6	KMS.4

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle chiamate API non autorizzate		3.1		4.1			Cloudwatch 1

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di log e un allarme per l'accesso alla Console di gestione AWS senza MFA		3.2		4.2			Cloudwatch.2

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di registro e un allarme per l'utilizzo da parte dell'utente «root»		3.3	CW.1	4.3			Cloudwatch 3

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle policy IAM		3.4		4.4			Cloudwatch 4

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di registro e un allarme per le CloudTrail modifiche alla configurazione		3.5		4.5			Cloudwatch 5

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di log e un allarme per gli errori di autenticazione della Console di gestione AWS		3.6		4.6			Cloudwatch 6

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di registro e un allarme per la disabilitazione o la cancellazione programmata dei dati creati dal cliente CMKs		3.7		4.7			Cloudwatch 7

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle policy dei bucket S3		3.8		4.8			Cloudwatch 8

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Assicurati che esistano un filtro metrico di log e un allarme per le modifiche alla configurazione di AWS Config		3.9		4.9			Cloudwatch.9

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate al gruppo di sicurezza		3.10		4,10			Cloudwatch.10

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle liste di controllo degli accessi alla rete (NACL)		3.11		4,11			Cloudwatch.11

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate ai gateway di rete		3.12		4,12			Cloudwatch.12

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate alle tabelle di routing		3.13		4.13			Cloudwatch.13

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-CreateLogMetricFilterAndAlarm Verifica se esistono un filtro e un allarme per le metriche dei log relativamente alle modifiche apportate al VPC		3.14		4,14			Cloudwatch 14

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
AWS-DisablePublicAccessForSecurityGroup Assicurati che nessun gruppo di sicurezza consenta l'ingresso dalla porta 0.0.0.0/0 alla porta 22		4.1	EC25.		EC21.3		EC2.13

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
AWS-DisablePublicAccessForSecurityGroup Assicurati che nessun gruppo di sicurezza consenta l'ingresso dalla porta 0.0.0.0/0 alla porta 3389		4.2			EC21.4		EC2.14
Configurazione ASR SNSTopicForStack	CloudFormation1.				CloudFormation1.		CloudFormation1.
Ruolo ASR-CreateIAMSupport		1.20		1,17		1,17	IAM.18

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-AssegnaDisablePublicIPAuto Le EC2 sottoreti Amazon non devono assegnare automaticamente indirizzi IP pubblici	EC21.5				EC2.15		EC2.15
A.S.R. EnableCloudTrailLogFileValidation	CloudTrail4.	2.2	CloudTrail3.	3.2			CloudTrail4.
ASR-EnableEncryptionFor SNSTopic	SNS.1				SNS.1		SNS.1

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-EnableDeliveryStatusLoggingFor SNSTopic La registrazione dello stato di consegna deve essere abilitata per i messaggi di notifica inviati a un argomento	SNS.2				SNS.2		SNS.2
ASR-EnableEncryptionFor SQSQueue	SQS.1				SQS.1		SQS.1

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
L'istantanea ASR-Make RDSSnapshot Private RDS deve essere privata	RDS.1		RDS.1				RDS.1
Blocco ASR SSMDocument PublicAccess I documenti SSM non devono essere pubblici	SSM.4				SSM.4		SSM.4

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-EnableCloudFrontDefaultRootObject CloudFront le distribuzioni dovrebbero avere un oggetto root predefinito configurato	CloudFront1.				CloudFront1.		CloudFront1.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-SetCloudFrontOriginDomain CloudFront le distribuzioni non devono puntare a origini S3 inesistenti	CloudFront1.2				CloudFront.12		CloudFront.12

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
A.S.R. RemoveCodeBuildPrivilegedMode CodeBuild gli ambienti di progetto dovrebbero avere una configurazione AWS di registrazione	CodeBuild 5.				CodeBuild 5.		CodeBuild 5.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Istanza EC2 ASR-terminate EC2 Le istanze interrotte devono essere rimosse dopo un periodo di tempo specificato	EC24.				EC24.		EC24.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Attivazione ASR IMDSV2 OnInstance EC2 le istanze devono utilizzare Instance Metadata Service Version 2 () IMDSv2	EC28.				EC28.	5.6	EC28.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
A.S.R. RevokeUnauthorized InboudRules I gruppi di sicurezza dovrebbero consentire il traffico in entrata senza restrizioni solo per le porte autorizzate	EC21.8				EC2.18		EC2.18

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
INSERISCI QUI IL TITOLO I gruppi di sicurezza non dovrebbero consentire l'accesso illimitato alle porte ad alto rischio	EC21.9				EC2.19		EC2.19

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Disabilita ASR TGWAutoAcceptSharedAttachments Amazon EC2 Transit Gateways non dovrebbe accettare automaticamente le richieste di allegati VPC	EC22.3				EC2.23		EC2.23

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
A.S.R. EnablePrivateRepositoryScanning Gli archivi privati ECR devono avere la scansione delle immagini configurata	ECR.1				ECR.1		ECR.1
ASR-EnableGuardDuty GuardDuty dovrebbe essere abilitato	GuardDuty 1.		GuardDuty 1.		GuardDuty 1.		GuardDuty 1.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR configura S3 BucketLogging La registrazione degli accessi al server bucket S3 deve essere abilitata	S3.9				S3.9		S3.9
ASR-EnableBucketEventNotifications I bucket S3 devono avere le notifiche degli eventi abilitate	S3.11				S3.11		S3.11

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Set ASR 3 Lifecycle Policy I bucket S3 devono avere politiche del ciclo di vita configurate	S3.13				S3.13		S3.13
ASR-EnableAutoSecretRotation I segreti di Secrets Manager devono avere la rotazione automatica abilitata	SecretsManager1.				SecretsManager1.		SecretsManager1.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-RemoveUnsedSecret Rimuovi i segreti inutilizzati di Secrets Manager	SecretsManager3.				SecretsManager3.		SecretsManager3.
ASR-UpdateSecretRotationPeriod I segreti di Secrets Manager devono essere ruotati entro un determinato numero di giorni	SecretsManager4.				SecretsManager4.		SecretsManager4.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Attivazione ASR APIGateway CacheDataEncryption I dati della cache dell'API REST di API Gateway devono essere crittografati quando sono inattivi					APIGateway5.		APIGateway5.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-SetLogGroupRetentionDays CloudWatch i gruppi di log devono essere conservati per un periodo di tempo specificato					CloudWatch1.6		CloudWatch.16

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
A.S.R. AttachService VPCEndpont Amazon EC2 deve essere configurato per utilizzare gli endpoint VPC creati per il servizio Amazon EC2	EC2.10				EC2.10		EC2.10
A.S.R. TagGuardDutyResource GuardDuty i filtri devono essere etichettati							GuardDuty 2.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-TagGuardDutyResource GuardDuty i rilevatori devono essere etichettati							GuardDuty 4.
SSMPermissionsASR-Allega a EC2 EC2 Le istanze Amazon devono essere gestite da Systems Manager	SSM.1		SSM.3				SSM.1

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-ConfigureLaunchConfigNoPublic IPDocument EC2 Le istanze Amazon lanciate utilizzando le configurazioni di avvio del gruppo Auto Scaling non devono avere indirizzi IP pubblici					Autoscaling.5		Autoscaling.5

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Abilita ASR APIGateway Execution Logs	APIGateway1.						APIGateway1.
ASR-EnableMacie Amazon Macie dovrebbe essere abilitato	Macie.1				Macie.1		Macie.1
ASR-EnableAthenaWorkGroupLogging I gruppi di lavoro Athena devono avere la registrazione abilitata	Atena.4						Atena.4

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-Enforce LAB HTTPSFor Application Load Balancer deve essere configurato per reindirizzare tutte le richieste HTTP a HTTPS	ELB.1		ELB.1		ELB.1		ELB.1

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Limite ASR ECSRootFilesystemAccess I contenitori ECS devono essere limitati all'accesso in sola lettura ai filesystem root	ECS.5				ECS.5		ECS.5

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-EnableElastiCacheBackups ElastiCache I cluster (Redis OSS) devono avere i backup automatici abilitati	ElastiCache1.				ElastiCache1.		ElastiCache1.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-EnableElastiCacheVersionUpgrades ElastiCache i cluster dovrebbero avere gli aggiornamenti automatici delle versioni secondarie abilitati	ElastiCache2.				ElastiCache2.		ElastiCache2.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-EnableElastiCacheReplicationGroupFailover ElastiCache i gruppi di replica devono avere il failover automatico abilitato	ElastiCache3.				ElastiCache3.		ElastiCache3.

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
Scalabilità ASR Configure DynamoDBAuto Le tabelle DynamoDB dovrebbero scalare automaticamente la capacità in base alla domanda	DynamoDB.1				DynamoDB.1		DynamoDB.1
Risorsa ASR TagDynamoDBTable Le tabelle DynamoDB devono essere etichettate							DynamoDB.5

Descrizione	AWS FSBP	CIS versione 1.2.0	PCI versione 3.2.1	CIS versione 1.4.0	NIST	CIS versione 3.0.0	ID di controllo di sicurezza
ASR-Protezione EnableDynamoDBDeletion Le tabelle DynamoDB devono avere la protezione da eliminazione abilitata					DynamoDB.6		DynamoDB.6

Aggiungere nuove correzioni

Le riparazioni possono essere aggiunte manualmente aggiornando i file del playbook appropriati o a livello di codice estendendo la soluzione tramite costrutti CDK, a seconda del flusso di lavoro preferito.

> **Note**
>
> Le istruzioni che seguono sfruttano le risorse installate dalla soluzione come punto di partenza. Per convenzione, la maggior parte dei nomi delle risorse delle soluzioni contiene ASR and/or SO0111 per facilitarne l'individuazione e l'identificazione.

Panoramica del flusso di lavoro manuale

I runbook di Automated Security Response on AWS devono seguire la seguente denominazione standard:

ASR- - - *<standard>* *<version>* *<control>*

Standard: l'abbreviazione dello standard di sicurezza. Questo deve corrispondere agli standard supportati da ASR. Deve essere uno tra «CIS», «AFSBP», «PCI», «NIST» o «SC».

Versione: la versione dello standard. Anche in questo caso, deve corrispondere alla versione supportata da ASR e alla versione contenuta nei dati di ricerca.

Controllo: l'ID del controllo da correggere. Deve corrispondere ai dati di ricerca.

1. Crea un runbook negli account dei membri.
2. Crea un ruolo IAM negli account dei membri.
3. (Facoltativo) Crea una regola di correzione automatica nell'account amministratore.

Fase 1: Crea un runbook negli account dei membri

1. Accedi alla console AWS Systems Manager e ottieni un esempio di come trovare JSON.
2. Crea un runbook di automazione che corregga il risultato. Nella scheda Owned by me, usa uno qualsiasi dei `ASR-` documenti nella scheda Documenti come punto di partenza.
3. AWS Step Functions nell'account amministratore eseguirà il tuo runbook. Il runbook deve specificare il ruolo di riparazione per poter essere passato quando si chiama il runbook.

Fase 2: Crea un ruolo IAM negli account dei membri

1. Accedi alla console AWS Identity and Access Management.
2. Ottieni un esempio dai ruoli IAM SO0111 e crea un nuovo ruolo. Il nome del ruolo deve iniziare con SO0111-Remediate- - -. *<standard>* *<version>* *<control>* Ad esempio, se si aggiunge il controllo CIS v1.2.0 5.6, il ruolo deve essere. `SO0111-Remediate-CIS-1.2.0-5.6`
3. Utilizzando l'esempio, create un ruolo con ambito appropriato che consenta solo le chiamate API necessarie per eseguire la correzione.

A questo punto, la riparazione è attiva e disponibile per la riparazione automatica tramite ASR Custom Action in AWS Security Hub.

Passaggio 3: (Facoltativo) Crea una regola di riparazione automatica nell'account amministratore

La correzione automatica (non «automatizzata») è l'esecuzione immediata della riparazione non appena il risultato viene ricevuto da AWS Security Hub. Valuta attentamente i rischi prima di utilizzare questa opzione.

1. Visualizza una regola di esempio per lo stesso standard di sicurezza in CloudWatch Events. Lo standard di denominazione per le regole è`standard_control_*AutoTrigger*`.
2. Copia il modello di evento dall'esempio da utilizzare.
3. Modifica il `GeneratorId` valore in modo che corrisponda a quello `GeneratorId` nel tuo Finding JSON.
4. Salva e attiva la regola.

Panoramica del flusso di lavoro CDK

In sintesi, i seguenti file nel repository ASR verranno modificati o aggiunti. In questo esempio, è stata aggiunta una nuova correzione per ElastiCache .2 ai playbook SC e AFSBP.

> **Note**
>
> Tutte le nuove correzioni devono essere aggiunte al playbook SC, poiché consolida tutte le riparazioni disponibili in ASR. Se intendi distribuire solo un set specifico di playbook (ad esempio AFSBP), puoi: (1) aggiungere la correzione solo ai playbook desiderati oppure (2) aggiungere la correzione a tutti i playbook per i quali esiste nel corrispondente Security Hub Standard, oltre al playbook SC. La seconda opzione è consigliata per motivi di flessibilità.

In questo esempio, ElastiCache .2 è incluso nei seguenti standard Security Hub:

- AFSBP
- NIST.800-53.5r SI-2
- NIST.800-53.r5 SI-2 (2)
- NIST.800-53.r5 SI-2 (4)

- NIST.800-53.r5 SI-2 (5)
- PCI DSS versione 4.0.1/6.3.3

Poiché, per impostazione predefinita, ASR implementa solo i playbook per AFSBP e NIST.800-53, aggiungeremo questa nuova correzione a tali playbook oltre a SC.

Modifica

- source/lib/remediation-runbook-stack.ts
- source/playbooks/AFSBP/lib/[nome standard] _remediations.ts
- source/playbooks/NIST80053/lib/control_runbooks-construct.ts
- source/playbooks/NIST80053/lib/[nome standard] _remediations.ts
- source/playbooks/SC/lib/control_runbooks-construct.ts
- source/playbooks/SC/lib/sc_riparazioni.ts
- source/test/regex_registry.ts

Add

- source/playbooks/SC/ssmdocs/SC_.2.ts ElastiCache
- source/playbooks/SC/ssmdocs/descriptions/ElastiCache.2.md
- source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml

> **Note**
>
> Il nome scelto per il runbook può essere qualsiasi stringa, purché sia coerente con il resto delle modifiche apportate.

- source/playbooks/NIST80053/ssmdocs/NIST80053_ 2.ts ElastiCache
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Fasi di sviluppo

1. Crea il Remediation Runbook.

2. Create i Control Runbook.
3. Integra ogni Control Runbook con un playbook.
4. Crea il ruolo IAM di Remediation e integra il Remediation Runbook
5. Aggiorna i test unitari

Fase 1: Creare il Remediation Runbook

Questo è il documento SSM utilizzato per correggere le risorse. Deve includere il `AutomationAssumeRole` parametro, che è il ruolo IAM con le autorizzazioni per eseguire la riparazione. Visualizza il file esistente `source/remediation_runbooks/EnableElastiCacheVersionUpgrades.yaml` come riferimento durante la creazione di nuovi runbook di correzione.

Tutti i nuovi runbook devono essere aggiunti alla directory. `source/remediation_runbooks/`

Fase 2: Creare i Control Runbook

Un control runbook è un runbook specifico per un playbook che analizza i dati di ricerca dello standard specificato ed esegue il Remediation Runbook appropriato. Poiché stiamo aggiungendo la correzione ElastiCache .2 ai playbook SC, AFSBP e NIST8 0053, dobbiamo creare un nuovo runbook di controllo per ciascuno di essi. Vengono creati i seguenti file:

- source/playbooks/SC/ssmdocs/SC_ ElastiCache .2.ts
- source/playbooks/NIST80053/ssmdocs/NIST80053_ .2.ts ElastiCache
- source/playbooks/AFSBP/ssmdocs/AFSBP_ ElastiCache .2.yaml

Example

<PLAYBOOK_NAME><CONTROL.ID>La denominazione di questi file è importante e deve seguire il formato _ .ts/yaml

Alcuni playbook in ASR supportano i runbook di controllo IaC, mentre altri devono essere scritti in TypeScript formato YAML non elaborato. Fai riferimento alle correzioni esistenti nel rispettivo playbook come esempi. In questo esempio, tratteremo il playbook SC, che utilizza IAc.

Nel playbook SC, il nuovo runbook di controllo dovrebbe esportare una classe che si estende ControlRunbookDocument e corrisponde al nome del runbook di correzione. Dai un'occhiata all'esempio seguente:

```
export class EnableElastiCacheVersionUpgrades extends ControlRunbookDocument {
  constructor(scope: Construct, id: string, props: ControlRunbookProps) {
    super(scope, id, {
      ...props,
      securityControlId: 'ElastiCache.2',
      remediationName: 'EnableElastiCacheVersionUpgrades',
      scope: RemediationScope.REGIONAL,
      resourceIdRegex: <Regex>,
      resourceIdName: 'ClusterId',
      updateDescription: new StringFormat('Automatic minor version upgrades enabled for
 cluster %s.', [
        StringVariable.of(`ParseInput.ClusterId`),
      ]),
    });
  }
}
```

- `securityControlId`è l'ID di controllo per la correzione che si sta aggiungendo, così come definito nella vista dei controlli consolidati in Security Hub.
- `remediationName`è il nome che hai scelto per il tuo runbook di correzione.
- `scope`è l'ambito della risorsa da correggere, che indica se esiste a livello globale o in una regione specifica.
- `resourceIdRegex`è l'espressione regolare utilizzata per acquisire l'ID della risorsa che si desidera passare al runbook di correzione come parametro. È necessario acquisire solo un gruppo, tutti gli altri gruppi non devono essere acquisiti. Se desideri passare l'intero ARN, ometti questo campo.
- `resourceIdName`è il nome da impostare per l'ID della risorsa acquisito utilizzando`resourceIdRegex`, deve corrispondere al nome del parametro Resource ID nel runbook di correzione.
- `updateDescription`è la stringa che si desidera assegnare alla sezione «note» del risultato in Security Hub una volta completata la riparazione.

È inoltre necessario esportare una funzione chiamata `createControlRunbook` che restituisce una nuova istanza della classe. Per ElastiCache .2, questo assomiglia a:

```
export function createControlRunbook(scope: Construct, id: string, props:
 PlaybookProps): ControlRunbookDocument {
```

```
  return new EnableElastiCacheVersionUpgrades(scope, id, { ...props, controlId:
 'ElastiCache.2' });
}
```

dove `controlId` è l'ID di controllo definito nello standard di sicurezza associato al playbook in base al quale si opera.

Se il controllo Security Hub ha parametri che desideri passare al tuo runbook di correzione, puoi passarli aggiungendo sostituzioni ai seguenti metodi: -`getExtraSteps`: definisce i valori predefiniti per ogni parametro implementato per il controllo in Security Hub

> **Note**
>
> A ogni parametro di Security Hub deve essere assegnato un valore predefinito

- `getInputParamsStepOutput`: definisce gli output per la GetInputParams fase del control runbook
- Ogni uscita ha un `nameoutputType`, e. `selector` `selector`Dovrebbe essere lo stesso selettore utilizzato nell'override del `getExtraSteps` metodo.
- `getRemediationParams`: definisce i parametri passati al runbook di correzione, recuperati dagli output degli step. GetInputParams

Per visualizzare un esempio, accedi al file. `source/playbooks/SC/ssmdocs/SC_DynamoDB.1.ts`

Passaggio 3: integra ogni Control Runbook con un playbook

Per ogni runbook di controllo creato nel passaggio precedente, ora è necessario integrarlo con le definizioni dell'infrastruttura nel playbook associato. Segui i passaggi seguenti per ogni runbook di controllo.

> **Important**
>
> Se hai creato il runbook di controllo utilizzando YAML non elaborato anziché typescript IaC, passa alla sezione successiva.

In `/<playbook_name>/control_runbooks-construct.ts` Importa il tuo file di control runbook appena creato come:

```
import * as elasticache_2 from '../ssmdocs/SC_ElastiCache.2';
```

Quindi, vai all'array per

```
const controlRunbooksRecord: Record<string, any>
```

E aggiungi una nuova voce che mappi l'ID di controllo (specifico del playbook) al `createControlRunbook` metodo che hai creato:

```
'ElastiCache.2': elasticache_2.createControlRunbook,
```

Aggiungi l'ID di controllo specifico del playbook all'elenco delle correzioni nel modo seguente: `<playbook_name>\_remediations.ts`

```
{ control: 'ElastiCache.2', versionAdded: '2.3.0' },
```

Il `versionAdded` campo deve essere la versione più recente della soluzione. Se l'aggiunta della riparazione viola il limite di dimensione del modello, aumenta il. `versionAdded` Puoi modificare il numero di riparazioni incluse in ogni stack membro del playbook in. `solution_env.sh`

Fase 4: Creare il Remediation IAM Role & Integrate Remediation Runbook

Ogni riparazione ha il proprio ruolo IAM con autorizzazioni personalizzate necessarie per eseguire il runbook di riparazione. Inoltre, è necessario richiamare il `RunbookFactory.createRemediationRunbook` metodo per aggiungere il runbook di riparazione creato nel passaggio 1 ai modelli della soluzione. CloudFormation

In`remediation-runook-stack.ts`, ogni correzione ha il proprio blocco di codice nella classe. `RemediationRunbookStack` Il seguente blocco di codice mostra la creazione di un nuovo ruolo IAM e l'integrazione del runbook di riparazione per la ElastiCache correzione .2:

```
    //-----------------------
    // EnableElastiCacheVersionUpgrades
    //
    {
      const remediationName = 'EnableElastiCacheVersionUpgrades'; // should match the
 name of your remediation runbook
```

```
      const inlinePolicy = new Policy(props.roleStack, `ASR-Remediation-Policy-
${remediationName}`);

      const remediationPolicy = new PolicyStatement();
      remediationPolicy.addActions('elasticache:ModifyCacheCluster');
      remediationPolicy.effect = Effect.ALLOW;
      remediationPolicy.addResources(`arn:${this.partition}:elasticache:*:
${this.account}:cluster:*`);
      inlinePolicy.addStatements(remediationPolicy);

      new SsmRole(props.roleStack, 'RemediationRole ' + remediationName, { // creates
 the remediation IAM role
        solutionId: props.solutionId,
        ssmDocName: remediationName,
        remediationPolicy: inlinePolicy,
        remediationRoleName: `${remediationRoleNameBase}${remediationName}`,
      });

      RunbookFactory.createRemediationRunbook(this, 'ASR ' + remediationName, { // adds
 the remediation runbook to the solution's cloudformation templates
        ssmDocName: remediationName,
        ssmDocPath: ssmdocs,
        ssmDocFileName: `${remediationName}.yaml`,
        scriptPath: `${ssmdocs}/scripts`,
        solutionVersion: props.solutionVersion,
        solutionDistBucket: props.solutionDistBucket,
        solutionId: props.solutionId,
        namespace: namespace,
      });
    }
```

Fase 5: Aggiornamento dei test unitari

Consigliamo di aggiornare ed eseguire gli unit test dopo aver aggiunto una nuova correzione.

Innanzitutto, è necessario aggiungere tutte le nuove espressioni regolari (che non siano già state aggiunte) nel `source/test/regex_registry.ts` file. Questo file impone il test per ogni nuova espressione regolare inclusa nei runbook della soluzione. Dai un'occhiata alla `addElastiCacheClusterTestCases` funzione come esempio, che viene utilizzata per testare le espressioni regolari utilizzate nelle ElastiCache riparazioni.

Infine, dovrai aggiornare le istantanee per ogni stack. Le istantanee sono definizioni di CloudFormation modelli controllate dalla versione che vengono utilizzate per tenere traccia delle

modifiche apportate all'infrastruttura di ASR. È possibile aggiornare questi file di istantanee eseguendo il seguente comando dalla directory: `deployment`

```
./run-unit-tests.sh update
```

Ora sei pronto per implementare la tua nuova soluzione correttiva! Vai alla sezione Compila e distribuisci di seguito per istruzioni su come creare e distribuire la soluzione con le nuove modifiche.

Aggiungere un nuovo playbook

Scarica i playbook della soluzione Automated Security Response on AWS e distribuisci il codice sorgente dal GitHub repository.

Le CloudFormation risorse AWS vengono create dai componenti di AWS CDK e contengono il codice del modello di playbook che puoi utilizzare per creare e configurare nuovi playbook. Per ulteriori informazioni sulla configurazione del progetto e sulla personalizzazione dei playbook, consulta il file README.md in. GitHub

AWS Systems Manager Parameter Store

Automated Security Response on AWS utilizza AWS Systems Manager Parameter Store per lo storage dei dati operativi. I seguenti parametri sono memorizzati in Parameter Store:

Nome	Valore	Utilizzo
`/Solutions/SO0111/CMK_REMEDIATION_ARN`	Chiave AWS KMS che crittograferà i dati per le riparazioni FSBP	Crittografia dei dati dei clienti, come i CloudTrail log, come parte delle riparazioni
`/Solutions/SO0111/CMK_ARN`	Chiave AWS KMS che ASR utilizzerà per crittografare i dati	Crittografia dei dati della soluzione
`/Solutions/SO0111/SNS_Topic_ARN`	ARN dell'argomento relativo alla soluzione su Amazon SNS	Notifica degli eventi di riparazione
`/Solutions/SO0111/SNS_Topic_Config.1`	Argomento SNS per gli aggiornamenti di AWS Config	Correzione Config.1

Nome	Valore	Utilizzo
`/Solutions/SO0111/sendAnonymousMetrics`	`Yes`	Raccolta di metriche anonimizzate
`/Solutions/SO0111/version`	Versione della soluzione	
`/Solutions/SO0111/`*`<security standard long name>`*`/`*`<version>`* /status	`enabled`	Indica se lo standard è attivo nella soluzione. Uno standard può essere disabilitato per la riparazione automatica modificandolo in `disabled`
`/Solutions/SO0111` // nomebreve *`<security standard long name>`*	`String`	Nome abbreviato dello standard di sicurezza. Ad esempio:`CIS`,`AFSBP`, `PCI`
`/Solutions/SO0111//`*`<security standard long name><version>`* /*`<control>`* /remap	`String`	Quando un controllo utilizza la stessa correzione di un altro, questi parametri eseguono la rimappatura

Argomento di Amazon SNS: avanzamento della riparazione

Automated Security Response on AWS crea un argomento Amazon SNS, SO0111-ASR_topic. Questo argomento viene utilizzato per pubblicare aggiornamenti sullo stato di avanzamento delle riparazioni. Di seguito sono riportate le tre possibili notifiche inviate a questo argomento.

```
Remediation queued for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
Remediation failed for [.replaceable]`<standard>` control [.replaceable]`<control_ID>`
 in account [.replaceable]`<account_ID>`
```

```
[.replaceable]`<control_ID>` remediation was successfully invoke via AWS Systems
 Manager in account [.replaceable]`<account_ID>`
```

Questo è il messaggio di completamento. Indica che la riparazione è stata completata senza errori; tuttavia, il test definitivo per una corretta correzione è la convalida manuale di AWS Config check. and/or

Filtraggio di un abbonamento a un argomento SNS

Politiche di filtro degli abbonamenti Amazon SNS:

1. Vai alla sottoscrizione dell'argomento SNS.
2. In Politica di filtro degli abbonamenti, seleziona «Modifica».
3. Espandi «Politica di filtro degli abbonamenti» e attiva l'opzione «Politica di filtro degli abbonamenti» per abilitare i filtri.
4. Seleziona l'ambito «Corpo del messaggio».
5. Aggiungi la tua policy all'editor JSON.
6. Salva le modifiche.

Politiche di esempio:

Filtra per account

```
{
"finding": {
"account": [
"111111111111",
"222222222222"
]
}
```

Filtra per errori

```
{
"severity": ["ERROR"]
}
```

Filtra per controlli

```
{
"finding": {
"standard_control": ["S3.9","S3.6"]
}
}
```

Argomento Amazon SNS: allarmi CloudWatch

Questa soluzione crea un argomento Amazon SNS,. `SO0111-ASR_Alarm_Topic` Questo argomento viene utilizzato per pubblicare avvisi di allarme.

I dettagli di tutti gli allarmi che entrano nello stato ALARM verranno inviati a questo argomento.

Avvia Runbook su Config Findings

Questa soluzione può avviare runbook basati su risultati personalizzati di AWS Config. Per fare ciò dovrai:

1. Trova il nome della regola AWS Config a cui desideri correggere. Questo può essere trovato in AWS Config o nei risultati generati da Security Hub per questa regola.
2. Accedi ad AWS Systems Manager Parameter Store e seleziona Create Parameter.
3. Il nome della regola dovrebbe essere `/Solutions/SO0111/` [.replaceable] `Rule name from Step 1`
4. Il valore deve essere formattato come segue:

```
{

"RunbookName":"Name of SSM runbook",

"RunbookRole": "Role that Orchestrator will assume"

}
```

1. RunbookName è un campo obbligatorio e sarà il runbook che viene eseguito quando si corregge questa regola di Config. RunbookRole è il ruolo che l'orchestratore assumerà durante l'esecuzione

di questo ruolo. Non è un campo obbligatorio e, se omesso, l'orchestratore utilizzerà per impostazione predefinita il ruolo di membro dell'account.

2. Una volta completata questa operazione, puoi correggere la regola di Config utilizzando l'azione personalizzata «Ripara con ASR» disponibile nel Security Hub.

Riferimento

Questa sezione include informazioni su una funzionalità opzionale per la raccolta di metriche uniche per questa soluzione, riferimenti a risorse correlate e un elenco di costruttori che hanno contribuito a questa soluzione.

Raccolta di dati anonimizzata

Questa soluzione include un'opzione per inviare metriche operative anonime ad AWS. Utilizziamo questi dati per comprendere meglio come i clienti utilizzano questa soluzione e i servizi e i prodotti correlati. Se abilitata, le seguenti informazioni vengono raccolte e inviate ad AWS:

- ID della soluzione: l'identificatore della soluzione AWS
- ID univoco (UUID): identificatore univoco generato casualmente per ogni distribuzione di AWS Security Hub Response and Remediation
- Timestamp: timestamp di raccolta dati
- Dati dell'istanza: informazioni sulla distribuzione di questo stack
- Configurazione della soluzione: funzionalità attivate e parametri impostati durante l'avvio iniziale
- Stato: stato della distribuzione (soluzione approvata o non riuscita) o (riparazione approvata o fallita)
- Messaggio di errore: il messaggio di errore generico nel campo dello stato
- Generator_ID - Informazioni sulle regole del Security Hub
- Tipo: tipo e nome della riparazione
- ProductARN - La regione in cui viene distribuito Security Hub
- finding_triggered_by - Il tipo di riparazione eseguita (azione personalizzata o trigger automatico)

AWS è proprietaria dei dati raccolti tramite questo sondaggio. La raccolta dei dati è soggetta all'Informativa sulla privacy di AWS. Per disattivare questa funzionalità, completa i seguenti passaggi prima di avviare il CloudFormation modello AWS.

1. Scarica il CloudFormation modello AWS sul tuo disco rigido locale.
2. Apri il CloudFormation modello AWS con un editor di testo.
3. Modifica la sezione di mappatura dei CloudFormation modelli AWS da:

```
Mappings:
Solution:
Data:
SendAnonymizedUsageData: 'Yes'
```

to:

```
Mappings:
Solution:
Data:
SendAnonymizedUsageData: 'No'
```

4. Accedi alla CloudFormation console AWS.
5. Seleziona Create stack.
6. Nella pagina Crea stack, sezione Specificare il modello, seleziona Carica un file modello.
7. In Carica un file modello, scegli Scegli file e seleziona il modello modificato dall'unità locale.
8. Scegli Avanti e segui i passaggi descritti in Avvia lo stack nella sezione Distribuzione automatizzata di questa guida.

Risorse correlate

- Risposta e riparazione automatizzate con AWS Security Hub
- Benchmark CIS Amazon Web Services Foundations, versione 1.2.0
- Standard AWS Foundational Security Best Practice
- Payment Card Industry Data Security Standard (PCI DSS)
- Istituto nazionale di standard e tecnologia (NIST) SP 800-53 Rev. 5

Collaboratori

Le seguenti persone hanno contribuito a questo documento:

- Mike O'Brien
- Nikhil Reddy
- Chandini Penmetsa

- Chaitanya Deolankar
- Max Granat
- Tim Mekari
- Aaron Schuetter
- Andrew Yankowsky
- Josh Moss
- Ryan Garay
- Thiemo Belmega
- Mikhail Markhain

Revisioni

Data di pubblicazione: agosto 2020 (ultimo aggiornamento: gennaio 2025)

Visita Changelog.md nel nostro GitHub repository per tenere traccia dei miglioramenti e delle correzioni specifici della versione.

Note

I clienti sono responsabili della propria valutazione indipendente delle informazioni contenute nel presente documento. Questo documento: (a) è solo a scopo informativo, (b) rappresenta le attuali offerte e pratiche di prodotti AWS, che sono soggette a modifiche senza preavviso, e (c) non crea alcun impegno o garanzia da parte di AWS e delle sue affiliate, fornitori o licenzianti. I prodotti o i servizi AWS sono forniti «così come sono» senza garanzie, dichiarazioni o condizioni di alcun tipo, esplicite o implicite. Le responsabilità e gli obblighi di AWS nei confronti dei propri clienti sono controllati da accordi AWS e questo documento non fa parte né modifica alcun accordo tra AWS e i suoi clienti.

Automated Security Response on AWS è concesso in licenza secondo i termini della versione 2.0 della licenza Apache, disponibile presso The Apache Software Foundation.

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.