aws

Guida per l'utente

Amazon Inspector

Amazon Inspector: Guida per l'utente

Table of Contents

Che cos'è Amazon Inspector?

Amazon Inspector è un servizio di gestione delle vulnerabilità che analizza continuamente i AWS carichi di lavoro alla ricerca di vulnerabilità del software ed esposizione involontaria della rete. Amazon Inspector rileva e analizza automaticamente le istanze Amazon EC2 in esecuzione, le immagini dei container in Amazon Elastic Container Registry (Amazon ECR) e le funzioni alla ricerca di vulnerabilità software note e di esposizione involontaria alla rete. AWS Lambda

Amazon Inspector crea un risultato quando rileva una vulnerabilità del software o un problema di configurazione della rete. Una scoperta descrive la vulnerabilità, identifica la risorsa interessata, valuta la gravità della vulnerabilità e fornisce indicazioni per la risoluzione. Puoi analizzare i risultati utilizzando la console Amazon Inspector o visualizzare ed elaborare i risultati tramite altri. Servizi AWS Per ulteriori informazioni, consulta Comprendere i risultati in Amazon Inspector.

Argomenti

Caratteristiche di Amazon Inspector

Gestione centralizzata di più account Amazon Inspector

Se AWS l'ambiente dispone di più account, è possibile gestire centralmente l'ambiente tramite un singolo account utilizzando AWS Organizations. Utilizzando questo approccio, puoi designare un account come account amministratore delegato per Amazon Inspector.

Amazon Inspector può essere attivato per l'intera organizzazione con un solo clic. Inoltre, puoi automatizzare l'attivazione del servizio per i futuri membri ogni volta che entrano a far parte della tua organizzazione. L'account amministratore delegato di Amazon Inspector può gestire i risultati, i dati e determinate impostazioni per i membri dell'organizzazione. Ciò include la visualizzazione dei dettagli aggregati dei risultati per tutti gli account dei membri, l'attivazione o la disattivazione delle scansioni per gli account dei membri e la revisione delle risorse scansionate all'interno dell'organizzazione. AWS

Scansiona continuamente il tuo ambiente per individuare vulnerabilità ed esposizione della rete

Con Amazon Inspector, non è necessario pianificare o configurare manualmente le scansioni di valutazione. Amazon Inspector rileva e avvia automaticamente la scansione delle risorse idonee.

Amazon Inspector continua a valutare l'ambiente durante l'intero ciclo di vita delle risorse effettuando una nuova scansione automatica delle risorse in risposta a modifiche che potrebbero introdurre una nuova vulnerabilità, ad esempio: installazione di un nuovo pacchetto in un'istanza EC2, installazione di una patch e quando viene pubblicata una nuova vulnerabilità ed esposizione comune (CVE) che ha un impatto sulla risorsa. A differenza dei tradizionali software di scansione di sicurezza, Amazon Inspector ha un impatto minimo sulle prestazioni della tua flotta.

Quando vengono identificate vulnerabilità o percorsi di rete aperti, Amazon Inspector produce un risultato che puoi esaminare. La scoperta include dettagli completi sulla vulnerabilità, sulla risorsa interessata e raccomandazioni per la correzione. Se correggi in modo appropriato un risultato, Amazon Inspector rileva automaticamente il problema e lo chiude.

Valuta accuratamente le vulnerabilità con il punteggio di rischio di Amazon Inspector

Poiché Amazon Inspector raccoglie informazioni sull'ambiente tramite scansioni, fornisce punteggi di gravità specificamente adattati al tuo ambiente. Amazon Inspector esamina i parametri di sicurezza che compongono il punteggio di base del National Vulnerability Database (NVD) per una vulnerabilità e li regola in base all'ambiente di elaborazione. Ad esempio, il servizio può ridurre il punteggio Amazon Inspector di un risultato per un'istanza Amazon EC2 se la vulnerabilità è sfruttabile sulla rete ma dall'istanza non è disponibile alcun percorso di rete aperto verso Internet. Questo punteggio è in formato CVSS ed è una modifica del punteggio di base del Common Vulnerability Scoring System (CVSS) fornito da NVD.

Identifica i risultati ad alto impatto con la dashboard di Amazon Inspector

La dashboard di Amazon Inspector offre una visione di alto livello dei risultati provenienti da tutto l'ambiente. Dalla dashboard, puoi accedere ai dettagli granulari di un risultato. La dashboard contiene informazioni semplificate sulla copertura delle scansioni nell'ambiente in uso, sui risultati più critici e sulle risorse con il maggior numero di risultati. Il pannello di correzione basata sul rischio nella dashboard di Amazon Inspector presenta i risultati che riguardano il maggior numero di istanze e immagini. Questo pannello semplifica l'identificazione dei risultati con il maggiore impatto sull'ambiente, l'analisi dei dettagli dei risultati e l'esame delle soluzioni suggerite.

Gestisci i risultati utilizzando visualizzazioni personalizzabili

Oltre alla dashboard, la console Amazon Inspector offre una visualizzazione dei risultati. Questa pagina elenca tutti i risultati relativi al tuo ambiente e fornisce i dettagli dei singoli risultati. È possibile visualizzare i risultati raggruppati per categoria o tipo di vulnerabilità. In ogni visualizzazione, puoi personalizzare ulteriormente i risultati utilizzando i filtri. Puoi anche utilizzare i filtri per creare regole di soppressione che nascondono i risultati indesiderati dalle tue visualizzazioni.

È possibile utilizzare filtri e regole di soppressione per generare report sui risultati che mostrano tutti i risultati o una selezione personalizzata di risultati. I report possono essere generati in formato CSV o JSON.

Monitora ed elabora i risultati con altri servizi e sistemi

Per supportare l'integrazione con altri servizi e sistemi, Amazon Inspector pubblica i risultati su Amazon EventBridge come eventi di ricerca. EventBridge è un servizio di bus eventi senza server in grado di indirizzare i dati dei risultati verso destinazioni come AWS Lambda funzioni e argomenti di Amazon Simple Notification Service (Amazon SNS). Con EventBridge, puoi monitorare ed elaborare i risultati quasi in tempo reale come parte dei flussi di lavoro di sicurezza e conformità esistenti.

Se l'hai attivato AWS Security Hub, Amazon Inspector pubblicherà anche i risultati su Security Hub. Security Hub è un servizio che fornisce una visione completa del livello di sicurezza in tutto l' AWS ambiente e ti aiuta a controllare il tuo ambiente rispetto agli standard e alle best practice del settore della sicurezza. Con Security Hub, puoi monitorare ed elaborare più facilmente i tuoi risultati come parte di un'analisi più ampia del livello di sicurezza della tua organizzazione. AWS

Accesso ad Amazon Inspector

Amazon Inspector è disponibile nella maggior parte dei casi. Regioni AWS Per un elenco delle regioni in cui Amazon Inspector è attualmente disponibile, consulta gli endpoint e le quote di Amazon Inspector nell'Amazon Web Services General Reference. Per ulteriori informazioni Regioni AWS, consulta Managing Regioni AWS in Amazon Web Services General Reference. In ogni regione, puoi lavorare con Amazon Inspector nei seguenti modi.

AWS Console di gestione

AWS Management Console È un'interfaccia basata su browser che è possibile utilizzare per creare e gestire AWS risorse. Come parte di tale console, la console Amazon Inspector fornisce l'accesso al tuo account e alle tue risorse Amazon Inspector. Puoi eseguire attività di Amazon Inspector dalla console Amazon Inspector.

AWS strumenti da riga di comando

Con gli strumenti da riga di AWS comando, puoi emettere comandi dalla riga di comando del tuo sistema per eseguire attività di Amazon Inspector. L'utilizzo della riga di comando può essere più rapido e conveniente rispetto all'utilizzo della console. Gli strumenti a riga di comando sono inoltre utili per creare script che eseguono le attività di .

AWS fornisce due set di strumenti da riga di comando: the AWS Command Line Interface (AWS CLI) e the AWS Tools for PowerShell. Per informazioni sull'installazione e l'utilizzo di AWS CLI, consultate la Guida per l'utente dell'interfaccia a riga di AWS comando. Per informazioni sull'installazione e l'utilizzo degli strumenti per PowerShell, consultate la Guida per AWS Tools for PowerShell l'utente.

AWS SDK

AWS fornisce SDK costituiti da librerie e codice di esempio per vari linguaggi e piattaforme di programmazione, tra cui Java, Go, Python, C++ e.NET. Gli SDK forniscono un accesso pratico e programmatico ad Amazon Inspector e ad altri. Servizi AWS Gestiscono anche attività come la firma crittografica delle richieste, la gestione degli errori e il ritentativo automatico delle richieste. Per informazioni sull'installazione e l'utilizzo degli AWS SDK, consulta Tools to Build on. AWS

API REST di Amazon Inspector

L'API REST di Amazon Inspector ti offre un accesso completo e programmatico al tuo account e alle tue risorse Amazon Inspector. Con questa API, puoi inviare richieste HTTPS direttamente ad Amazon Inspector. Tuttavia, a differenza degli strumenti da riga di AWS comando e degli SDK, l'uso di questa API richiede che l'applicazione gestisca dettagli di basso livello, come la generazione di un hash per firmare una richiesta.

Guida introduttiva ad Amazon Inspector

Questo tutorial fornisce un'introduzione pratica ad Amazon Inspector.

La fase 1 riguarda l'attivazione delle scansioni di Amazon Inspector per un account autonomo o come amministratore delegato di Amazon Inspector in un ambiente con più account. AWS Organizations

La fase 2 riguarda la comprensione dei risultati di Amazon Inspector nella console.

> **Note**
>
> In questo tutorial, completerai le attività con la tua attuale Regione AWS modalità. Per configurare Amazon Inspector in altre regioni, devi completare questi passaggi in ciascuna di tali regioni.

Argomenti

Prima di iniziare

Amazon Inspector è un servizio di gestione delle vulnerabilità che analizza continuamente le istanze Amazon EC2, le immagini dei container Amazon ECR e le funzioni alla ricerca di vulnerabilità del software AWS Lambda ed esposizione involontaria alla rete.

Tieni presente quanto segue prima di attivare Amazon Inspector:

- Amazon Inspector è un servizio regionale e i dati vengono archiviati nel luogo in Regione AWS cui utilizzi il servizio. Tutte le procedure di configurazione che completi in questo tutorial devono essere ripetute in ognuna delle procedure di configurazione Regione AWS che desideri monitorare con Amazon Inspector.
- Amazon Inspector ti offre la flessibilità necessaria per attivare l'istanza Amazon EC2, l'immagine del contenitore Amazon ECR e la scansione delle funzioni. AWS Lambda Puoi gestire i tipi di scansione dalla pagina di gestione dell'account nella console Amazon Inspector o utilizzando le API di Amazon Inspector.

- Amazon Inspector può fornire dati CVE (Common Vulnerabilities and Exposures) per le tue istanze EC2 solo se l'agente Amazon EC2 Systems Manager (SSM) è installato e attivato. Questo agente è preinstallato su molte istanze EC2, ma potrebbe essere necessario attivarlo manualmente. Indipendentemente dallo stato dell'agente SSM, tutte le istanze EC2 vengono analizzate per individuare eventuali problemi di esposizione alla rete. Per ulteriori informazioni sulla configurazione delle scansioni per Amazon EC2, consulta. Scansione delle istanze Amazon EC2 Amazon ECR e la scansione delle AWS Lambda funzioni non richiedono l'uso di un agente.
- Un'identità utente IAM con autorizzazioni di amministratore Account AWS può abilitare Amazon Inspector. Ai fini della protezione dei dati, ti consigliamo di proteggere le tue credenziali e di configurare singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In questo modo, a ciascun utente vengono concesse solo le autorizzazioni necessarie per gestire Amazon Inspector. Per informazioni sulle autorizzazioni necessarie per abilitare Amazon Inspector, consulta. AWS politica gestita: AmazonInspector2FullAccess
- Quando attivi Amazon Inspector per la prima volta in qualsiasi regione, viene creato un ruolo collegato al servizio a livello globale per il tuo account chiamato. `AWSServiceRoleForAmazonInspector2` Questo ruolo include le autorizzazioni e le policy di fiducia che consentono ad Amazon Inspector di raccogliere i dettagli dei pacchetti software e analizzare le configurazioni di Amazon VPC per generare rilevazioni di vulnerabilità. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon Inspector. Per ulteriori informazioni sui ruoli collegati ai servizi, consulta Utilizzo di ruoli collegati ai servizi.

Fase 1: Attivazione di Amazon Inspector

Il primo passaggio per utilizzare Amazon Inspector è attivarlo per il tuo. Account AWS Dopo aver attivato qualsiasi tipo di scansione di Amazon Inspector, Amazon Inspector inizia immediatamente a scoprire e scansionare tutte le risorse idonee.

Se desideri gestire Amazon Inspector per più account all'interno della tua organizzazione tramite un account amministratore centralizzato, devi assegnare un amministratore delegato per Amazon Inspector. Scegli una delle seguenti opzioni per scoprire come attivare Amazon Inspector per il tuo ambiente.

Standalone account environment

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Seleziona Inizia.

3. Scegli Activate Amazon Inspector.

Quando attivi Amazon Inspector in un account standalone, tutti i tipi di scansione vengono attivati per impostazione predefinita. Puoi gestire i tipi di scansione attivati dalla pagina di gestione dell'account all'interno della console Amazon Inspector o utilizzando le API di Amazon Inspector. Dopo l'attivazione, Amazon Inspector rileva automaticamente e avvia la scansione di tutte le risorse idonee. Consulta le seguenti informazioni sul tipo di scansione per capire quali risorse sono idonee di default:

Scansione Amazon EC2

Per fornire dati CVE (Common Vulnerabilities and Exposures) per la tua istanza EC2, Amazon Inspector richiede l'installazione e l'attivazione dell'agente Systems AWS Manager (SSM). Questo agente è preinstallato su molte istanze EC2, ma potrebbe essere necessario attivarlo manualmente. Indipendentemente dallo stato dell'agente SSM, tutte le istanze EC2 verranno analizzate per individuare eventuali problemi di esposizione alla rete. Per ulteriori informazioni sulla configurazione delle scansioni per Amazon EC2, consulta. Scansione delle istanze Amazon EC2 con Amazon Inspector

Scansione Amazon ECR

Quando attivi la scansione Amazon ECR, Amazon Inspector converte tutti gli archivi di container nel tuo registro privato configurati per la scansione Basic predefinita fornita da Amazon ECR in scansione avanzata con scansione continua. Puoi anche configurare facoltativamente questa impostazione per eseguire la scansione solo in modalità push o per scansionare determinati repository tramite regole di inclusione. Tutte le immagini inviate negli ultimi 30 giorni sono programmate per la scansione a vita, questa impostazione di scansione di Amazon ECR può essere modificata in qualsiasi momento. Per ulteriori informazioni sulla configurazione delle scansioni per Amazon ECR, consulta. Scansione delle immagini dei container Amazon ECR con Amazon Inspector

AWS Lambda funzione di scansione

Quando attivi la scansione delle AWS Lambda funzioni, Amazon Inspector rileva le funzioni Lambda nel tuo account e inizia immediatamente a scansionarle per individuare eventuali vulnerabilità. Amazon Inspector analizza nuove funzioni e layer Lambda quando vengono distribuiti e li scansiona nuovamente quando vengono aggiornati o quando vengono pubblicati nuovi Common Vulnerabilities and Exposures (CVE). Amazon Inspector offre due diversi livelli di scansione della funzione Lambda. Per impostazione predefinita, quando attivi

Amazon Inspector per la prima volta, viene attivata la scansione standard Lambda, che analizza le dipendenze dei pacchetti nelle tue funzioni. Puoi anche attivare la scansione del codice Lambda per scansionare il codice dello sviluppatore nelle tue funzioni alla ricerca di vulnerabilità del codice. Per ulteriori informazioni sulla configurazione della scansione della funzione Lambda, vedere. AWS Lambda Funzioni di scansione con Amazon Inspector

Multi-account environment

Important

Per completare questi passaggi, devi far parte della stessa organizzazione di tutti gli account che desideri gestire e avere accesso all'account di AWS Organizations gestione per delegare un amministratore di Amazon Inspector all'interno della tua organizzazione. Potrebbero essere necessarie autorizzazioni aggiuntive per delegare un amministratore. Per ulteriori informazioni, consulta Autorizzazioni necessarie per designare un amministratore delegato.

Note

Per abilitare in modo programmatico Amazon Inspector per più account in più regioni, puoi utilizzare uno script di shell sviluppato da Amazon Inspector. Per ulteriori informazioni sull'uso di questo script, consulta inspector2 - on. enablement-with-cli GitHub

Delega di un amministratore per Amazon Inspector

1. Accedi all'account di AWS Organizations gestione.
2. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
3. Nel riquadro Amministratore delegato, inserisci l'ID a dodici cifre di chi desideri designare come amministratore delegato di Amazon Inspector per l'organizzazione. Account AWS Quindi scegli Delegato. Quindi, nella finestra di conferma, scegli nuovamente Delega.

> **Note**
>
> Amazon Inspector viene attivato per il tuo account quando deleghi un amministratore.

Aggiungere account membri

In qualità di amministratore delegato, puoi attivare la scansione per qualsiasi membro associato all'account di gestione Organizations. Questo flusso di lavoro attiva tutti i tipi di scansione per tutti gli account dei membri. Tuttavia, i membri possono anche attivare Amazon Inspector per i propri account oppure le scansioni di un servizio possono essere attivate selettivamente dall'amministratore delegato. Per ulteriori informazioni, consulta Gestione di più account .

1. Accedi all'account amministratore delegato.
2. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
3. Nel riquadro di navigazione, scegli Gestione account. La tabella Account mostra tutti gli account membro associati all'account di gestione Organizations.
4. Dalla pagina Gestione degli account, puoi scegliere Attiva la scansione per tutti gli account dal banner superiore per attivare le istanze EC2, le immagini dei contenitori ECR e la AWS Lambda funzione di scansione per tutti gli account dell'organizzazione. In alternativa, puoi scegliere gli account che desideri aggiungere come membri selezionandoli nella tabella Account. Quindi, dal menu Attiva, seleziona Tutte le scansioni.
5. (Facoltativo) Attiva la funzionalità Attiva automaticamente Inspector per i nuovi account membro e seleziona i tipi di scansione da includere per attivare tali scansioni per tutti i nuovi account membro aggiunti alla tua organizzazione.

Amazon Inspector attualmente offre scansioni per istanze EC2, immagini di contenitori ECR e funzioni. AWS Lambda Dopo aver attivato Amazon Inspector, inizia automaticamente a scoprire e scansionare tutte le risorse idonee. Consulta le seguenti informazioni sul tipo di scansione per capire quali risorse sono idonee di default:

Scansione Amazon EC2

Per fornire dati sulle vulnerabilità CVE per le istanze EC2, Amazon Inspector richiede l'installazione e l'attivazione dell'agente AWS Systems Manager (SSM). Questo agente è

preinstallato su molte istanze EC2, ma potrebbe essere necessario attivarlo manualmente. Indipendentemente dallo stato dell'agente SSM, tutte le istanze EC2 verranno analizzate per individuare eventuali problemi di esposizione alla rete. Per ulteriori informazioni sulla configurazione delle scansioni per Amazon EC2, consulta. Scansione delle istanze Amazon EC2 con Amazon Inspector

Scansione Amazon ECR

Quando attivi la scansione Amazon ECR, Amazon Inspector converte tutti gli archivi di container nel tuo registro privato configurati per la scansione Basic predefinita fornita da Amazon ECR in scansione avanzata con scansione continua. Puoi anche configurare facoltativamente questa impostazione per eseguire la scansione solo in modalità push o per scansionare determinati repository tramite regole di inclusione. È prevista la scansione a vita per tutte le immagini inviate negli ultimi 30 giorni. Questa impostazione di scansione di Amazon ECR può essere modificata dall'amministratore delegato in qualsiasi momento. Per ulteriori informazioni sulla configurazione delle scansioni per Amazon ECR, consulta. Scansione delle immagini dei container Amazon ECR con Amazon Inspector

AWS Lambda funzione di scansione

Quando attivi la scansione delle AWS Lambda funzioni, Amazon Inspector rileva le funzioni Lambda nel tuo account e inizia immediatamente a scansionarle per individuare eventuali vulnerabilità. Amazon Inspector analizza nuove funzioni e layer Lambda quando vengono distribuiti e li scansiona nuovamente quando vengono aggiornati o quando vengono pubblicati nuovi Common Vulnerabilities and Exposures (CVE). Per ulteriori informazioni sulla configurazione della scansione della funzione Lambda, vedere. AWS Lambda Funzioni di scansione con Amazon Inspector

Fase 2: Visualizza i risultati di Amazon Inspector

Puoi visualizzare i risultati relativi al tuo ambiente nella console Amazon Inspector o tramite l'API. Tutti i risultati vengono inoltre inviati ad Amazon EventBridge e AWS Security Hub (se attivati). Inoltre, i risultati delle immagini dei container vengono inviati ad Amazon ECR.

La console Amazon Inspector offre diversi formati di visualizzazione dei risultati. La dashboard di Amazon Inspector offre una panoramica di alto livello dei rischi per il tuo ambiente, mentre la tabella Findings ti consente di visualizzare i dettagli di un risultato specifico.

In questa fase, esplori i dettagli di un risultato utilizzando la tabella Findings e il dashboard Findings. Per informazioni sulla dashboard di Amazon Inspector, consulta. Comprendere la dashboard

Per visualizzare i dettagli dei risultati relativi al tuo ambiente nella console Amazon Inspector:

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Dal pannello di navigazione, seleziona Dashboard. Puoi selezionare uno qualsiasi dei link nella dashboard per accedere a una pagina nella console Amazon Inspector con maggiori dettagli su quell'elemento.
3. Dal pannello di navigazione, seleziona Findings.
4. Per impostazione predefinita, viene visualizzata la scheda Tutti i risultati, che mostra tutti i risultati relativi alle istanze EC2, all'immagine del contenitore ECR e alle AWS Lambda funzioni per il tuo ambiente.
5. Nell'elenco Findings, scegli il nome di un risultato nella colonna Titolo per aprire il riquadro dei dettagli relativo a quel risultato. Tutti i risultati hanno una scheda con i dettagli del ritrovamento. Puoi interagire con la scheda Dettagli del ritrovamento nei seguenti modi:

   - Per maggiori dettagli sulla vulnerabilità, segui il link nella sezione Dettagli sulla vulnerabilità per aprire la documentazione relativa a questa vulnerabilità.
   - Per esaminare ulteriormente la risorsa, segui il link ID risorsa nella sezione Risorsa interessata per aprire la console di servizio relativa alla risorsa interessata.

   Le rilevazioni relative ai tipi di vulnerabilità dei pacchetti includono anche una scheda Inspector Score e informazioni sulle vulnerabilità che spiegano come è stato calcolato il punteggio Amazon Inspector per tale scoperta e forniscono informazioni sui Common Vulnerability and Exploits (CVE) associati alla scoperta. Per ulteriori dettagli sulla ricerca dei tipi, consulta. Ricerca dei tipi in Amazon Inspector

Comprendere la dashboard di Amazon Inspector

La dashboard di Amazon Inspector fornisce un'istantanea delle statistiche aggregate per le tue AWS risorse nella regione corrente. AWS Queste statistiche includono metriche chiave per la copertura delle risorse e le vulnerabilità attive. La dashboard mostra anche gruppi di dati aggregati relativi ai risultati del tuo account, come le istanze Amazon Elastic Compute Cloud (Amazon EC2), Amazon Elastic Container Registry (Amazon ECR) e le funzioni con i risultati più critici. AWS Lambda Per eseguire un'analisi più approfondita, puoi visualizzare i dati di supporto per gli elementi del dashboard.

Se il tuo account è l'account amministratore delegato di Amazon Inspector di un'organizzazione, la dashboard include la copertura dell'account, le statistiche aggregate e i dati sui risultati per tutti gli account della tua organizzazione, incluso il tuo account.

Visualizzazione del pannello di controllo

La dashboard mostra una panoramica della copertura dell'ambiente e dei risultati critici.

Per visualizzare la dashboard:

1. Apri la console Amazon Inspector https://console.aws.amazon.com/inspector/v2/home.
2. Nel pannello di navigazione seleziona Pannello di controllo.
3. Puoi interagire con la dashboard nei seguenti modi:

    - La dashboard si aggiorna automaticamente ogni cinque minuti. Tuttavia, puoi aggiornare i dati manualmente selezionando l'icona di aggiornamento nell'angolo in alto a destra della pagina.
    - Per visualizzare i dati di supporto per un elemento sulla dashboard, scegli l'elemento.
    - Se gestisci più account tramite AWS organizzazioni come amministratore delegato di Amazon Inspector, la dashboard mostra statistiche aggregate per i tuoi account membro. Per filtrare la dashboard e visualizzare i dati solo per un determinato account, inserisci l'ID dell'account nella casella Account.

Comprensione dei componenti della dashboard e interpretazione dei dati

Ogni sezione della dashboard di Amazon Inspector fornisce informazioni sulle metriche chiave o sui dati relativi ai risultati attivi che possono aiutarti a comprendere lo stato di vulnerabilità delle tue AWS risorse nel momento attuale. Regione AWS

Copertura ambientale

La sezione Copertura ambientale fornisce statistiche sulle risorse analizzate da Amazon Inspector. In questa sezione, puoi visualizzare il numero e la percentuale di istanze Amazon EC2, immagini e AWS Lambda funzioni Amazon ECR scansionate da Amazon Inspector. Se gestisci più account in AWS Organizations qualità di amministratore delegato di Amazon Inspector, vedrai anche il numero totale di account dell'organizzazione, il numero con Amazon Inspector attivato e la percentuale di copertura risultante per l'organizzazione. Puoi anche utilizzare questa sezione per determinare quali risorse non sono coperte da Amazon Inspector. Queste risorse possono contenere vulnerabilità che potrebbero essere sfruttate per mettere a rischio la tua organizzazione. Per ulteriori dettagli, consulta Valutazione della copertura di Amazon Inspector del tuo ambiente AWS.

La scelta di un gruppo di copertura porta alla pagina di gestione dell'account relativa al raggruppamento selezionato. La pagina di gestione degli account mostra i dettagli su quali account, istanze Amazon EC2 e repository Amazon ECR sono coperti da Amazon Inspector.

Sono disponibili i seguenti gruppi di copertura:

- Account
- Istanze
- Archivi di contenitori
- Immagini di container
- Lambda

Risultati critici

La sezione Risultati critici fornisce un conteggio delle vulnerabilità critiche nell'ambiente e un conteggio totale di tutti i risultati presenti nell'ambiente. In questa sezione, i conteggi sono mostrati per risorsa e tipo di valutazione. Per ulteriori informazioni sui risultati critici e su come Amazon Inspector determina la criticità, consulta. Comprendere i risultati in Amazon Inspector

La scelta di un gruppo di risultati critici ti porta alla pagina Tutti i risultati e applica automaticamente i filtri per mostrare tutti i risultati critici che corrispondono al raggruppamento selezionato.

Sono disponibili i seguenti gruppi di risultati critici:

- Risultati delle immagini dei contenitori ECR
- Risultati di Amazon EC2
- Risultati sulla raggiungibilità della rete
- AWS Lambda risultati delle funzioni

Correzioni basate sul rischio

La sezione Correzioni basate sul rischio mostra i cinque principali pacchetti software con vulnerabilità critiche che interessano la maggior parte delle risorse dell'ambiente. La correzione di questi pacchetti può ridurre in modo significativo il numero di rischi critici per l'ambiente. Scegliete il nome del pacchetto software per visualizzare i dettagli delle vulnerabilità associate e le risorse interessate.

Account con i risultati più critici

La sezione Account con i risultati più critici mostra i primi cinque AWS account dell'ambiente con i risultati più critici e il numero totale di risultati per quell'account. Questa sezione è visualizzabile dall'account amministratore delegato solo se Amazon Inspector è configurato per la scansione di più account con. AWS Organizations Questa visualizzazione aiuta gli amministratori delegati a capire quali account possono essere maggiormente a rischio all'interno dell'organizzazione.

Scegli Account ID per visualizzare ulteriori informazioni sull'account membro interessato.

Repository Amazon ECR con i risultati più critici

La sezione Repositories Elastic Container Registry (ECR) con i risultati più critici mostra i cinque principali repository Amazon ECR del tuo ambiente con i risultati più critici relativi alle immagini dei container. La vista mostra il nome del repository, l'identificatore AWS dell'account, la data di creazione del repository, il numero di vulnerabilità critiche e il numero totale di vulnerabilità. Questa visualizzazione consente di identificare i repository più a rischio.

Scegli il nome del repository per visualizzare ulteriori informazioni sul repository interessato.

Immagini dei container con i risultati più critici

La sezione Immagini dei container con i risultati più critici mostra le prime cinque immagini dei container presenti nell'ambiente con i risultati più critici. La visualizzazione mostra i dati dei tag

di immagine, il nome del repository, l'image digest, l'identificatore AWS dell'account, il numero di vulnerabilità critiche e il numero totale di vulnerabilità. Questa visualizzazione aiuta i proprietari delle applicazioni a identificare quali immagini del contenitore potrebbero dover essere ricostruite e riavviate.

Scegliete Immagine del contenitore per visualizzare ulteriori informazioni sull'immagine del contenitore interessata.

Istanze con i risultati più critici

La sezione Istanze con i risultati più critici mostra le prime cinque istanze di Amazon EC2 con i risultati più critici. La vista mostra l'identificatore dell'istanza, l'identificatore AWS dell'account, l'identificatore Amazon Machine Image (AMI), il numero di vulnerabilità critiche e il numero totale di vulnerabilità. Questa visualizzazione aiuta i proprietari dell'infrastruttura a identificare quali istanze potrebbero richiedere l'applicazione di patch.

Scegli Instance ID per visualizzare ulteriori informazioni sull'istanza Amazon EC2 interessata.

Amazon Machine Images (AMI) con i risultati più critici

La sezione Amazon Machine Images (AMI) con i risultati più critici mostra le cinque AMI principali del tuo ambiente con i risultati più critici. La visualizzazione mostra l'identificatore AMI, l'identificatore dell' AWS account, il numero di istanze EC2 interessate in esecuzione nell'ambiente, la data di creazione dell'AMI, la piattaforma del sistema operativo dell'AMI, il numero di vulnerabilità critiche e il numero totale di vulnerabilità. Questa visualizzazione aiuta i proprietari dell'infrastruttura a identificare quali AMI potrebbero richiedere la ricostruzione.

Scegli Istanze interessate per visualizzare ulteriori informazioni sulle istanze avviate dall'AMI interessata.

AWS Lambda funzioni con i risultati più critici

La sezione AWS Lambda Funzioni con i risultati più critici mostra le cinque funzioni Lambda principali dell'ambiente con i risultati più critici. La vista mostra il nome della funzione Lambda, l'identificatore dell' AWS account, l'ambiente di runtime, il numero di vulnerabilità critiche, il numero di vulnerabilità elevate e il numero totale di vulnerabilità. Questa visualizzazione aiuta i proprietari dell'infrastruttura a identificare quali funzioni Lambda potrebbero richiedere una correzione.

Scegli il nome della funzione per visualizzare ulteriori informazioni sulla funzione interessata AWS Lambda .

Comprendere i risultati in Amazon Inspector

Un risultato è un rapporto dettagliato su una vulnerabilità che interessa una delle tue AWS risorse. I risultati prendono il nome dalle vulnerabilità rilevate e forniscono valutazioni di gravità, informazioni sulle risorse interessate e dettagli che descrivono come correggere le vulnerabilità segnalate.

Amazon Inspector genera un risultato ogni volta che rileva una vulnerabilità in un'istanza Amazon EC2, un'immagine di un contenitore in un repository Amazon ECR o una funzione. AWS Lambda Amazon Inspector analizza continuamente il tuo ambiente di elaborazione e archivia tutti i risultati attivi fino a quando non li correggi.

Quando correggi un risultato, il risultato viene automaticamente chiuso e Amazon Inspector lo elimina dopo 7 giorni. Quando elimini una risorsa, Amazon Inspector elimina qualsiasi risultato associato alla risorsa dopo 30 giorni.

Se disabiliti Amazon Inspector, i risultati vengono rimossi dopo 24 ore. Se AWS sospende il tuo account, i risultati vengono rimossi dopo 90 giorni.

I risultati sono classificati in uno dei seguenti stati:

Active (Attivo)

Amazon Inspector identifica i risultati che non sono stati corretti come attivi.

Soppresso

Amazon Inspector identifica come soppressi i risultati soggetti a una o più regole di soppressione. Puoi trovare i risultati soppressi nell'elenco dei risultati soppressi. Per ulteriori informazioni, consulta Eliminazione dei risultati di Amazon Inspector con regole di soppressione.

Closed

Dopo aver corretto una vulnerabilità, Amazon Inspector la rileva automaticamente e modifica lo stato del risultato in Chiuso. I risultati chiusi vengono eliminati dopo 7 giorni.

Argomenti

- Livelli di gravità per i risultati di Amazon Inspector

Ricerca dei tipi in Amazon Inspector

Amazon Inspector genera risultati per le istanze di Amazon Elastic Compute Cloud (Amazon EC2), immagini dei container nei repository Amazon Elastic Container Registry (Amazon ECR) e funzioni. AWS Lambda Amazon Inspector può generare i seguenti tipi di risultati.

Vulnerabilità del pacchetto

I risultati delle vulnerabilità dei pacchetti identificano i pacchetti software presenti nell' AWS ambiente che sono esposti a vulnerabilità ed esposizioni comuni (CVE). Gli aggressori possono sfruttare queste vulnerabilità prive di patch per compromettere la riservatezza, l'integrità o la disponibilità dei dati o per accedere ad altri sistemi. Il sistema CVE è un metodo di riferimento per vulnerabilità ed esposizioni alla sicurezza delle informazioni note pubblicamente. Per ulteriori informazioni, vedere https://www.cve.org/.

I rilevamenti CVE per Linux vengono aggiunti ad Amazon Inspector entro 24 ore dal rilascio tramite gli avvisi di sicurezza del fornitore. I rilevamenti CVE per Windows vengono aggiunti ad Amazon Inspector entro 48 ore dal rilascio da parte di Microsoft. Puoi usare il Ricerca nel database delle vulnerabilità di Amazon Inspector per verificare se un rilevamento CVE è supportato.

Amazon Inspector può generare rilevamenti di vulnerabilità dei pacchetti per istanze EC2, immagini di contenitori ECR e funzioni Lambda. I risultati delle vulnerabilità dei pacchetti contengono dettagli aggiuntivi esclusivi per questo tipo di risultati, ovvero il punteggio Inspector e l'intelligence sulle vulnerabilità.

Vulnerabilità del codice

I risultati delle vulnerabilità del codice identificano le righe del codice che gli aggressori potrebbero sfruttare. Le vulnerabilità del codice includono difetti di iniezione, fughe di dati, crittografia debole o crittografia mancante nel codice.

Amazon Inspector valuta il codice applicativo della funzione Lambda utilizzando il ragionamento automatico e l'apprendimento automatico che analizza il codice dell'applicazione per la conformità generale alla sicurezza. Identifica le violazioni delle politiche e le vulnerabilità sulla base di rilevatori interni sviluppati in collaborazione con Amazon. CodeGuru Per un elenco dei possibili rilevamenti, consulta Detector Library. CodeGuru

> **Important**
>
> La scansione del codice di Amazon Inspector acquisisce frammenti di codice per evidenziare le vulnerabilità rilevate. Questi frammenti possono mostrare credenziali codificate o altri materiali sensibili in testo non crittografato.

Amazon Inspector può generare risultati di vulnerabilità del codice per le funzioni Lambda, se sono state attivate. Scansione del codice Amazon Inspector Lambda

I frammenti di codice rilevati in relazione a una vulnerabilità del codice vengono archiviati dal servizio. CodeGuru Per impostazione predefinita, CodeGuru viene utilizzata una chiave di AWS proprietà controllata da per crittografare il codice, tuttavia, puoi utilizzare la tua chiave gestita dal cliente per la crittografia tramite l'API Amazon Inspector. Per ulteriori informazioni, consulta Crittografia inattiva per il codice contenuto nei tuoi risultati.

Raggiungibilità della rete

I risultati sulla raggiungibilità della rete indicano che nel tuo ambiente esistono percorsi di rete aperti verso le istanze Amazon EC2. Questi risultati appaiono quando le porte TCP e UDP sono raggiungibili dai bordi del VPC, come un gateway Internet (incluse le istanze di Application Load Balancer o Classic Load Balancer), una connessione peering VPC o una VPN tramite un gateway virtuale. Questi risultati evidenziano configurazioni di rete che potrebbero essere eccessivamente permissive, come gruppi di sicurezza mal gestiti, elenchi di controllo degli accessi o gateway Internet, o che potrebbero consentire accessi potenzialmente dannosi.

Amazon Inspector genera risultati sulla raggiungibilità della rete solo per le istanze Amazon EC2. Amazon Inspector esegue scansioni per individuare i risultati della raggiungibilità della rete ogni 24 ore.

Amazon Inspector valuta le seguenti configurazioni durante la scansione dei percorsi di rete:

- Istanze Amazon EC2
- AWS Lambda funzioni
- Application Load Balancer
- Direct Connect
- Elastic Load Balancer

- Interfacce di rete elastiche
- Internet Gateway
- Elenchi di controllo dell'accesso alla rete
- Tabelle di routing
- Gruppi di sicurezza
- Sottoreti
- Cloud privati virtuali
- Gateway privati virtuali
- Endpoint VPC
- Endpoint gateway VPC
- Connessioni in peering di VPC
- Connessioni VPN

Individuazione e visualizzazione dei risultati di Amazon Inspector

Le procedure in questa sezione descrivono come individuare e visualizzare i risultati in Amazon Inspector tramite la console e l'API Amazon Inspector. I dettagli di ricerca variano in base al tipo di ricerca, al tipo di vulnerabilità e alle risorse interessate. Per ulteriori informazioni, consulta Informazioni sulla ricerca di Amazon Inspector.

Console

Per visualizzare i risultati nella console

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Dal pannello di navigazione, scegli Findings. Verrai indirizzato a una schermata dei risultati in cui puoi visualizzare tutti i risultati. Nella tabella Risultati, puoi scegliere un risultato selezionando il nome del risultato nella colonna Titolo.
3. (Facoltativo) È inoltre possibile visualizzare i risultati raggruppati per categoria. Dal riquadro di navigazione, scegli Risultati, quindi scegli una delle seguenti categorie:
   - Per vulnerabilità
   - Per esempio

> **Note**
>
> I risultati raggruppati per istanza non includono informazioni sulla disponibilità della rete.

- Per immagine del contenitore
- Per repository di container
- Per funzione Lambda

API

Esegui l'operazione ListFindingsAPI. Nella richiesta, puoi specificare `filterCriteria`di restituire risultati specifici.

Informazioni sulla ricerca di Amazon Inspector

Nella console Amazon Inspector, puoi visualizzare i dettagli di ogni risultato. I dettagli di ricerca variano in base al tipo di ricerca.

Per visualizzare i dettagli di un risultato

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home
2. Seleziona la regione in cui visualizzare i risultati.
3. Nel riquadro di navigazione, scegli Risultati per visualizzare l'elenco dei risultati
4. (Facoltativo) Utilizzate la barra dei filtri per selezionare un risultato specifico. Per ulteriori informazioni, consulta Filtraggio dei risultati di Amazon Inspector.
5. Scegliete un risultato per visualizzarne il pannello dei dettagli.

Il pannello dei dettagli del risultato contiene le caratteristiche identificative di base del risultato. Ciò include il titolo della scoperta, una descrizione di base della vulnerabilità identificata, suggerimenti per la correzione e un punteggio di gravità. Per informazioni sul punteggio, vedere. Livelli di gravità per i risultati di Amazon Inspector

I dettagli disponibili per un risultato variano a seconda del tipo di risultato e della risorsa interessata.

Tutti i risultati contengono il numero Account AWS identificativo per cui è stato identificato il risultato, la gravità, il tipo di risultato, la data di creazione del risultato e una sezione relativa alla risorsa interessata con i dettagli sulla risorsa.

Il tipo di risultato determina le informazioni sulla correzione e sulle vulnerabilità disponibili per il risultato. A seconda del tipo di risultato, sono disponibili diversi dettagli di ricerca.

Vulnerabilità del pacchetto

I risultati delle vulnerabilità dei pacchetti sono disponibili per le istanze EC2, le immagini dei contenitori ECR e le funzioni Lambda. Per ulteriori informazioni, consulta Vulnerabilità del pacchetto.

I risultati delle vulnerabilità dei pacchetti includono Punteggio e informazioni sulle vulnerabilità di Amazon Inspector anche.

Questo tipo di risultato contiene i seguenti dettagli:

- Correzione disponibile: indica se la vulnerabilità è stata corretta in una versione più recente dei pacchetti interessati. Ha uno dei seguenti valori:
  - `YES`, il che significa che tutti i pacchetti interessati hanno una versione fissa.
  - `NO`, il che significa che nessun pacchetto interessato ha una versione fissa.
  - `PARTIAL`, il che significa che uno o più (ma non tutti) dei pacchetti interessati hanno una versione fissa.
- Exploit disponibile: indica che la vulnerabilità ha un exploit noto.
  - `YES`, il che significa che la vulnerabilità rilevata nell'ambiente in uso presenta un exploit noto. Amazon Inspector non ha visibilità sull'uso degli exploit in un ambiente.
  - `NO`, il che significa che questa vulnerabilità non ha un exploit noto.
- Pacchetti interessati: elenca ogni pacchetto identificato come vulnerabile nella ricerca e i dettagli di ogni pacchetto:
- Filepath: l'ID del volume EBS e il numero di partizione associati a un risultato. Questo campo è presente nei risultati relativi alle istanze EC2 scansionate utilizzando. Scansione senza agenti
- Versione installata/Versione fissa: il numero di versione del pacchetto attualmente installato per il quale è stata rilevata una vulnerabilità. Confronta il numero di versione installata con il valore dopo la barra (/). Il secondo valore è il numero di versione del pacchetto che corregge la vulnerabilità rilevata, come fornito dai Common Vulnerabilities and Exposures (CVE) o dall'avviso associato al risultato. Se la vulnerabilità è stata corretta in più versioni, questo

campo elenca la versione più recente che include la correzione. Se non è disponibile una correzione, questo valore è`None available`.

> **Note**
>
> Se è stato rilevato un risultato prima che Amazon Inspector iniziasse a includere questo campo nei risultati, il valore per questo campo è vuoto. Tuttavia, potrebbe essere disponibile una correzione.

- Package manager — Il gestore di pacchetti utilizzato per configurare questo pacchetto.
- Correzione: se è disponibile una correzione tramite un pacchetto o una libreria di programmazione aggiornati, questa sezione include i comandi che è possibile eseguire per effettuare l'aggiornamento. È possibile copiare il comando fornito ed eseguirlo nel proprio ambiente.

> **Note**
>
> I comandi di riparazione vengono forniti dai data feed del fornitore e possono variare in base alla configurazione del sistema. Per indicazioni più specifiche, consulta la sezione dedicata alla ricerca di riferimenti o alla documentazione del sistema operativo.

- Dettagli sulla vulnerabilità: fornisce un collegamento alla fonte preferita di Amazon Inspector per il CVE identificato nella scoperta, ad esempio National Vulnerability Database (NVD), REDHAT o un altro fornitore del sistema operativo. Inoltre, troverai i punteggi di gravità della scoperta. Per ulteriori informazioni sui punteggi di gravità, ad esempio, vedereLivelli di gravità per i risultati di Amazon Inspector. Sono inclusi i seguenti punteggi, inclusi i vettori di punteggio per ciascuno di essi:
  - Punteggio EPSS
  - Punteggio Inspector
  - CVSS 3.1 di Amazon CVE
  - CVSS 3.1 di NVD
  - CVSS 2.0 di NVD (ove applicabile, per i CVE più vecchi)
- Vulnerabilità correlate: specifica altre vulnerabilità relative alla scoperta. In genere si tratta di altri CVE che influiscono sulla stessa versione del pacchetto o di altri CVE all'interno dello stesso gruppo del CVE di ricerca, come determinato dal fornitore.

Vulnerabilità del codice

I risultati delle vulnerabilità del codice sono disponibili solo per le funzioni Lambda. Per ulteriori informazioni, consulta Vulnerabilità del codice. Questo tipo di risultato contiene i seguenti dettagli:

- Correzione disponibile: per le vulnerabilità del codice questo valore è sempre`YES`.
- Nome del rilevatore: il nome del CodeGuru rilevatore utilizzato per rilevare la vulnerabilità del codice. Per un elenco dei possibili rilevamenti, consulta la Detector Library. CodeGuru
- Tag del rilevatore: i CodeGuru tag associati al rilevatore CodeGuru utilizzano i tag per classificare i rilevamenti.
- CWE pertinenti: ID delle Common Weakness Enumeration (CWE) associate alla vulnerabilità del codice.
- Percorso del file: la posizione del file della vulnerabilità del codice.
- Posizione della vulnerabilità: per le vulnerabilità del codice di scansione Lambda, questo campo mostra le righe di codice esatte in cui Amazon Inspector ha rilevato la vulnerabilità.
- Correzione suggerita: suggerisce come modificare il codice per correggere il risultato.

Raggiungibilità della rete

I risultati sulla raggiungibilità della rete sono disponibili solo per le istanze EC2. Per ulteriori informazioni, consulta Raggiungibilità della rete. Questo tipo di risultato contiene i seguenti dettagli:

- Intervallo di porte aperto: l'intervallo di porte attraverso il quale è possibile accedere all'istanza EC2.
- Percorsi di rete aperti: mostra il percorso di accesso aperto all'istanza EC2. Seleziona un elemento sul percorso per ulteriori informazioni.
- Correzione: consiglia un metodo per chiudere il percorso di rete aperto.

Punteggio e informazioni sulle vulnerabilità di Amazon Inspector

Nella console Amazon Inspector, quando selezioni un risultato, puoi visualizzare la scheda Inspector score and vulnerability intelligence che mostra i dettagli del punteggio per l'individuazione della vulnerabilità di un pacchetto, nonché i dettagli di intelligence sulla vulnerabilità. Questi dettagli sono disponibili solo per i risultati. Vulnerabilità del pacchetto

Punteggio Amazon Inspector

Il punteggio Amazon Inspector è un punteggio contestualizzato che Amazon Inspector crea per ogni ricerca di istanze EC2. Il punteggio Amazon Inspector viene determinato correlando le informazioni sul punteggio CVSS v3.1 di base con le informazioni raccolte dall'ambiente di calcolo durante le scansioni, come i risultati di raggiungibilità della rete e i dati di sfruttabilità. Ad esempio, il punteggio Amazon Inspector di un risultato può essere inferiore al punteggio di base se la vulnerabilità è sfruttabile sulla rete, ma Amazon Inspector determina che nessun percorso di rete aperto verso l'istanza vulnerabile è disponibile da Internet.

Il punteggio di base per un risultato è il punteggio di base CVSS v3.1 fornito dal fornitore. I punteggi di base dei fornitori RHEL, Debian o Amazon sono supportati, per altri fornitori o nei casi in cui il fornitore non ha fornito un punteggio Amazon Inspector utilizza il punteggio di base del National Vulnerability Database (NVD). Amazon Inspector utilizza il calcolatore Common Vulnerability Scoring System versione 3.1 per calcolare il punteggio. Puoi vedere la fonte del punteggio di base di un singolo risultato nei dettagli del risultato, nella sezione Dettagli sulla vulnerabilità, come Fonte di vulnerabilità (o nel risultato JSON) packageVulnerabilityDetails.source

> **Note**
>
> Il punteggio di Amazon Inspector non è disponibile per le istanze Linux che eseguono Ubuntu. Questo perché Ubuntu definisce la propria gravità di vulnerabilità che può differire dalla gravità CVE associata.

Dettagli del punteggio Amazon Inspector

Quando apri la pagina dei dettagli di un risultato, puoi selezionare la scheda Inspector score and vulnerability intelligence. Questo pannello mostra la differenza tra il punteggio base e il punteggio Inspector. Questa sezione spiega come Amazon Inspector ha assegnato la classificazione di gravità in base a una combinazione del punteggio Amazon Inspector e del punteggio del fornitore per il pacchetto software. Se i punteggi sono diversi, questo pannello mostra una spiegazione del perché.

Nella sezione delle metriche del punteggio CVSS puoi vedere una tabella con i confronti tra le metriche del punteggio di base CVSS e il punteggio Inspector. Le metriche confrontate sono le metriche di base definite nel documento delle specifiche CVSS gestito da. first.org Di seguito è riportato un riepilogo delle metriche di base:

Vettore di attacco

Il contesto in base al quale una vulnerabilità può essere sfruttata. Per i risultati di Amazon Inspector, questi possono essere di rete, rete adiacente o locale.

Complessità dell'attacco

Questo descrive il livello di difficoltà che un utente malintenzionato dovrà affrontare quando sfrutta la vulnerabilità. Un punteggio basso significa che l'aggressore dovrà soddisfare poche o nessuna condizione aggiuntiva per sfruttare la vulnerabilità. Un punteggio elevato significa che un aggressore dovrà investire una notevole quantità di sforzi per portare a termine con successo un attacco con questa vulnerabilità.

Privilegi richiesti

Questo descrive il livello di privilegio di cui un utente malintenzionato avrà bisogno per sfruttare una vulnerabilità.

Interazione con l'utente

Questa metrica indica se un attacco riuscito che utilizza questa vulnerabilità richiede un utente umano diverso dall'aggressore.

Scope (Ambito)

Indica se una vulnerabilità in un componente vulnerabile influisce sulle risorse dei componenti che esulano dall'ambito di sicurezza del componente vulnerabile. Se questo valore è invariato, la risorsa interessata e la risorsa interessata sono le stesse. Se questo valore viene modificato, il componente vulnerabile può essere sfruttato per influire sulle risorse gestite da diverse autorità di sicurezza.

La riservatezza

Questo misura il livello di impatto sulla riservatezza dei dati all'interno di una risorsa quando la vulnerabilità viene sfruttata. Si va da Nessuno, dove non si perde la riservatezza, a Alto, dove tutte le informazioni all'interno di una risorsa vengono divulgate o possono essere divulgate informazioni riservate come password o chiavi di crittografia.

Integrità

Questo misura il livello di impatto sull'integrità dei dati all'interno della risorsa interessata se la vulnerabilità viene sfruttata. L'integrità è a rischio quando l'aggressore modifica i file all'interno delle risorse interessate. Il punteggio va da Nessuno, dove l'exploit non consente a un utente malintenzionato di modificare alcuna informazione, a Alto, dove, se sfruttata, la vulnerabilità

consentirebbe all'aggressore di modificare alcuni o tutti i file, oppure i file che potrebbero essere modificati avrebbero gravi conseguenze.

Disponibilità

Questo misura il livello di impatto sulla disponibilità della risorsa interessata quando la vulnerabilità viene sfruttata. Il punteggio va da Nessuno, quando la vulnerabilità non influisce affatto sulla disponibilità, a Alto, dove, se sfruttato, l'aggressore può negare completamente la disponibilità della risorsa o rendere indisponibile un servizio.

Informazioni sulla vulnerabilità

Questa sezione riassume le informazioni disponibili sul CVE di Amazon e le fonti di intelligence sulla sicurezza standard del settore come Recorded Future e Cybersecurity and Infrastructure Security Agency (CISA).

> **Note**
>
> Intel di CISA, Amazon o Recorded Future non sarà disponibile per tutti i CVE.

È possibile visualizzare i dettagli delle informazioni sulle vulnerabilità nella console o utilizzando l'API. BatchGetFindingDetails Nella console sono disponibili i seguenti dettagli:

ATT&CK

Questa sezione mostra le tattiche, le tecniche e le procedure (TTP) MITRE associate al CVE. Vengono visualizzati i TTP associati, se sono presenti più di due TTP applicabili è possibile selezionare il collegamento per visualizzare un elenco completo. La selezione di una tattica o di una tecnica apre informazioni al riguardo sul sito web MITRE.

CISA

Questa sezione copre le date rilevanti associate alla vulnerabilità. La data in cui la Cybersecurity and Infrastructure Security Agency (CISA) ha aggiunto la vulnerabilità al Known Exploited Vulnerabilities Catalog, sulla base delle prove di uno sfruttamento attivo, e la data di scadenza entro cui CISA prevede che i sistemi vengano corretti. Queste informazioni provengono dal CISA.

Malware noto

Questa sezione elenca i kit e gli strumenti di exploit noti che sfruttano questa vulnerabilità.

Evidenza

Questa sezione riassume gli eventi di sicurezza più critici che coinvolgono questa vulnerabilità. Se più di 3 eventi hanno lo stesso livello di criticità, vengono visualizzati i primi tre eventi più recenti.

Ultima volta segnalata

Questa sezione mostra la data dell'ultimo exploit pubblico noto per questa vulnerabilità.

Livelli di gravità per i risultati di Amazon Inspector

Quando Amazon Inspector genera una rilevazione di vulnerabilità, assegna automaticamente una gravità alla scoperta. La gravità di un rilevamento riflette le caratteristiche principali del risultato e può quindi aiutarti a valutare e dare priorità ai risultati. La gravità di un risultato non implica né indica in altro modo la criticità o l'importanza che una risorsa interessata potrebbe avere per l'organizzazione.

La classificazione di gravità di un risultato è determinata da un punteggio numerico che corrisponde a uno dei seguenti livelli di gravità: informativo, basso, medio, alto o critico.

Il metodo con cui Amazon Inspector determina la gravità varia in base al tipo di risultato. Consulta le seguenti sezioni per saperne di più su come Amazon Inspector determina la classificazione di gravità per ogni tipo di risultato.

Gravità della vulnerabilità dei pacchetti software

Amazon Inspector utilizza il punteggio NVD/CVSS come base per il punteggio di gravità per le vulnerabilità dei pacchetti software. Il punteggio NVD/CVSS è il punteggio di gravità delle vulnerabilità pubblicato da NVD e definito dal CVSS. Il punteggio NVD/CVSS è una composizione di metriche di sicurezza, come la complessità degli attacchi, la maturità del codice di exploit e i privilegi richiesti. Amazon Inspector produce un punteggio numerico da 1 a 10 che riflette la gravità della vulnerabilità. Amazon Inspector lo classifica come punteggio di base perché riflette la gravità di una vulnerabilità in base alle sue caratteristiche intrinseche, che sono costanti nel tempo. Questo punteggio presuppone anche l'impatto ragionevole nel peggiore dei casi su diversi ambienti distribuiti. Lo standard CVSS v3 associa i punteggi CVSS ai seguenti livelli di gravità.

Punteggio	Valutazione
0	Messaggio informativo
0,1—3,9	Bassa

4,0—6,9	Media
7,0—8,9	Elevata
9,0—10,0	Critico

Le vulnerabilità rilevate nei pacchetti possono anche avere una gravità pari a Untriaged. Ciò significa che il fornitore non ha ancora impostato un punteggio di vulnerabilità per la vulnerabilità rilevata. In questo caso, consigliamo di utilizzare gli URL di riferimento relativi alla scoperta per ricercare la vulnerabilità e rispondere di conseguenza.

I risultati delle vulnerabilità dei pacchetti includono i seguenti punteggi e i vettori di punteggio associati come parte dei dettagli dei risultati:

- Punteggio EPSS
- Punteggio Inspector
- CVSS 3.1 di Amazon CVE
- CVSS 3.1 di NVD
- CVSS 2.0 da NVD (dove applicabile)

Gravità della vulnerabilità del codice

Per rilevare le vulnerabilità del codice, Amazon Inspector utilizza i livelli di gravità definiti dai rilevatori CodeGuru Amazon che hanno generato il risultato. A ciascun rilevatore viene assegnata una gravità utilizzando il sistema di punteggio CVSS v3. Per una spiegazione degli CodeGuru usi delle severità, consulta le definizioni di gravità nella guida. CodeGuru Per un elenco dei rilevatori in base alla gravità, seleziona uno dei linguaggi di programmazione supportati di seguito:

- Rilevatori Python per gravità
- Rilevatori Java per gravità

Severità della raggiungibilità della rete

Amazon Inspector determina la gravità di una vulnerabilità di raggiungibilità della rete in base al servizio, alle porte e ai protocolli esposti e al tipo di percorso aperto. La tabella seguente definisce

questi livelli di gravità. Il valore nella colonna Open path rating rappresenta i percorsi aperti provenienti da gateway virtuali, VPC peer e reti. AWS Direct Connect Tutti gli altri servizi, porte e protocolli esposti hanno una classificazione di gravità informativa.

Servizio	Porte TCP	Porte UDP	Valutazione del percorso Internet	Classificazione del percorso aperto
DHCP	67, 68, 546, 547	67, 68, 546, 547	Media	Messaggio informativo
Elasticsearch	9300, 9200	N/A	Media	Messaggio informativo
FTP	21	21	Elevata	Media
Global catalog LDAP	3268	N/A	Media	Messaggio informativo
Global catalog LDAP over TLS	3269	N/A	Media	Messaggio informativo
HTTP	80	80	Bassa	Messaggio informativo
HTTPS	443	443	Bassa	Messaggio informativo
Kerberos	88, 464, 543, 544, 749, 751	88, 464, 749, 750, 751, 752	Media	Messaggio informativo
LDAP	389	389	Media	Messaggio informativo
LDAP over TLS	636	N/A	Media	Messaggio informativo
MongoDB	27017, 27018, 27019, 28017	N/A	Media	Messaggio informativo

MySQL	3306	N/A	Media	Messaggio informativo
NetBIOS	137, 139	137, 138	Media	Messaggio informativo
NFS	111, 2049, 4045, 1110	111, 2049, 4045, 1110	Media	Messaggio informativo
Oracle	1521, 1630	N/A	Media	Messaggio informativo
PostgreSQL	5432	N/A	Media	Messaggio informativo
Servizi di stampa	515	N/A	Elevata	Media
RDP	3389	3389	Media	Bassa
RPC	111, 135, 530	111, 135, 530	Media	Messaggio informativo
SMB	445	445	Media	Messaggio informativo
SSH	22	22	Media	Bassa
SQL Server	1433	1434	Media	Messaggio informativo
Syslog	601	514	Media	Messaggio informativo
Telnet	23	23	Elevata	Media
WINS	1512, 42	1512, 42	Media	Messaggio informativo

Gestione dei risultati in Amazon Inspector

Amazon Inspector offre diversi modi per ordinare, raggruppare e gestire i risultati. Queste funzionalità ti aiutano a personalizzare i risultati in base al tuo ambiente, ad aggregare i risultati in base a diverse visualizzazioni e a concentrarti sulle vulnerabilità del tuo ambiente specifico. AWS

I risultati vengono visualizzati in varie visualizzazioni in base al loro stato: attivo, soppresso o chiuso. Per impostazione predefinita, ogni visualizzazione mostra solo i risultati attivi. Un risultato attivo rappresenta un potenziale problema di sicurezza rilevato da Amazon Inspector che indica una vulnerabilità o una potenziale minaccia. I risultati soppressi sono risultati attivi che hai escluso utilizzando regole di soppressione. Amazon Inspector imposta automaticamente lo stato di un risultato su Chiuso quando rileva che il risultato è stato risolto. I risultati non vengono chiusi manualmente.

È inoltre possibile visualizzare i risultati in AWS Security Hub, un servizio che fornisce una visione completa dello stato di sicurezza in tutto l' AWS ambiente. Per ulteriori informazioni, consulta Integrazione di Amazon Inspector con AWS Security Hub. I risultati delle immagini dei container sono disponibili anche nella console Amazon ECR e puoi visualizzare i risultati per tutte le risorse utilizzando AWS Command Line Interface (AWS CLI) o l'API.

Argomenti

Visualizzazione dei risultati di Amazon Inspector

La console Amazon Inspector mostra i risultati in visualizzazioni a schede basate su raggruppamenti correlati. Ogni visualizzazione include informazioni che possono aiutarti ad analizzare vulnerabilità specifiche, identificare le risorse più vulnerabili e valutare l'impatto complessivo delle vulnerabilità nel tuo ambiente. Puoi passare a una visualizzazione di ricerca diversa scegliendo un'opzione nel pannello laterale di navigazione Findings. Puoi anche creare un filtro in ogni vista per concentrarti su tipi specifici di risultati. Per ulteriori informazioni sull'uso dei filtri, vedi Filtraggio dei risultati di Amazon Inspector.

I risultati possono essere raggruppati in base ai seguenti parametri:

- Per vulnerabilità: elenca le vulnerabilità più critiche rilevate nell'ambiente. Scegli un titolo di vulnerabilità da questa visualizzazione per aprire un riquadro dei dettagli con informazioni aggiuntive.
- Per account: elenca i tuoi account, la percentuale di copertura di scansione di Amazon Inspector per ogni account e il numero totale di risultati critici e di elevata gravità per ogni account. Questo raggruppamento è disponibile solo per gli amministratori delegati.
- Per istanza: elenca le istanze Amazon EC2 più vulnerabili nel tuo ambiente.
- Per immagine del contenitore: elenca le immagini dei container Amazon ECR più vulnerabili nel tuo ambiente.
- Per repository di container: mostra i repository con il maggior numero di vulnerabilità.
- Per funzione Lambda: mostra le funzioni Lambda con il maggior numero di vulnerabilità.
- Tutti i risultati: mostra un elenco completo dei risultati relativi all'ambiente in uso. Questa è la visualizzazione predefinita quando si accede alla pagina Risultati. In questa visualizzazione puoi filtrare per risultati attivi, soppressi e chiusi.

È possibile creare regole di soppressione basate su filtri per escludere i risultati dalle viste dei risultati. Per ulteriori informazioni, consulta Eliminazione dei risultati di Amazon Inspector con regole di soppressione.

Filtraggio dei risultati di Amazon Inspector

Un filtro di ricerca ti consente di visualizzare solo i risultati che corrispondono ai criteri specificati. I risultati che non corrispondono ai criteri di filtro vengono esclusi dalla visualizzazione. Puoi creare filtri di ricerca utilizzando la console Amazon Inspector. Per utilizzare questi filtri per sopprimere automaticamente i risultati esistenti e futuri, vedereEliminazione dei risultati di Amazon Inspector con regole di soppressione.

Creazione di filtri nella console Amazon Inspector

In ogni visualizzazione dei risultati, puoi utilizzare la funzionalità di filtro per individuare i risultati con caratteristiche specifiche. I filtri vengono rimossi quando si passa a una visualizzazione a schede diversa.

Un filtro è costituito da un criterio di filtro, che consiste in un attributo di filtro abbinato a un valore di filtro. I risultati che non corrispondono ai criteri di filtro impostati vengono esclusi dall'elenco dei

risultati. Ad esempio, per visualizzare tutti i risultati associati al tuo account amministratore, puoi scegliere l'attributo ID dell' AWS account e associarlo al valore dell'ID dell' AWS account a dodici cifre.

Alcuni criteri di filtro si applicano a tutti i risultati, mentre altri sono disponibili solo per tipi di risorse specifici o per tipi di ricerca.

Per applicare un filtro alla visualizzazione dei risultati

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Nel riquadro di navigazione, seleziona Esiti. La visualizzazione predefinita mostra tutti i risultati con uno stato Attivo.
3. Per filtrare i risultati in base a criteri, seleziona la barra Aggiungi filtro per visualizzare un elenco di tutti i criteri di filtro applicabili per quella vista. Sono disponibili criteri di filtro diversi in diverse visualizzazioni.
4. Scegliete un criterio in base al quale filtrare dall'elenco.
5. Dal riquadro di immissione del criterio, immettete i valori del filtro desiderati per definire tale criterio.
6. Scegliete Applica per applicare quel criterio di filtro ai risultati correnti. Puoi continuare ad aggiungere altri criteri di filtro selezionando nuovamente la barra di immissione del filtro.
7. (Facoltativo) Per visualizzare i risultati soppressi o chiusi, scegliete Attivo nella barra dei filtri, quindi scegliete Soppressi o Chiusi. Scegli Mostra tutto per visualizzare i risultati attivi, soppressi e chiusi nella stessa visualizzazione.

Eliminazione dei risultati di Amazon Inspector con regole di soppressione

Utilizza le regole di soppressione per escludere i risultati che corrispondono ai criteri. Ad esempio, puoi creare una regola che sopprima tutti i risultati con punteggi di vulnerabilità bassi, in modo da poterti concentrare solo sui risultati più critici.

> **Note**
>
> Le regole di soppressione vengono utilizzate solo per filtrare l'elenco dei risultati e non hanno alcun impatto sui risultati né impediscono ad Amazon Inspector di generare risultati.

Se Amazon Inspector genera risultati che corrispondono a una regola di soppressione, i risultati vengono impostati su Eliminati. Per impostazione predefinita, i risultati che corrispondono a una regola di soppressione non vengono visualizzati nell'elenco.

Amazon Inspector archivia i risultati soppressi fino a quando non vengono corretti. Amazon Inspector rileva i risultati corretti. Quando Amazon Inspector rileva un risultato corretto, lo imposta su Closed e lo archivia per 7 giorni.

I risultati soppressi vengono pubblicati su AWS Security Hub e Amazon EventBridge come eventi. È possibile eliminare automaticamente i risultati indesiderati in Security Hub modificando lo stato dei risultati utilizzando una EventBridge regola. Per ulteriori informazioni, consulta Come creare regole di soppressione automatica in. AWS Security Hub

Non è possibile creare una regola di soppressione che chiuda o corregga i risultati. È possibile creare una regola di soppressione solo per filtrare i risultati visualizzati nell'elenco. Puoi visualizzare i risultati soppressi in qualsiasi momento nella console Amazon Inspector.

> **Note**
>
> Gli account dei membri di un'organizzazione non possono creare o gestire regole di soppressione.

Creazione di una regola di soppressione

È possibile creare regole di soppressione per filtrare l'elenco dei risultati visualizzati per impostazione predefinita. È possibile creare una regola di soppressione a livello di codice utilizzando l'CreateFilterAPI e specificando `SUPRESS` come valore per. `action`

> **Note**
>
> Solo gli account autonomi e gli amministratori delegati di Amazon Inspector possono creare e gestire regole di soppressione. I membri di un'organizzazione non vedranno l'opzione per le regole di soppressione nel pannello di navigazione.

Per creare una regola di soppressione (console)

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Nel pannello di navigazione, scegli Regole di soppressione. Quindi scegli Create rule (Crea regola).
3. Per ogni criterio, effettuate le seguenti operazioni:
   - Seleziona la barra dei filtri per visualizzare un elenco di criteri di filtro che puoi aggiungere alla regola di soppressione.
   - Seleziona i criteri di filtro per la tua regola di soppressione.
4. Dopo aver aggiunto i criteri, inserite un nome per la regola e una descrizione facoltativa.
5. Scegli Salva regola. Amazon Inspector applica immediatamente la nuova regola di soppressione e nasconde tutti i risultati che corrispondono ai criteri.

Visualizzazione dei risultati soppressi

Per impostazione predefinita, Amazon Inspector non visualizza i risultati soppressi nella console Amazon Inspector. Tuttavia, puoi visualizzare i risultati soppressi da una regola particolare.

Per visualizzare i risultati soppressi

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Nel riquadro di navigazione, seleziona Regole di soppressione.
3. Nell'elenco delle regole di soppressione, seleziona il titolo della regola.

Modifica delle regole di soppressione

È possibile apportare modifiche alle regole di soppressione in qualsiasi momento.

Per modificare le regole di soppressione

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home
2. Nel riquadro di navigazione, seleziona Regole di soppressione.
3. Seleziona il titolo della regola di soppressione che desideri modificare.
4. Apportate le modifiche desiderate, quindi scegliete Salva per aggiornare la regola.

Eliminazione delle regole di soppressione

È possibile eliminare le regole di soppressione. Se elimini una regola di soppressione, Amazon Inspector smette di sopprimere le occorrenze nuove ed esistenti di risultati che soddisfano i criteri della regola e che non sono soppressi da altre regole.

Dopo aver eliminato una regola di soppressione, le occorrenze di risultati nuove ed esistenti che soddisfacevano i criteri della regola hanno lo stato Attivo. Ciò significa che vengono visualizzati per impostazione predefinita sulla console Amazon Inspector. Inoltre, Amazon Inspector pubblica questi risultati su AWS Security Hub e Amazon EventBridge come eventi.

Per eliminare una regola di soppressione

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Nel riquadro di navigazione, seleziona Regole di soppressione.
3. Seleziona la casella di controllo accanto al titolo della regola di soppressione che desideri eliminare.
4. Scegliete Elimina, quindi confermate la scelta di eliminare definitivamente la regola.

Esportazione dei report dei risultati da Amazon Inspector

Oltre a inviare i risultati ad Amazon EventBridge AWS Security Hub, puoi facoltativamente esportare i risultati in un bucket Amazon Simple Storage Service (Amazon S3) come rapporto sui risultati. Un rapporto sui risultati è un file CSV o JSON che contiene i dettagli dei risultati che scegli di includere

nel rapporto. Fornisce un'istantanea dettagliata dei risultati in un momento specifico. Per ogni risultato, il file include dettagli come l'Amazon Resource Name (ARN) della risorsa interessata, la data e l'ora di creazione del risultato, l'ID Common Vulnerabilities and Exposures (CVE) associato, la gravità, lo stato e i punteggi Amazon Inspector e CVSS del risultato.

Quando configuri un report sui risultati, inizi specificando quali risultati includere nel rapporto. Per impostazione predefinita, Amazon Inspector include i dati per tutte le tue scoperte nel sistema corrente Regione AWS che hanno lo stato di Attivo. Se sei l'amministratore delegato di Amazon Inspector di un'organizzazione, questo include i dati relativi ai risultati di tutti gli account membri della tua organizzazione.

Facoltativamente, puoi personalizzare un report filtrando i dati. Con i filtri, puoi includere o escludere i dati per i risultati con caratteristiche specifiche, ad esempio tutti i risultati critici creati in un intervallo di tempo specifico, tutti i risultati attivi per una particolare risorsa o tutti i risultati critici di un tipo specifico. Se sei l'amministratore di Amazon Inspector di un'organizzazione, puoi utilizzare i filtri per creare un report che includa i risultati relativi Account AWS a uno specifico elemento dell'organizzazione, ad esempio tutti i risultati critici di un account con stato Attivo e per i quali è disponibile una correzione. Puoi quindi condividere il rapporto con il proprietario dell'account per porvi rimedio.

> **Note**
>
> Quando esporti un rapporto sui risultati utilizzando l'CreateFindingsReportAPI, per impostazione predefinita vedrai solo i risultati attivi. Per visualizzare i risultati soppressi o chiusi, devi specificare `SUPPRESSED` o `CLOSED` come valori per i criteri del filtro FindingStatus.

Quando esporti un report sui risultati, Amazon Inspector crittografa i dati con una chiave AWS Key Management Service (AWS KMS) specificata e aggiunge il report a un bucket S3 da te specificato. La chiave di crittografia deve essere una chiave di crittografia AWS Key Management Service (AWS KMS) simmetrica gestita dal cliente e inclusa nella versione corrente. Regione AWS Inoltre, la politica chiave deve consentire ad Amazon Inspector di utilizzare la chiave. Il bucket S3 deve inoltre trovarsi nella regione corrente e la politica del bucket deve consentire ad Amazon Inspector di aggiungere oggetti al bucket.

Dopo che Amazon Inspector ha completato la crittografia e l'archiviazione del report, puoi scaricare il report dal bucket S3 specificato o spostarlo in un'altra posizione. In alternativa, puoi conservare

il report nello stesso bucket S3 e utilizzarlo come repository per i report sui risultati da esportare successivamente.

Questo argomento ti guida attraverso il processo di utilizzo di AWS Management Console per esportare un rapporto sui risultati. Il processo consiste nella verifica di disporre delle autorizzazioni necessarie, nella configurazione delle risorse necessarie e quindi nella configurazione ed esportazione del rapporto.

> **Note**
>
> È possibile esportare un solo rapporto sui risultati alla volta. Se è attualmente in corso un'esportazione, attendi il completamento dell'esportazione prima di provare a esportare un altro rapporto.

Attività

- Passaggio 1: verifica le autorizzazioni
- Passaggio 2: configura un bucket S3
- Fase 3: Configurare un AWS KMS key
- Fase 4: Configurare ed esportare un rapporto sui risultati
- Risolvi gli errori di esportazione

Dopo aver esportato un rapporto sui risultati per la prima volta, i passaggi da 1 a 3 possono essere facoltativi. Ciò dipende principalmente dal fatto che desideri utilizzare lo stesso bucket S3 e AWS KMS key per i report successivi.

Se preferisci esportare un report a livello di codice dopo i passaggi 1-3, utilizza il CreateFindingsReportfunzionamento dell'API Amazon Inspector.

Passaggio 1: verifica le autorizzazioni

Prima di esportare un report sui risultati da Amazon Inspector, verifica di disporre delle autorizzazioni necessarie sia per esportare i report sui risultati sia per configurare le risorse per la crittografia e l'archiviazione dei report. Per verificare le tue autorizzazioni, utilizza AWS Identity and Access Management (IAM) per rivedere le policy IAM associate alla tua identità IAM. Quindi confronta le informazioni contenute in tali policy con il seguente elenco di azioni che devi essere autorizzato a eseguire per esportare un rapporto sui risultati.

Amazon Inspector

Per Amazon Inspector, verifica di essere autorizzato a eseguire le seguenti azioni:

- `inspector2:ListFindings`
- `inspector2:CreateFindingsReport`

Queste azioni ti consentono di recuperare i dati dei risultati per il tuo account e di esportare tali dati nei report sui risultati.

Se prevedi di esportare report di grandi dimensioni a livello di codice, potresti anche verificare di essere autorizzato a eseguire le seguenti azioni: `inspector2:GetFindingsReportStatus` controllare lo stato dei report e `inspector2:CancelFindingsReport` annullare le esportazioni in corso.

AWS KMS

Verifica AWS KMS, infatti, di avere il permesso di eseguire le seguenti azioni:

- `kms:GetKeyPolicy`
- `kms:PutKeyPolicy`

Queste azioni ti consentono di recuperare e aggiornare la policy chiave AWS KMS key che desideri che Amazon Inspector utilizzi per crittografare il report.

Per utilizzare la console Amazon Inspector per esportare un report, verifica anche di essere autorizzato a eseguire le seguenti AWS KMS azioni:

- `kms:DescribeKey`
- `kms:ListAliases`

Queste azioni ti consentono di recuperare e visualizzare informazioni AWS KMS keys relative al tuo account. Puoi quindi scegliere una di queste chiavi per crittografare il rapporto.

Se intendi creare una nuova chiave KMS per la crittografia del rapporto, devi anche essere autorizzato a eseguire l'`kms:CreateKey`azione.

Amazon S3

Per Amazon S3, verifica di essere autorizzato a eseguire le seguenti azioni:

- `s3:CreateBucket`
- `s3:DeleteObject`

- `s3:PutBucketAcl`
- `s3:PutBucketPolicy`
- `s3:PutBucketPublicAccessBlock`
- `s3:PutObject`
- `s3:PutObjectAcl`

  Queste azioni ti consentono di creare e configurare il bucket S3 in cui desideri che Amazon Inspector memorizzi il report. Consentono inoltre di aggiungere ed eliminare oggetti dal bucket.

  Se prevedi di utilizzare la console Amazon Inspector per esportare il report, verifica anche di avere il permesso di eseguire le azioni `s3:ListAllMyBuckets` e`s3:GetBucketLocation`. Queste azioni ti consentono di recuperare e visualizzare informazioni sui bucket S3 del tuo account. Puoi quindi scegliere uno di questi bucket per archiviare il rapporto.

Se non sei autorizzato a eseguire una o più delle azioni richieste, chiedi assistenza AWS all'amministratore prima di procedere al passaggio successivo.

Passaggio 2: configura un bucket S3

Dopo aver verificato le autorizzazioni, sei pronto per configurare il bucket S3 in cui desideri archiviare il rapporto sui risultati. Può essere un bucket esistente per il tuo account o un bucket esistente di proprietà di un altro Account AWS a cui puoi accedere. Se desideri archiviare il rapporto in un nuovo bucket, crea il bucket prima di procedere.

Il bucket S3 deve trovarsi nella Regione AWS stessa cartella dei risultati che desideri esportare. Ad esempio, se utilizzi Amazon Inspector nella regione Stati Uniti orientali (Virginia settentrionale) e desideri esportare i dati dei risultati per quella regione, il bucket deve trovarsi anche nella regione Stati Uniti orientali (Virginia settentrionale).

Inoltre, la politica del bucket deve consentire ad Amazon Inspector di aggiungere oggetti al bucket. Questo argomento spiega come aggiornare la policy del bucket e fornisce un esempio della dichiarazione da aggiungere alla policy. Per informazioni dettagliate sull'aggiunta e l'aggiornamento delle policy dei bucket, consulta Using bucket policies nella Amazon Simple Storage Service User Guide.

Se desideri archiviare il report in un bucket S3 di proprietà di un altro account, contatta il proprietario del bucket per aggiornare la policy del bucket. Ottieni anche l'URI per il bucket. Dovrai inserire questo URI quando esporti il rapporto.

Per aggiornare la policy sui bucket

1. Apri la console Amazon S3 all'indirizzo https://console.aws.amazon.com/s3.
2. Nel pannello di navigazione, scegli Bucket.
3. Scegli il bucket S3 in cui desideri archiviare il report dei risultati.
4. Scegli la scheda Autorizzazioni.
5. Seleziona Modifica nella sezione Policy bucket.
6. Copia la seguente dichiarazione di esempio negli appunti:

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "allow-inspector",
   "Effect": "Allow",
   "Principal": {
    "Service": "inspector2.amazonaws.com"
   },
   "Action": [
    "s3:PutObject",
    "s3:PutObjectAcl",
    "s3:AbortMultipartUpload"
   ],
   "Resource": "arn:aws:s3:::DOC-EXAMPLE-BUCKET/*",
   "Condition": {
    "StringEquals": {
     "aws:SourceAccount": "111122223333"
    },
    "ArnLike": {
     "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
    }
   }
  }
 ]
}
```

7. Nell'editor di policy Bucket sulla console Amazon S3, incolla l'istruzione precedente nella policy per aggiungerla alla policy.

Quando aggiungi l'istruzione, assicurati che la sintassi sia valida. Le policy Bucket utilizzano il formato JSON. Ciò significa che è necessario aggiungere una virgola prima o dopo l'istruzione, a seconda di dove si aggiunge l'istruzione alla politica. Se aggiungete l'istruzione come ultima istruzione, aggiungete una virgola dopo la parentesi di chiusura dell'istruzione precedente. Se la aggiungete come prima istruzione o tra due istruzioni esistenti, aggiungete una virgola dopo la parentesi che chiude l'istruzione.

8. Aggiorna l'istruzione con i valori corretti per il tuo ambiente, dove:

   - *DOC-EXAMPLE-BUCKET è il nome del bucket*.
   - *111122223333* è l'ID dell'account per il tuo. Account AWS
   - La *regione* è la regione Regione AWS in cui utilizzi Amazon Inspector e desideri consentire ad Amazon Inspector di aggiungere report al bucket. Ad esempio, `us-east-1` per la regione Stati Uniti orientali (Virginia settentrionale).

   > **Note**
   >
   > Se utilizzi Amazon Inspector in modalità abilitata manualmente Regione AWS, aggiungi anche il codice regionale appropriato al valore del campo. `Service` Questo campo specifica il principale del servizio Amazon Inspector.
   > Ad esempio, se utilizzi Amazon Inspector nella regione del Medio Oriente (Bahrain), che ha il codice regionaleme-`south-1`, sostituiscilo `inspector2.amazonaws.com` con `inspector2.me-south-1.amazonaws.com` nell'istruzione.

   Tieni presente che l'istruzione di esempio definisce condizioni che utilizzano due chiavi di condizione globali IAM:

   - aws: SourceAccount — Questa condizione consente ad Amazon Inspector di aggiungere report al bucket solo per il tuo account. Impedisce ad Amazon Inspector di aggiungere report per altri account. Più specificamente, la condizione specifica quale account può utilizzare il bucket per le risorse e le azioni specificate dalla condizione. `aws:SourceArn`

     Per archiviare i report relativi ad account aggiuntivi nel bucket, aggiungi l'ID account per ogni account aggiuntivo a questa condizione. Per esempio:

```
"aws:SourceAccount": [111122223333,444455556666,123456789012]
```

- aws: SourceArn — Questa condizione limita l'accesso al bucket in base alla fonte degli oggetti che vengono aggiunti al bucket. Impedisce ad altri Servizi AWS di aggiungere oggetti al bucket. Inoltre, impedisce ad Amazon Inspector di aggiungere oggetti al bucket mentre esegue altre azioni per il tuo account. Più specificamente, la condizione consente ad Amazon Inspector di aggiungere oggetti al bucket solo se si tratta di report sui risultati e solo se tali report vengono creati dall'account e nella regione specificata nella condizione.

  Per consentire ad Amazon Inspector di eseguire le azioni specificate per account aggiuntivi, aggiungi Amazon Resource Names (ARN) per ogni account aggiuntivo a questa condizione. Per esempio:

```
"aws:SourceArn": [
    "arn:aws:inspector2:Region:111122223333:report/*",
    "arn:aws:inspector2:Region:444455556666:report/*",
    "arn:aws:inspector2:Region:123456789012:report/*"
]
```

  Gli account specificati dalle `aws:SourceArn` condizioni `aws:SourceAccount` e devono corrispondere.

Entrambe le condizioni aiutano a evitare che Amazon Inspector venga usato come sostituto confuso durante le transazioni con Amazon S3. Sebbene non sia consigliabile, puoi rimuovere queste condizioni dalla bucket policy.

9. Al termine dell'aggiornamento della policy del bucket, scegli Salva modifiche.

Fase 3: Configurare un AWS KMS key

Dopo aver verificato le autorizzazioni e configurato il bucket S3, stabilisci quale AWS KMS key vuoi che Amazon Inspector utilizzi per crittografare il report dei risultati. La chiave deve essere una chiave KMS di crittografia simmetrica gestita dal cliente. Inoltre, la chiave deve trovarsi nello stesso Regione AWS bucket S3 configurato per archiviare il report.

La chiave può essere una chiave KMS esistente del tuo account o una chiave KMS esistente di proprietà di un altro account. Se desideri utilizzare una nuova chiave KMS, crea la chiave prima di procedere. Se desideri utilizzare una chiave esistente di proprietà di un altro account, ottieni l'Amazon

Resource Name (ARN) della chiave. Dovrai inserire questo ARN quando esporti il report da Amazon Inspector. Per informazioni sulla creazione e la revisione delle impostazioni per le chiavi KMS, consulta Managing keys nella Developer Guide.AWS Key Management Service

Dopo aver determinato quale chiave KMS desideri utilizzare, autorizza Amazon Inspector a utilizzare la chiave. In caso contrario, Amazon Inspector non sarà in grado di crittografare ed esportare il report. Per autorizzare Amazon Inspector a utilizzare la chiave, aggiorna la policy relativa alla chiave. Per informazioni dettagliate sulle politiche chiave e sulla gestione dell'accesso alle chiavi KMS, consulta le politiche chiave AWS KMS nella Guida per gli AWS Key Management Service sviluppatori.

Per aggiornare la politica chiave

> **Note**
>
> La procedura seguente serve per aggiornare una chiave esistente per consentire ad Amazon Inspector di utilizzarla. Se non disponi già di una chiave, consulta https://docs.aws.amazon.com/kms/latest/developerguide/create-keys.html le indicazioni su come crearne una.

1. Apri la AWS KMS console all'indirizzo https://console.aws.amazon.com/kms.
2. Per modificare la Regione AWS, usa il selettore della regione nell'angolo superiore destro della pagina.
3. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
4. Scegli la chiave KMS che desideri utilizzare per crittografare il rapporto. La chiave deve essere una chiave di crittografia simmetrica (SYMMETRIC_DEFAULT).
5. Nella scheda Politica chiave, scegliete Modifica. Se non vedi una politica chiave con il pulsante Modifica, devi prima selezionare Passa alla visualizzazione della politica.
6. Copia la seguente dichiarazione di esempio negli appunti:

```
{
    "Sid": "Allow Amazon Inspector to use the key",
    "Effect": "Allow",
    "Principal": {
        "Service": "inspector2.amazonaws.com"
    },
    "Action": [
        "kms:Decrypt",
```

```
            "kms:GenerateDataKey*"
        ],
        "Resource": "*",
        "Condition": {
            "StringEquals": {
                "aws:SourceAccount": "111122223333"
            },
            "ArnLike": {
                "aws:SourceArn": "arn:aws:inspector2:Region:111122223333:report/*"
            }
        }
}
```

7. Nell'editor Key policy sulla AWS KMS console, incolla l'istruzione precedente nella policy chiave per aggiungerla alla policy.

   Quando aggiungi l'istruzione, assicurati che la sintassi sia valida. Le politiche chiave utilizzano il formato JSON. Ciò significa che è necessario aggiungere una virgola prima o dopo l'istruzione, a seconda di dove si aggiunge l'istruzione alla politica. Se aggiungete l'istruzione come ultima istruzione, aggiungete una virgola dopo la parentesi di chiusura dell'istruzione precedente. Se la aggiungete come prima istruzione o tra due istruzioni esistenti, aggiungete una virgola dopo la parentesi che chiude l'istruzione.

8. Aggiorna l'istruzione con i valori corretti per il tuo ambiente, dove:

   - *111122223333* è l'ID dell'account per il tuo. Account AWS
   - La *regione* è la regione Regione AWS in cui desideri consentire ad Amazon Inspector di crittografare i report con la chiave. Ad esempio, `us-east-1` per la regione Stati Uniti orientali (Virginia settentrionale).

   > **Note**
   >
   > Se utilizzi Amazon Inspector in modalità abilitata manualmente Regione AWS, aggiungi anche il codice regionale appropriato al valore del campo. `Service` Ad esempio, se utilizzi Amazon Inspector nella regione del Medio Oriente (Bahrain), sostituiscilo con. `inspector2.amazonaws.com` `inspector2.me-south-1.amazonaws.com`

   Come l'istruzione di esempio per la bucket policy nel passaggio precedente, i `Condition` campi di questo esempio utilizzano due chiavi di condizione globali IAM:

- aws: SourceAccount — Questa condizione consente ad Amazon Inspector di eseguire le azioni specificate solo per il tuo account. Più specificamente, determina quale account può eseguire le azioni specificate per le risorse e le azioni specificate dalla `aws:SourceArn` condizione.

  Per consentire ad Amazon Inspector di eseguire le azioni specificate per account aggiuntivi, aggiungi l'ID account per ogni account aggiuntivo a questa condizione. Per esempio:

  ```
  "aws:SourceAccount": [111122223333,444455556666,123456789012]
  ```

- aws: SourceArn — Questa condizione Servizi AWS impedisce ad altri di eseguire le azioni specificate. Inoltre, impedisce ad Amazon Inspector di utilizzare la chiave mentre esegue altre azioni per il tuo account. In altre parole, consente ad Amazon Inspector di crittografare gli oggetti S3 con la chiave solo se si tratta di report sui risultati e solo se tali report vengono creati dall'account e nella regione specificata nella condizione.

  Per consentire ad Amazon Inspector di eseguire le azioni specificate per account aggiuntivi, aggiungi gli ARN per ogni account aggiuntivo a questa condizione. Per esempio:

  ```
  "aws:SourceArn": [
      "arn:aws:inspector2:us-east-1:111122223333:report/*",
      "arn:aws:inspector2:us-east-1:444455556666:report/*",
      "arn:aws:inspector2:us-east-1:123456789012:report/*"
  ]
  ```

  Gli account specificati dalle `aws:SourceArn` condizioni `aws:SourceAccount` e devono corrispondere.

  Queste condizioni aiutano a evitare che Amazon Inspector venga usato come assistente confuso durante le transazioni con. AWS KMS Sebbene non sia consigliabile, puoi rimuovere queste condizioni dall'informativa.

9. Al termine dell'aggiornamento della politica chiave, scegli Salva modifiche.

Fase 4: Configurare ed esportare un rapporto sui risultati

Dopo aver verificato le autorizzazioni e configurato le risorse per crittografare e archiviare il rapporto sui risultati, sei pronto per configurare ed esportare il rapporto.

Per configurare ed esportare un rapporto sui risultati

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Nel pannello di navigazione, in Risultati, scegli Tutti i risultati.
3. (Facoltativo) Utilizzando la barra dei filtri sopra la tabella Risultati, aggiungete criteri di filtro che specificano quali risultati includere nel rapporto. Man mano che aggiungi criteri, Amazon Inspector aggiorna la tabella per includere solo i risultati che soddisfano i criteri. La tabella fornisce un'anteprima dei dati che conterrà il rapporto.

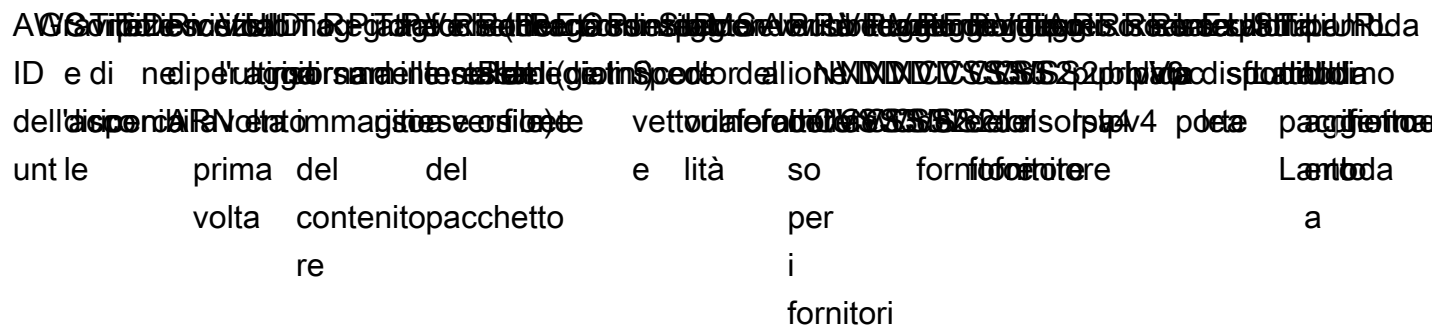
   > **Note**
   >
   > Ti consigliamo di aggiungere criteri di filtro. In caso contrario, il rapporto includerà i dati relativi a tutti i risultati attualmente trovati Regione AWS con lo stato Attivo. Se sei l'amministratore di Amazon Inspector di un'organizzazione, questo include i dati relativi ai risultati di tutti gli account membri della tua organizzazione.
   > Se un report include dati relativi a tutti o a molti risultati, la generazione e l'esportazione del report possono richiedere molto tempo e puoi esportare solo un report alla volta.

4. Scegli Esporta risultati.
5. Nella sezione Impostazioni di esportazione, per Tipo di file di esportazione, specifica un formato di file per il rapporto:

   - Per creare un file JavaScript Object Notation (.json) che contenga i dati, scegliete JSON.

     Se scegli l'opzione JSON, il rapporto includerà tutti i campi per ogni risultato. Per un elenco di possibili campi JSON, consulta il tipo di dati Finding nel riferimento all'API Amazon Inspector.
   - Per creare un file con valori separati da virgole (.csv) che contenga i dati, scegli CSV.

     Se scegli l'opzione CSV, il rapporto includerà solo un sottoinsieme dei campi per ogni risultato, circa 45 campi che riportano gli attributi chiave di un risultato. I campi includono: Tipo di ricerca, Titolo, Severità, Stato, Descrizione, Primo visualizzato, Ultima visualizzazione, Correzione disponibile, ID AWS account, ID risorsa, Tag risorsa e Correzione. Questi si aggiungono ai campi che raccolgono i dettagli del punteggio e gli URL di riferimento per ogni risultato. Di seguito è riportato un esempio delle intestazioni CSV in un rapporto sui risultati:



6. In Export location, per S3 URI, specifica il bucket S3 in cui desideri archiviare il report:

   - Per archiviare il report in un bucket di proprietà del tuo account, scegli Browse S3. Amazon Inspector visualizza una tabella dei bucket S3 per il tuo account. Seleziona la riga per il bucket che desideri, quindi scegli Scegli.

     > **Tip**
     >
     > Per specificare anche un prefisso di percorso Amazon S3 per il report, aggiungi una barra (/) e il prefisso al valore nella casella URI S3. Amazon Inspector include quindi il prefisso quando aggiunge il report al bucket e Amazon S3 genera il percorso specificato dal prefisso.
     > Ad esempio, se desideri utilizzare il tuo Account AWS ID come prefisso e l'ID dell'account è 111122223333, **`/111122223333`** aggiungilo al valore nella casella URI S3.
     > Un prefisso è simile al percorso di una directory all'interno di un bucket S3. Ti consente di raggruppare oggetti simili in un bucket, proprio come potresti archiviare file simili in una cartella su un file system. Per ulteriori informazioni, consulta Organizzazione degli oggetti nella console Amazon S3 utilizzando le cartelle nella Guida per l'utente di Amazon Simple Storage Service.

   - Per archiviare il report in un bucket di proprietà di un altro account, inserisci l'URI del bucket, ad esempio **`s3://DOC-EXAMPLE_BUCKET`**, dove DOC-EXAMPLE_BUCKET è il nome del bucket. Il proprietario del bucket può trovare queste informazioni per te nelle proprietà del bucket.

7. Per la chiave KMS, specifica quella AWS KMS key che desideri utilizzare per crittografare il rapporto:

- Per utilizzare una chiave del tuo account, scegli la chiave dall'elenco. L'elenco mostra le chiavi KMS con crittografia simmetrica gestite dal cliente per il tuo account.
- Per utilizzare una chiave di proprietà di un altro account, inserisci l'Amazon Resource Name (ARN) della chiave. Il proprietario della chiave può trovare queste informazioni per te nelle proprietà della chiave. Per ulteriori informazioni, consulta Finding the key ID and key ARN nella AWS Key Management Service Developer Guide.

8. Scegli Export (Esporta).

Amazon Inspector genera il report dei risultati, lo crittografa con la chiave KMS specificata e lo aggiunge al bucket S3 specificato. A seconda del numero di risultati che hai scelto di includere nel report, questo processo può richiedere diversi minuti o ore. Una volta completata l'esportazione, Amazon Inspector visualizza un messaggio che indica che il report dei risultati è stato esportato correttamente. Facoltativamente, scegli Visualizza report nel messaggio per accedere al report in Amazon S3.

Tieni presente che puoi esportare solo un report alla volta. Se è attualmente in corso un'esportazione, attendi il completamento dell'esportazione prima di provare a esportare un altro rapporto.

Risolvi gli errori di esportazione

Se si verifica un errore durante il tentativo di esportare un report sui risultati, Amazon Inspector visualizza un messaggio che descrive l'errore. Puoi utilizzare le informazioni contenute in questo argomento come guida per identificare le possibili cause e soluzioni dell'errore.

Ad esempio, verifica che il bucket S3 sia nella versione corrente Regione AWS e che la politica del bucket consenta ad Amazon Inspector di aggiungere oggetti al bucket. Verifica inoltre che AWS KMS key sia abilitato nella regione corrente e assicurati che la policy chiave consenta ad Amazon Inspector di utilizzare la chiave.

Dopo aver risolto l'errore, prova a esportare nuovamente il report.

Non è possibile avere più segnalazioni di errore

Se stai tentando di creare un report ma Amazon Inspector lo sta già generando, riceverai un errore che indica Motivo: impossibile avere più report in corso. Questo errore si verifica perché Amazon Inspector può generare un solo report per account alla volta.

Per risolvere l'errore, puoi attendere che l'altro report finisca o annullarlo prima di richiedere un nuovo report.

È possibile controllare lo stato di un rapporto utilizzando l'GetFindingsReportStatusoperazione, questa operazione restituisce l'ID del rapporto di qualsiasi rapporto attualmente in fase di generazione.

Se necessario, è possibile utilizzare l'ID del rapporto fornito dall'`GetFindingsReportStatus`operazione per annullare un'esportazione attualmente in corso utilizzando l'CancelFindingsReportoperazione.

Creazione di risposte personalizzate ai risultati di Amazon Inspector con Amazon EventBridge

Amazon Inspector crea un evento EventBridge per Amazon per i risultati appena generati, i nuovi risultati aggregati e le modifiche allo stato dei risultati. Qualsiasi cosa diversa da una modifica ai `lastObservedAt` campi `updatedAt` and pubblicherà un nuovo evento. Ciò significa che vengono generati nuovi eventi per un risultato quando si intraprendono azioni come il riavvio di una risorsa o la modifica dei tag associati a una risorsa. Tuttavia, l'ID di ricerca nel `id` campo rimane lo stesso. Gli eventi vengono emessi sulla base del best effort.

> **Note**
>
> Se il tuo account è un amministratore delegato di Amazon Inspector, EventBridge pubblica gli eventi sul tuo account oltre all'account membro da cui hanno avuto origine.

Quando utilizzi EventBridge gli eventi con Amazon Inspector, puoi automatizzare le attività per aiutarti a rispondere ai problemi di sicurezza rivelati dai risultati di Amazon Inspector.

Amazon Inspector emette eventi sul bus eventi predefinito nella stessa regione. Ciò significa che devi configurare le regole degli eventi per ogni regione in cui esegui Amazon Inspector per visualizzare gli eventi per quella regione.

Per ricevere notifiche sui risultati di Amazon Inspector in base EventBridge agli eventi, devi creare una EventBridge regola e un obiettivo per Amazon Inspector. Questa regola consente di EventBridge inviare notifiche per i risultati generati da Amazon Inspector alla destinazione specificata nella regola.

Per ulteriori informazioni, consulta EventBridgele regole di Amazon nella Amazon EventBridge User Guide.

Schema degli eventi

Di seguito è riportato un esempio del formato di evento Amazon Inspector per un evento di ricerca EC2. Per uno schema di esempio di altri tipi di ricerca e tipi di eventi, vedi. EventBridge schema


```
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
```

```
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2022-3303",
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
                "remediation": "apt update && apt install --only-upgrade linux-image-
aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
```

```
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```


Creazione di una EventBridge regola per notificarti i risultati di Amazon Inspector

Per aumentare la visibilità dei risultati di Amazon Inspector, puoi impostare avvisi EventBridge di ricerca automatizzati che vengono inviati a un hub di messaggistica. Questo argomento mostra come inviare avvisi `CRITICAL` e rilevazioni sulla `HIGH` gravità a e-mail, Slack o Amazon Chime. Imparerai come impostare un argomento di Amazon Simple Notification Service e quindi collegare tale argomento a una regola di EventBridge evento.

Fase 1: Configurare un argomento e un endpoint di Amazon SNS

Per configurare avvisi automatici, devi prima impostare un argomento in Amazon Simple Notification Service e aggiungere un endpoint. Per ulteriori informazioni, consulta la guida SNS.

Questa procedura stabilisce dove inviare i dati relativi ai risultati di Amazon Inspector. L'argomento SNS può essere aggiunto a una regola di EventBridge evento durante o dopo la creazione della regola dell'evento.

Email setup

Creazione di un argomento SNS

1. Accedi alla console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Dal riquadro di navigazione, seleziona Argomenti, quindi seleziona Crea argomento.
3. Nella sezione Crea argomento, seleziona Standard. Quindi, inserisci il nome di un argomento, ad esempio**`Inspector_to_Email`**. Altri dettagli sono facoltativi.

4. Seleziona Create Topic (Crea argomento). Verrà aperto un nuovo pannello con i dettagli del nuovo argomento.
5. Nella sezione Abbonamenti, seleziona Crea abbonamento.
6. a. Dal menu Protocollo selezionare E-mail.
   b. Nel campo Endpoint, inserisci l'indirizzo email a cui desideri ricevere le notifiche.

   > **Note**
   >
   > Ti verrà richiesto di confermare l'iscrizione tramite il tuo client di posta elettronica dopo aver creato l'abbonamento.

   c. Scegli Crea sottoscrizione.
7. Cerca un messaggio di iscrizione nella tua casella di posta e scegli Conferma abbonamento.

Slack setup

Creazione di un argomento SNS

1. Accedi alla console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Dal riquadro di navigazione, seleziona Argomenti, quindi seleziona Crea argomento.
3. Nella sezione Crea argomento, seleziona Standard. Quindi, inserisci il nome di un argomento, ad esempio**`Inspector_to_Slack`**. Altri dettagli sono facoltativi. Scegli Crea argomento per completare la creazione dell'endpoint.

Configurazione di un client AWS Chatbot

1. Accedi alla AWS Chatbot console all'indirizzohttps://console.aws.amazon.com/chatbot/.
2. Dal riquadro Client configurati, seleziona Configura nuovo client.
3. Scegli Slack, quindi scegli Configura per confermare.

   > **Note**
   >
   > Quando scegli Slack, devi confermare le autorizzazioni per accedere AWS Chatbot al tuo canale selezionando consenti.

4. Seleziona Configura un nuovo canale per aprire il riquadro dei dettagli di configurazione.

a. Inserisci un nome per il canale.

b. Per il canale Slack, scegli il canale che desideri utilizzare.

c. In Slack, copia l'ID del canale privato facendo clic con il pulsante destro del mouse sul nome del canale e selezionando Copia collegamento.

d. Nella AWS Chatbot finestra AWS Management Console, incolla l'ID del canale che hai copiato da Slack nel campo ID del canale privato.

e. In Autorizzazioni, scegli di creare un ruolo IAM utilizzando un modello se non disponi già di un ruolo.

f. Per i modelli di policy, scegli Autorizzazioni di notifica. Questo è il modello di policy IAM per AWS Chatbot. Questa politica fornisce le autorizzazioni di lettura ed elenco necessarie per CloudWatch allarmi, eventi e registri e per gli argomenti di Amazon SNS.

g. Per le politiche Channel Guardrail, scegli 2. AmazonInspector ReadOnlyAccess

h. Scegli la regione in cui hai precedentemente creato l'argomento SNS, quindi seleziona l'argomento Amazon SNS che hai creato per inviare notifiche al canale Slack.

5. Selezionare Configura.

Amazon Chime setup

Creazione di un argomento SNS

1. Accedi alla console Amazon SNS all'indirizzo https://console.aws.amazon.com/sns/v3/home.
2. Seleziona Argomenti dal riquadro di navigazione, quindi seleziona Crea argomento.
3. Nella sezione Crea argomento, seleziona Standard. Quindi, inserisci il nome di un argomento, ad esempio**`Inspector_to_Chime`**. Altri dettagli sono facoltativi. Scegli Crea argomento per completare.

Configurazione di un client AWS Chatbot

1. Accedi alla AWS Chatbot console all'indirizzohttps://console.aws.amazon.com/chatbot/.
2. Dal pannello Client configurati, seleziona Configura nuovo client.
3. Scegli Chime, quindi scegli Configura per confermare.
4. Dal riquadro Dettagli di configurazione, inserisci un nome per il canale.
5. In Amazon Chime, apri la chat room desiderata.

a. Seleziona l'icona a forma di ingranaggio nell'angolo in alto a destra e scegli Manage webhooks and bots (Gestisci webhook e bot).

b. Seleziona Copia URL per copiare l'URL del webhook negli appunti.

6. Nella AWS Chatbot finestra AWS Management Console, incolla l'URL che hai copiato nel campo URL del Webhook.
7. In Autorizzazioni, scegli di creare un ruolo IAM utilizzando un modello se non disponi già di un ruolo.
8. Per i modelli di policy, scegli Autorizzazioni di notifica. Questo è il modello di policy IAM per AWS Chatbot. Fornisce le autorizzazioni di lettura ed elenco necessarie per CloudWatch allarmi, eventi e registri e per gli argomenti di Amazon SNS.
9. Scegli la regione in cui hai precedentemente creato l'argomento SNS, quindi seleziona l'argomento Amazon SNS che hai creato per inviare notifiche alla sala Amazon Chime.
10. Selezionare Configura.

Fase 2: Crea una EventBridge regola per i risultati di Amazon Inspector

1. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
2. Seleziona Regole dal riquadro di navigazione, quindi seleziona Crea regola.
3. Inserisci un nome e una descrizione facoltativa per la regola.
4. Seleziona Regola con uno schema di eventi, quindi Avanti.
5. Nel riquadro Event Pattern, scegli Modelli personalizzati (editor JSON).
6. Incolla il seguente JSON nell'editor.

```
{
  "source": ["aws.inspector2"],
  "detail-type": ["Inspector2 Finding"],
  "detail": {
    "severity": ["HIGH", "CRITICAL"],
    "status": ["ACTIVE"]
  }
}
```

> **Note**
>
> Questo pattern invia notifiche per qualsiasi rilevazione attiva `CRITICAL` o di `HIGH` gravità rilevata da Amazon Inspector.

Seleziona Avanti quando hai finito di inserire lo schema dell'evento.

7. Nella pagina Seleziona obiettivi, scegli Servizio AWS. Quindi, per Seleziona il tipo di destinazione, scegli l'argomento SNS.
8. Per Argomento, seleziona il nome dell'argomento SNS che hai creato nel passaggio 1. Quindi scegli Successivo.
9. Aggiungi tag opzionali se necessario e scegli Avanti.
10. Rivedi la regola, quindi scegli Crea regola.

EventBridge per ambienti con più account Amazon Inspector

Se sei un amministratore delegato di Amazon Inspector, EventBridge le regole vengono visualizzate sul tuo account in base ai risultati applicabili dei tuoi account membro. Se configuri le notifiche relative ai risultati tramite EventBridge il tuo account amministratore, come descritto nella sezione precedente, riceverai notifiche relative a più account. In altre parole, riceverai una notifica dei risultati e degli eventi generati dai tuoi account membro oltre a quelli generati dal tuo account.

Puoi utilizzare i `accountId` dettagli JSON del risultato per identificare l'account membro da cui ha avuto origine il risultato di Amazon Inspector.

Esportazione di SBOM con Amazon Inspector

Puoi utilizzare la console o l'API di Amazon Inspector per generare la SBOM (Software Bill of Materials) per le tue risorse. Un SBOM è un inventario annidato di tutti i componenti software open source e di terze parti della tua codebase. Amazon Inspector fornisce SBOM per le singole risorse del tuo ambiente. Gli SBOM esportati da Amazon Inspector possono aiutarti a ottenere visibilità sulle informazioni sulla tua fornitura di software, come i pacchetti più utilizzati e le vulnerabilità associate all'interno dell'organizzazione.

Puoi esportare gli SBOM per tutte le risorse supportate che vengono monitorate attivamente da Amazon Inspector. Puoi controllare lo stato delle tue risorse tramite. Valutazione della copertura di Amazon Inspector del tuo ambiente AWS

> **Note**
>
> Amazon Inspector non supporta l'esportazione di SBOM per istanze Windows EC2.

Formati Amazon Inspector

Amazon Inspector supporta l'esportazione di SBOM in formati compatibili con CyclonedX 1.4 e SPDX 2.3. Amazon Inspector esporta gli SBOM come `JSON` file nel bucket Amazon S3 di tua scelta.

> **Note**
>
> Le esportazioni in formato SPDX da Amazon Inspector sono compatibili con i sistemi che utilizzano SPDX 2.3, tuttavia non contengono il campo Creative Commons Zero (CC0). Questo perché l'inclusione di questo campo consentirebbe agli utenti di ridistribuire o modificare il materiale.

Esempio di formato SBOM CyclonedX 1.4 di Amazon Inspector

```
                {
"bomFormat": "CycloneDX",
"specVersion": "1.4",
"version": 1,
```

```
  "metadata": {
    "timestamp": "2023-06-02T01:17:46Z",
    "component": null,
    "properties": [
      {
        "name": "imageId",
        "value":
 "sha256:c8ee97f7052776ef223080741f61fcdf6a3a9107810ea9649f904aa4269fdac6"
      },
      {
        "name": "architecture",
        "value": "arm64"
      },
      {
        "name": "accountId",
        "value": "111122223333"
      },
      {
        "name": "resourceType",
        "value": "AWS_ECR_CONTAINER_IMAGE"
      }
    ]
  },
  "components": [
    {
      "type": "library",
      "name": "pip",
      "purl": "pkg:pypi/pip@22.0.4?path=usr/local/lib/python3.8/site-packages/
pip-22.0.4.dist-info/METADATA",
      "bom-ref": "98dc550d1e9a0b24161daaa0d535c699"
    },
    {
      "type": "application",
      "name": "libss2",
      "purl": "pkg:dpkg/libss2@1.44.5-1+deb10u3?
arch=ARM64&epoch=0&upstream=libss2-1.44.5-1+deb10u3.src.dpkg",
      "bom-ref": "2f4d199d4ef9e2ae639b4f8d04a813a2"
    },
    {
      "type": "application",
      "name": "liblz4-1",
      "purl": "pkg:dpkg/liblz4-1@1.8.3-1+deb10u1?
arch=ARM64&epoch=0&upstream=liblz4-1-1.8.3-1+deb10u1.src.dpkg",
      "bom-ref": "9a6be8907ead891b070e60f5a7b7aa9a"
```

```
    },
    {
      "type": "application",
      "name": "mawk",
      "purl": "pkg:dpkg/mawk@1.3.3-17+b3?
arch=ARM64&epoch=0&upstream=mawk-1.3.3-17+b3.src.dpkg",
      "bom-ref": "c2015852a729f97fde924e62a16f78a5"
    },
    {
      "type": "application",
      "name": "libgmp10",
      "purl": "pkg:dpkg/libgmp10@6.1.2+dfsg-4+deb10u1?
arch=ARM64&epoch=2&upstream=libgmp10-6.1.2+dfsg-4+deb10u1.src.dpkg",
      "bom-ref": "52907290f5beef00dff8da77901b1085"
    },
    {
      "type": "application",
      "name": "ncurses-bin",
      "purl": "pkg:dpkg/ncurses-bin@6.1+20181013-2+deb10u3?
arch=ARM64&epoch=0&upstream=ncurses-bin-6.1+20181013-2+deb10u3.src.dpkg",
      "bom-ref": "cd20cfb9ebeeadba3809764376f43bce"
    }
  ],
  "vulnerabilities": [
    {
      "id": "CVE-2022-40897",
      "affects": [
        {
          "ref": "a74a4862cc654a2520ec56da0c81cdb3"
        },
        {
          "ref": "0119eb286405d780dc437e7dbf2f9d9d"
        }
      ]
    }
  ]
}
```

Esempio di formato SBOM SPDX 2.3 di Amazon Inspector

```
{
```

```
 "name": "409870544328/EC2/i-022fba820db137c64/ami-074ea14c08effb2d8",
 "spdxVersion": "SPDX-2.3",
 "creationInfo": {
  "created": "2023-06-02T21:19:22Z",
  "creators": [
   "Organization: 409870544328",
   "Tool: Amazon Inspector SBOM Generator"
  ]
 },
 "documentNamespace": "EC2://i-022fba820db137c64/AMAZON_LINUX_2/null/x86_64",
 "comment": "",
 "packages": [{
   "name": "elfutils-libelf",
   "versionInfo": "0.176-2.amzn2",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
    "referenceCategory": "PACKAGE-MANAGER",
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/elfutils-libelf@0.176-2.amzn2?
arch=X86_64&epoch=0&upstream=elfutils-libelf-0.176-2.amzn2.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-elfutils-libelf-ddf56a513c0e76ab2ae3246d9a91c463"
  },
  {
   "name": "libcurl",
   "versionInfo": "7.79.1-1.amzn2.0.1",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
     "referenceType": "purl",
     "referenceLocator": "pkg:rpm/libcurl@7.79.1-1.amzn2.0.1?
arch=X86_64&epoch=0&upstream=libcurl-7.79.1-1.amzn2.0.1.src.rpm"
    },
    {
     "referenceCategory": "SECURITY",
     "referenceType": "vulnerability",
     "referenceLocator": "CVE-2022-32205"
    }
   ],
   "SPDXID": "SPDXRef-Package-rpm-libcurl-710fb33829bc5106559bcd380cddb7d5"
```

```
  },
  {
   "name": "hunspell-en-US",
   "versionInfo": "0.20121024-6.amzn2.0.1",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
    "referenceCategory": "PACKAGE-MANAGER",
    "referenceType": "purl",
    "referenceLocator": "pkg:rpm/hunspell-en-US@0.20121024-6.amzn2.0.1?
arch=NOARCH&epoch=0&upstream=hunspell-en-US-0.20121024-6.amzn2.0.1.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-hunspell-en-US-de19ae0883973d6cea5e7e079d544fe5"
  },
  {
   "name": "grub2-tools-minimal",
   "versionInfo": "2.06-2.amzn2.0.6",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
     "referenceCategory": "PACKAGE-MANAGER",
     "referenceType": "purl",
     "referenceLocator": "pkg:rpm/grub2-tools-minimal@2.06-2.amzn2.0.6?
arch=X86_64&epoch=1&upstream=grub2-tools-minimal-2.06-2.amzn2.0.6.src.rpm"
    },
    {
     "referenceCategory": "SECURITY",
     "referenceType": "vulnerability",
     "referenceLocator": "CVE-2021-3981"
    }
   ],
   "SPDXID": "SPDXRef-Package-rpm-grub2-tools-minimal-c56b7ea76e5a28ab8f232ef6d7564636"
  },
  {
   "name": "unixODBC-devel",
   "versionInfo": "2.3.1-14.amzn2",
   "downloadLocation": "NOASSERTION",
   "sourceInfo": "/var/lib/rpm/Packages",
   "filesAnalyzed": false,
   "externalRefs": [{
    "referenceCategory": "PACKAGE-MANAGER",
    "referenceType": "purl",
```

```
    "referenceLocator": "pkg:rpm/unixODBC-devel@2.3.1-14.amzn2?
arch=X86_64&epoch=0&upstream=unixODBC-devel-2.3.1-14.amzn2.src.rpm"
   }],
   "SPDXID": "SPDXRef-Package-rpm-unixODBC-devel-1bb35add92978df021a13fc9f81237d2"
  }
 ],
 "relationships": [{
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-elfutils-libelf-
ddf56a513c0e76ab2ae3246d9a91c463",
   "relationshipType": "DESCRIBES"
  },
  {
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-yajl-8476ce2db98b28cfab2b4484f84f1903",
   "relationshipType": "DESCRIBES"
  },
  {
   "spdxElementId": "SPDXRef-DOCUMENT",
   "relatedSpdxElement": "SPDXRef-Package-rpm-unixODBC-
devel-1bb35add92978df021a13fc9f81237d2",
   "relationshipType": "DESCRIBES"
  }
 ],
 "SPDXID": "SPDXRef-DOCUMENT"
}
```


Filtri per SBOM

Quando esportate gli SBOM, potete includere filtri per creare report per sottoinsiemi specifici di risorse. Se non fornite un filtro, vengono esportati gli SBOM per tutte le risorse attive e supportate. E se sei un amministratore delegato, questo include anche risorse per tutti i membri. I filtri disponibili sono:

- AccountID: questo filtro può essere utilizzato per esportare SBOM per qualsiasi risorsa associata a un ID account specifico.
- Tag di istanza EC2: questo filtro può essere utilizzato per esportare SBOM per istanze EC2 con tag specifici.
- Nome funzione: questo filtro può essere utilizzato per esportare SBOM per funzioni Lambda specifiche.

- Tag immagine: questo filtro può essere utilizzato per esportare SBOM per immagini di contenitori con tag specifici.
- Tag funzione Lambda: questo filtro può essere utilizzato per esportare SBOM per funzioni Lambda con tag specifici.
- Tipo di risorsa: questo filtro può essere utilizzato per filtrare il tipo di risorsa: EC2/ECR/Lambda.
- ID risorsa: questo filtro può essere utilizzato per esportare un SBOM per una risorsa specifica.
- Nome del repository: questo filtro può essere utilizzato per generare SBOM per le immagini dei contenitori in repository specifici.

Configura ed esporta gli SBOM

Per esportare gli SBOM, devi prima configurare un bucket Amazon S3 e AWS KMS una chiave che Amazon Inspector può utilizzare. Puoi utilizzare i filtri per esportare gli SBOM per sottoinsiemi specifici delle tue risorse. Per esportare gli SBOM per più account in un' AWS organizzazione, segui questi passaggi dopo aver effettuato l'accesso come amministratore delegato di Amazon Inspector.

Prerequisiti

- Risorse supportate che vengono monitorate attivamente da Amazon Inspector.
- Un bucket Amazon S3 configurato con una policy che consente ad Amazon Inspector di aggiungere oggetti. Per informazioni sulla configurazione della policy, consulta Configurare le autorizzazioni di esportazione.
- Una AWS KMS chiave configurata con una politica che consente di utilizzare Amazon Inspector per crittografare i report. Per informazioni sulla configurazione della politica, consulta Configurare una AWS KMS chiave per l'esportazione.

> **Note**
>
> Se in precedenza hai configurato un bucket Amazon S3 e una AWS KMS chiave per l'esportazione dei risultati, puoi utilizzare lo stesso bucket e la stessa chiave per l'esportazione SBOM.

Scegli il tuo metodo di accesso preferito per esportare un SBOM.

Console

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione con le risorse per cui desideri esportare SBOM.
3. Nel pannello di navigazione, scegli Esporta SBOM.
4. (Facoltativo) Nella pagina Esporta SBOM, utilizzate il menu Aggiungi filtro per selezionare un sottoinsieme di risorse per cui creare report. Se non viene fornito alcun filtro, Amazon Inspector esporterà i report per tutte le risorse attive. Se sei un amministratore delegato, questo includerà tutte le risorse attive della tua organizzazione.
5. In Impostazioni di esportazione selezionate il formato desiderato per la SBOM.
6. Inserisci un URI Amazon S3 o scegli Browse Amazon S3 per selezionare una posizione Amazon S3 in cui archiviare la SBOM.
7. Inserisci una AWS KMS chiave configurata per Amazon Inspector da utilizzare per crittografare i report.

API

- Per esportare gli SBOM per le tue risorse in modo programmatico, utilizza il CreateSbomExportfunzionamento dell'API Amazon Inspector.

  Nella tua richiesta, utilizza il `reportFormat` parametro per specificare il formato di output SBOM, scegli o. `CYCLONEDX_1_4` `SPDX_2_3` Il `s3Destination` parametro è obbligatorio ed è necessario specificare un bucket S3 configurato con una policy che consenta ad Amazon Inspector di scrivere su di esso. Facoltativamente, utilizza `resourceFilterCriteria` i parametri per limitare l'ambito del report a risorse specifiche.

AWS CLI

- Per esportare gli SBOM per le tue risorse usando il seguente AWS Command Line Interface comando:

  ```
  aws inspector2 create-sbom-export --report-format
  FORMAT --s3-destination bucketName=DOC-EXAMPLE-
  BUCKET1,keyPrefix=PREFIX,kmsKeyArn=arn:aws:kms:Region:111122223333:key/123
  ```

Nella richiesta, sostituite *FORMAT* con il formato che preferite, CYCLONEDX_1_4 oppureSPDX_2_3. Quindi sostituisci *user input placeholders*for the s3 destination con il nome del bucket S3 in cui esportare, il prefisso da usare per l'output in S3 e l'ARN per la chiave KMS che stai utilizzando per crittografare i report.

Ricerca nel database delle vulnerabilità di Amazon Inspector

Puoi cercare vulnerabilità ed esposizioni (CVE) nel database delle vulnerabilità di Amazon Inspector. Amazon Inspector utilizza le informazioni del database delle vulnerabilità per produrre dettagli relativi a un ID CVE. Puoi accedere a questi dettagli in una pagina dei dettagli CVE.

Questo argomento descrive come cercare nel database delle vulnerabilità di Amazon Inspector utilizzando un ID CVE e interpretare la pagina dei dettagli CVE. Per informazioni sui risultati, consulta. Informazioni sulla ricerca di Amazon Inspector

> **Note**
>
> Amazon Inspector monitora e fornisce risultati per individuare altre vulnerabilità del software nel database. Tuttavia, Amazon Inspector supporta solo i CVE con piattaforme elencate nella sezione Piattaforme di rilevamento della pagina dei dettagli CVE. Al momento, la ricerca CVE non supporta. Microsoft Windows

Ricerca nel database delle vulnerabilità

Questa sezione descrive come cercare nel database delle vulnerabilità nella console e con l'API Amazon Inspector.

> **Note**
>
> È necessario attivare Amazon Inspector nella versione corrente Regione AWS prima di poter effettuare ricerche nel database delle vulnerabilità.

Console

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/
2. Dal pannello di navigazione, scegli Vulnerability database search.
3. Nella barra di ricerca, inserisci un ID CVE e scegli Cerca.

API

Esegui l'SearchVulnerabilitiesAPI Amazon Inspector e fornisci un singolo ID CVE `filterCriteria` nel seguente formato:. `CVE-<year>-<ID>`

Comprendere i dettagli del CVE

Questa sezione descrive come interpretare la pagina dei dettagli CVE.

Dettagli CVE

La sezione dei dettagli CVE include le seguenti informazioni:

- Descrizione e ID CVE
- Severità CVE
- Punteggi del Common Vulnerability Scoring System (CVSS) e dell'Exploit Prediction Scoring System (EPSS)
- Piattaforme di rilevamento

> **Note**
>
> Se questo campo è vuoto, Amazon Inspector non supporta il rilevamento del tuo ID CVE.

- Common Weakness Enumeration (CWE)
- Date di creazione e aggiornamento del fornitore

Intelligence sulle vulnerabilità

La sezione sull'intelligence sulle vulnerabilità fornisce dati di intelligence sulle minacce, come gli obiettivi degli exploit e la data dell'ultimo exploit pubblico nota.

Fornisce inoltre i dati della Cybersecurity and Infrastructure Security Agency (CISA), che includono l'azione di correzione, la data in cui il CVE è stato aggiunto al catalogo Known Exploited Vulnerability e la data e l'ora in cui CISA si aspetta che le agenzie federali risolvano il CVE.

Riferimenti

La sezione dei riferimenti fornisce collegamenti a risorse per ulteriori informazioni sul CVE.

Schema di EventBridge eventi Amazon per gli eventi Amazon Inspector

Per supportare l'integrazione con altre applicazioni, servizi e sistemi, come i sistemi di monitoraggio o di gestione degli eventi, Amazon Inspector pubblica automaticamente i risultati su Amazon EventBridge come eventi. EventBridgeè un servizio di bus eventi senza server che fornisce un flusso di dati in tempo reale da applicazioni e altro Servizi AWS verso destinazioni come AWS Lambda funzioni, argomenti di Amazon Simple Notification Service e flussi Amazon Kinesis Data Streams. Per ulteriori informazioni EventBridge ed EventBridge eventi, consulta la Amazon EventBridge User Guide.

Amazon Inspector pubblica eventi relativi a risultati, modifiche alla copertura delle risorse e scansioni iniziali delle singole risorse. Ogni evento è un oggetto JSON conforme allo schema degli eventi. EventBridge AWS Poiché i dati sono strutturati come un EventBridge evento, puoi monitorare, elaborare e agire in base ai risultati e agli eventi supportati da Amazon Inspector utilizzando altre applicazioni, servizi e strumenti.

Argomenti

Schema EventBridge di base Amazon per Amazon Inspector

Di seguito è riportato un esempio dello schema di base per un EventBridge evento per Amazon Inspector. I dettagli dell'evento variano in base al tipo di evento.

```
{
    "version": "0",
    "id": "Event ID",
    "detail-type": "Inspector2 *event type*",
    "source": "aws.inspector2",
    "account": "Account AWS ID (string)",
    "time": "event timestamp (string)",
    "region": "Regione AWS (string)",
```

```
    "resources": [
        *IDs or ARNs of the resources involved in the event*
    ],
    "detail": {
        *Details of an Amazon Inspector event type*
    }
}
```

Esempio di schema di eventi di ricerca di Amazon Inspector

Di seguito sono riportati alcuni esempi dello schema di un EventBridge evento per i risultati di Amazon Inspector. Gli eventi di ricerca vengono creati quando Amazon Inspector identifica una vulnerabilità del software o un problema di rete in una delle tue risorse. Per una guida alla creazione di notifiche in risposta a questo tipo di evento, consulta. Creazione di risposte personalizzate ai risultati di Amazon Inspector con Amazon EventBridge

I seguenti campi identificano un evento di ricerca:

- Il `detail-type` campo è impostato su`Inspector2 Finding`.
- L'`detail`oggetto descrive il risultato.

Seleziona una delle opzioni per visualizzare gli schemi di eventi di ricerca per diverse risorse e tipi di ricerca.

Amazon EC2 package vulnerability finding

```
{
    "version": "0",
    "id": "66a7a279-5f92-971c-6d3e-c92da0950992",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T22:46:15Z",
    "region": "us-east-1",
    "resources": ["i-0c2a343f1948d5205"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "\n It was discovered that the sound subsystem in the Linux
 kernel contained a\n race condition in some situations. A local attacker could use
 this to cause\n a denial of service (system crash).",
```

```
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Oct 24, 2022, 11:08:59 PM"
        },
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "fixAvailable": "YES",
        "lastObservedAt": "Jan 19, 2023, 10:46:15 PM",
        "packageVulnerabilityDetails": {
            "cvss": [{
                "baseScore": 4.7,
                "scoringVector": "CVSS:3.1/AV:L/AC:H/PR:L/UI:N/S:U/C:N/I:N/A:H",
                "source": "NVD",
                "version": "3.1"
            }],
            "referenceUrls": ["https://lore.kernel.org/all/
CAFcO6XN7JDM4xSXGhtusQfS2mSBcx50VJKwQpCq=WeLt57aaZA@mail.gmail.com/", "https://
ubuntu.com/security/notices/USN-5792-1", "https://ubuntu.com/security/notices/
USN-5791-2", "https://ubuntu.com/security/notices/USN-5791-1", "https://ubuntu.com/
security/notices/USN-5793-2", "https://git.kernel.org/pub/scm/linux/kernel/git/
torvalds/linux.git/commit/?id=8423f0b6d513b259fdab9c9bf4aaa6188d054c2d", "https://
ubuntu.com/security/notices/USN-5793-1", "https://ubuntu.com/security/notices/
USN-5792-2", "https://ubuntu.com/security/notices/USN-5791-3", "https://ubuntu.com/
security/notices/USN-5793-4", "https://ubuntu.com/security/notices/USN-5793-3",
 "https://git.kernel.org/linus/8423f0b6d513b259fdab9c9bf4aaa6188d054c2d(6.0-rc5)",
 "https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-3303"],
            "relatedVulnerabilities": [],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2022/
CVE-2022-3303.html",
            "vendorCreatedAt": "Sep 27, 2022, 11:15:00 PM",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2022-3303",
            "vulnerablePackages": [{
                "arch": "X86_64",
                "epoch": 0,
                "fixedInVersion": "0:5.15.0.1027.31~20.04.16",
                "name": "linux-image-aws",
                "packageManager": "OS",
                "remediation": "apt update && apt install --only-upgrade linux-
image-aws",
                "version": "5.15.0.1026.30~20.04.16"
            }]
```

```
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b7ff1a8d69f1bb35",
                    "ipV4Addresses": ["172.31.85.212", "44.203.45.27"],
                    "ipV6Addresses": [],
                    "launchedAt": "Jan 19, 2023, 7:53:14 PM",
                    "platform": "UBUNTU_20_04",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0c2a343f1948d5205",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2022-3303 - linux-image-aws",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 10:46:15 PM"
    }
}
```


Amazon EC2 network reachability finding


```
{
    "version": "0",
    "id": "d0384f63-1621-1b75-d014-a5e45628ef3e",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
```

```
    "account": "111122223333",
    "time": "2023-01-20T09:17:57Z",
    "region": "us-east-1",
    "resources": ["i-0a96278c2206a8e4b"],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "On the instance i-0a96278c2206a8e4b, the port range
 22-22 is reachable from the InternetGateway igw-72069c09 from an attached ENI
 eni-0976efe678170408f.",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 20, 2023, 9:17:57 AM",
        "lastObservedAt": "Jan 20, 2023, 9:17:57 AM",
        "networkReachabilityDetails": {
            "networkPath": {
                "steps": [{
                    "componentId": "igw-72069c09",
                    "componentType": "AWS::EC2::InternetGateway"
                }, {
                    "componentId": "acl-91d74eec",
                    "componentType": "AWS::EC2::NetworkAcl"
                }, {
                    "componentId": "sg-0aaed0af450bd0165",
                    "componentType": "AWS::EC2::SecurityGroup"
                }, {
                    "componentId": "eni-0976efe678170408f",
                    "componentType": "AWS::EC2::NetworkInterface"
                }, {
                    "componentId": "i-0a96278c2206a8e4b",
                    "componentType": "AWS::EC2::Instance"
                }]
            },
            "openPortRange": {
                "begin": 22,
                "end": 22
            },
            "protocol": "TCP"
        },
        "remediation": {
            "recommendation": {
                "text": "You can restrict access to your instance by modifying the
 Security Groups or ACLs in the network path."
            }
        },
```

```
        "resources": [{
            "details": {
                "awsEc2Instance": {
                    "iamInstanceProfileArn": "arn:aws:iam::111122223333:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-0b5eea76982371e91",
                    "ipV4Addresses": ["3.89.90.19", "172.31.93.57"],
                    "ipV6Addresses": [],
                    "keyName": "example-inspector-test",
                    "launchedAt": "Jan 19, 2023, 7:25:02 PM",
                    "platform": "AMAZON_LINUX_2",
                    "subnetId": "subnet-8213f2a3",
                    "type": "t2.micro",
                    "vpcId": "vpc-ab6650d1"
                }
            },
            "id": "i-0a96278c2206a8e4b",
            "partition": "aws",
            "region": "us-east-1",
            "type": "AWS_EC2_INSTANCE"
        }],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "Port 22 is reachable from an Internet Gateway",
        "type": "NETWORK_REACHABILITY",
        "updatedAt": "Jan 20, 2023, 9:17:57 AM"
    }
}
```

Amazon ECR package vulnerability finding

```
{
    "version": "0",
    "id": "5b52952e-26df-3a51-6d14-4dbe737e58ec",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T21:59:00Z",
    "region": "us-east-1",
    "resources": [
```

```
        "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/
sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13"
    ],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "libcurl would reuse a previously created connection even
 when a TLS or SSHrelated option had been changed that should have prohibited
 reuse.libcurl keeps previously used connections in a connection pool for
 subsequenttransfers to reuse if one of them matches the setup. However, several TLS
 andSSH settings were left out from the configuration match checks, making themmatch
 too easily.",
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 9:59:00 PM",
        "fixAvailable": "YES",
        "inspectorScore": 7.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "adjustments": [],
                "cvssSource": "NVD",
                "score": 7.5,
                "scoreSource": "NVD",
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Jan 19, 2023, 9:59:00 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 5,
                    "scoringVector": "AV:N/AC:L/Au:N/C:N/I:P/A:N",
                    "source": "NVD",
                    "version": "2.0"
                },
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:H/A:N",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
```

```
                "https://hackerone.com/reports/1555796",
                "https://security.gentoo.org/glsa/202212-01",
                "https://lists.debian.org/debian-lts-announce/2022/08/
msg00017.html",
                "https://www.debian.org/security/2022/dsa-5197"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2022-27782",
            "vendorCreatedAt": "Jun 2, 2022, 2:15:00 PM",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Jan 5, 2023, 5:51:00 PM",
            "vulnerabilityId": "CVE-2022-27782",
            "vulnerablePackages": [
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "fixedInVersion": "0:7.61.1-22.el8_6.3",
                    "name": "libcurl",
                    "packageManager": "OS",
                    "release": "22.el8",
                    "remediation": "yum update libcurl",
                    "sourceLayerHash":
 "sha256:38a980f2cc8accf69c23deae6743d42a87eb34a54f02396f3fcfd7c2d06e2c5b",
                    "version": "7.61.1"
                },
                {
                    "arch": "X86_64",
                    "epoch": 0,
                    "fixedInVersion": "0:7.61.1-22.el8_6.3",
                    "name": "curl",
                    "packageManager": "OS",
                    "release": "22.el8",
                    "remediation": "yum update curl",
                    "sourceLayerHash":
 "sha256:38a980f2cc8accf69c23deae6743d42a87eb34a54f02396f3fcfd7c2d06e2c5b",
                    "version": "7.61.1"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
```

```
        },
        "resources": [
            {
                "details": {
                    "awsEcrContainerImage": {
                        "architecture": "amd64",
                        "imageHash":
 "sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13",
                        "imageTags": [
                            "o3"
                        ],
                        "platform": "ORACLE_LINUX_8",
                        "pushedAt": "Jan 19, 2023, 7:38:39 PM",
                        "registry": "111122223333",
                        "repositoryName": "inspector2"
                    }
                },
                "id": "arn:aws:ecr:us-east-1:111122223333:repository/inspector2/
sha256:98f0304b3a3b7c12ce641177a99d1f3be56f532473a528fda38d53d519cafb13",
                "partition": "aws",
                "region": "us-east-1",
                "type": "AWS_ECR_CONTAINER_IMAGE"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2022-27782 - libcurl, curl",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 9:59:00 PM"
    }
}
```


Lambda package vulnerability finding


```
{
    "version": "0",
    "id": "040bb590-3a12-353f-ecb1-05e54b0fbea7",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-19T19:20:25Z",
```

```
    "region": "us-east-1",
    "resources": [
        "arn:aws:lambda:us-east-1:111122223333:function:ExampleFunction:$LATEST"
    ],
    "detail": {
        "awsAccountId": "111122223333",
        "description": "Those using Woodstox to parse XML data may be vulnerable to
 Denial of Service attacks (DOS) if DTD support is enabled. If the parser is running
 on user supplied input, an attacker may supply content that causes the parser to
 crash by stackoverflow. This effect may support a denial of service attack.",
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:us-east-1:111122223333:finding/
FINDING_ID",
        "firstObservedAt": "Jan 19, 2023, 7:20:25 PM",
        "fixAvailable": "YES",
        "inspectorScore": 7.5,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "cvssSource": "NVD",
                "score": 7.5,
                "scoreSource": "NVD",
                "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Jan 19, 2023, 7:20:25 PM",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
                "https://bugs.chromium.org/p/oss-fuzz/issues/detail?id=47434"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2022-40152",
            "vendorCreatedAt": "Sep 16, 2022, 10:15:00 AM",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Nov 25, 2022, 11:15:00 AM",
```

```
            "vulnerabilityId": "CVE-2022-40152",
            "vulnerablePackages": [
                {
                    "epoch": 0,
                    "filePath": "lib/woodstox-core-6.2.7.jar",
                    "fixedInVersion": "6.4.0",
                    "name": "com.fasterxml.woodstox:woodstox-core",
                    "packageManager": "JAR",
                    "remediation": "Update woodstox-core to 6.4.0",
                    "version": "6.2.7"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsLambdaFunction": {
                        "architectures": [
                            "X86_64"
                        ],
                        "codeSha256": "+EwrOrht2um4fdVCD73gj
+O7HJIAUvUxi8AD0eKHSkc=",
                        "executionRoleArn": "arn:aws:iam::111122223333:role/
ExampleFunction-ExecutionRole",
                        "functionName": "Example-function",
                        "lastModifiedAt": "Nov 7, 2022, 8:29:27 PM",
                        "packageType": "ZIP",
                        "runtime": "JAVA_11",
                        "version": "$LATEST"
                    }
                },
                "id": "arn:aws:lambda:us-
east-1:111122223333:function:ExampleFunction:$LATEST",
                "partition": "aws",
                "region": "us-east-1",
                "tags": {
                    "TargetAlias": "DeploymentStack",
                    "SoftwareType": "Infrastructure"
                },
```

```
                "type": "AWS_LAMBDA_FUNCTION"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2022-40152 - com.fasterxml.woodstox:woodstox-core",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Jan 19, 2023, 7:20:25 PM"
    }
}
```

Lambda code vulnerability finding

```
{
   "version":"0",
   "id":"9df01cb1-df24-bc46-5650-085a4087e7aa",
   "detail-type":"Inspector2 Finding",
   "source":"aws.inspector2",
   "account":"111122223333",
   "time":"2023-12-07T22:14:45Z",
   "region":"us-east-1",
   "resources":[
      "arn:aws:lambda:us-east-1:111122223333:function:code-finding:$LATEST"
   ],
   "detail":{
      "awsAccountId":"111122223333",
      "codeVulnerabilityDetails":{
         "detectorId":"python/lambda-override-reserved@v1.0",
         "detectorName":"Override of reserved variable names in a Lambda function",
         "detectorTags":[
            "availability",
            "aws-python-sdk",
            "aws-lambda",
            "data-integrity",
            "maintainability",
            "security",
            "security-context",
            "python"
         ],
         "filePath":{
            "endLine":6,
```

```
            "fileName":"lambda_function.py",
            "filePath":"lambda_function.py",
            "startLine":6
         },
         "ruleId":"Rule-434311"
      },
      "description":"Overriding environment variables that are reserved by AWS
 Lambda might lead to unexpected behavior or failure of the Lambda function.",
      "findingArn":"arn:aws:inspector2:us-east-1:111122223333:finding/FINDING_ID",
      "firstObservedAt":"Aug 8, 2023, 7:33:58 PM",
      "lastObservedAt":"Dec 7, 2023, 10:14:45 PM",
      "remediation":{
         "recommendation":{
            "text":"Your code attempts to override an environment variable that is
 reserved by the Lambda runtime environment. This can lead to unexpected behavior
 and might break the execution of your Lambda function.\n\n[Learn more](https://
docs.aws.amazon.com/lambda/latest/dg/configuration-envvars.html#configuration-
envvars-runtime)"
         }
      },
      "resources":[
         {
            "details":{
               "awsLambdaFunction":{
                  "architectures":[
                     "X86_64"
                  ],
                  "codeSha256":"2mtfH+CgubesG6NYpb2zEqBja5WN6FfbH4AAYDuF8RE=",
                  "executionRoleArn":"arn:aws:iam::193043430472:role/service-role/
code-finding-role-7jgg3wan",
                  "functionName":"code-finding",
                  "lastModifiedAt":"Dec 7, 2023, 10:12:48 PM",
                  "packageType":"ZIP",
                  "runtime":"PYTHON_3_7",
                  "version":"$LATEST"
               }
            },
            "id":"arn:aws:lambda:us-east-1:193043430472:function:code-finding:
$LATEST",
            "partition":"aws",
            "region":"us-east-1",
            "type":"AWS_LAMBDA_FUNCTION"
         }
      ],
```

```
      "severity":"HIGH",
      "status":"ACTIVE",
      "title":"Overriding environment variables that are reserved by AWS Lambda
 might lead to unexpected behavior.",
      "type":"CODE_VULNERABILITY",
      "updatedAt":"Dec 7, 2023, 10:14:45 PM"
   }
}
```

> **Note**
>
> Il valore di dettaglio restituisce i dettagli JSON di un singolo risultato come oggetto. Non restituisce l'intera sintassi di risposta ai risultati, che supporta più risultati all'interno di un array.

Esempio di schema di eventi completo per la scansione iniziale di Amazon Inspector

Di seguito è riportato un esempio dello schema di eventi per un EventBridge evento Amazon Inspector per il completamento di una scansione iniziale. Questo evento viene creato quando Amazon Inspector completa una scansione iniziale di una delle tue risorse.

I seguenti campi identificano un evento di completamento della scansione iniziale:

- Il `detail-type` campo è impostato su`Inspector2 Scan`.
- L'`detail`oggetto contiene un `finding-severity-counts` oggetto che descrive in dettaglio il numero di risultati nelle categorie di gravità applicabili, ad esempio `CRITICAL``HIGH`, e`MEDIUM`.

Seleziona una delle opzioni per visualizzare diversi schemi di eventi di scansione iniziale in base al tipo di risorsa.

Amazon EC2 instance initial scan

```
{
    "version": "0",
```

```
    "id": "28a46762-6ac8-6cc4-4f55-bc9ab99af928",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T22:52:35Z",
    "region": "us-east-1",
    "resources": [
        "i-087d63509b8c97098"
    ],
    "detail": {
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "finding-severity-counts": {
            "CRITICAL": 0,
            "HIGH": 0,
            "MEDIUM": 0,
            "TOTAL": 0
        },
        "instance-id": "i-087d63509b8c97098",
        "version": "1.0"
    }
}
```

Amazon ECR image initial scan

```
{
    "version": "0",
    "id": "fdaa751a-984c-a709-44f9-9a9da9cd3606",
    "detail-type": "Inspector2 Scan",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T23:15:18Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:ecr:us-east-1:111122223333:repository/inspector2"
    ],
    "detail": {
        "scan-status": "INITIAL_SCAN_COMPLETE",
        "repository-name": "arn:aws:ecr:us-east-1:111122223333:repository/
inspector2",
        "finding-severity-counts": {
            "CRITICAL": 0,
```

```
            "HIGH": 0,
            "MEDIUM": 0,
            "TOTAL": 0
        },
        "image-digest":
 "sha256:965fbcae990b0467ed5657caceaec165018ef44a4d2d46c7cdea80a9dff0d1ea",
        "image-tags": [
            "ubuntu22"
        ],
        "version": "1.0"
    }
}
```

Lambda function initial scan

```
{
  "version": "0",
  "id": "4f290a7c-361b-c442-03c8-a629f6f20d6c",
  "detail-type": "Inspector2 Scan",
  "source": "aws.inspector2",
  "account": "111122223333",
  "time": "2023-02-23T18:06:03Z",
  "region": "us-west-2",
  "resources": [
    "arn:aws:lambda:us-west-2:111122223333:function:lambda-example:$LATEST"
  ],
  "detail": {
    "scan-status": "INITIAL_SCAN_COMPLETE",
    "finding-severity-counts": {
      "CRITICAL": 0,
      "HIGH": 0,
      "MEDIUM": 0,
      "TOTAL": 0
    },
    "version": "1.0"
  }
}
```

Esempio di schema degli eventi di copertura di Amazon Inspector

Di seguito è riportato un esempio dello schema di eventi per un EventBridge evento Amazon Inspector per la copertura. Questo evento viene creato quando la copertura di scansione di Amazon Inspector per una risorsa viene modificata. I seguenti campi identificano un evento di copertura:

- Il `detail-type` campo è impostato su`Inspector2 Coverage`.
- L'`detail`oggetto contiene un `scanStatus` oggetto che indica il nuovo stato di scansione della risorsa.

```
{
    "version": "0",
    "id": "000adda5-0fbf-913e-bc0e-10f0376412aa",
    "detail-type": "Inspector2 Coverage",
    "source": "aws.inspector2",
    "account": "111122223333",
    "time": "2023-01-20T22:51:39Z",
    "region": "us-east-1",
    "resources": [
        "i-087d63509b8c97098"
    ],
    "detail": {
        "scanStatus": {
            "reason": "UNMANAGED_EC2_INSTANCE",
            "statusCodeValue": "INACTIVE"
        },
        "scanType": "PACKAGE",
        "eventTimestamp": "2023-01-20T22:51:35.665501Z",
        "version": "1.0"
    }
}
```

Integrazione delle scansioni di Amazon Inspector nella tua pipeline CI/CD

Puoi integrare le scansioni delle immagini dei container di Amazon Inspector direttamente nella tua pipeline CI/CD per individuare le vulnerabilità del software e fornire report alla fine della build. I report sulle vulnerabilità generati da Amazon Inspector consentono di esaminare e correggere i rischi prima della distribuzione.

L'integrazione CI/CD di Amazon Inspector utilizza una combinazione di Amazon Inspector SBOM Generator e Amazon Inspector Scan API per produrre report di vulnerabilità per le immagini dei container. Amazon Inspector SBOM Generator crea una distinta base del software (SBOM) da un'immagine del contenitore fornita, quindi l'API Amazon Inspector Scan analizza tale SBOM e crea un report con dettagli su eventuali vulnerabilità rilevate.

Puoi ottenere un'integrazione CI/CD con Amazon Inspector tramite i plug-in Amazon Inspector creati appositamente per singole soluzioni CI/CD e disponibili nel relativo marketplace, oppure puoi creare un'integrazione di scansione personalizzata.

Argomenti

Integrazione con i plugin

Amazon Inspector fornisce plug-in per le soluzioni CI/CD supportate. Puoi installare questi plugin dai rispettivi marketplace e poi utilizzarli per aggiungere Amazon Inspector Scans come fase di costruzione della tua pipeline. La fase di creazione del plug-in esegue il generatore Amazon Inspector SBOM sull'immagine fornita, quindi esegue l'API Amazon Inspector Scan sull'SBOM generato.

Di seguito è riportata una panoramica di come funziona un'integrazione CI/CD di Amazon Inspector tramite i plugin:

1. Si configura un Account AWS per consentire l'accesso all'API Amazon Inspector Scan. Per istruzioni, consulta Configurazione di un AWS account per utilizzare l'integrazione CI/CD di Amazon Inspector.
2. Installa il plug-in Amazon Inspector dal marketplace.
3. Installa e configura il binario Amazon Inspector SBOM Generator. Per istruzioni, consulta Generatore SBOM Amazon Inspector.
4. Aggiungi Amazon Inspector Scans come fase di compilazione nella tua pipeline CI/CD e configuri la scansione.
5. Quando esegui una build, il plug-in prende l'immagine del contenitore come input e quindi esegue Amazon Inspector SBOM Generator sull'immagine per generare un SBOM compatibile. CycloneDX
6. Da lì, il plug-in invia la SBOM generata a un endpoint dell'API Amazon Inspector Scan che valuta ogni componente SBOM alla ricerca di vulnerabilità.
7. La risposta dell'API Amazon Inspector Scan viene trasformata in un report di vulnerabilità nei formati CSV, SBOM JSON e HTML. Il rapporto contiene dettagli su eventuali vulnerabilità rilevate da Amazon Inspector.

Soluzioni CI/CD supportate

Amazon Inspector attualmente supporta le seguenti soluzioni CI/CD. Per istruzioni complete sulla configurazione dell'integrazione CI/CD tramite un plug-in, seleziona il plug-in per la tua soluzione CI/CD:

- Plugin Jenkins
- TeamCity Plugin

Integrazione personalizzata

Se Amazon Inspector non fornisce plug-in per la tua soluzione CI/CD, puoi creare un'integrazione CI/CD personalizzata utilizzando una combinazione di Amazon Inspector SBOM Generator e Amazon Inspector Scan API. Puoi anche utilizzare un'integrazione personalizzata per ottimizzare le scansioni utilizzando le opzioni disponibili tramite Amazon Inspector SBOM Generator.

Di seguito è riportata una panoramica di come funziona un'integrazione CI/CD personalizzata di Amazon Inspector:

1. Si configura un Account AWS per consentire l'accesso all'API Amazon Inspector Scan. Per istruzioni, consulta Configurazione di un AWS account per utilizzare l'integrazione CI/CD di Amazon Inspector.
2. Installa e configura il binario Amazon Inspector SBOM Generator. Per istruzioni, consulta Generatore SBOM Amazon Inspector.
3. Utilizzi Amazon Inspector SBOM Generator per generare un SBOM CycloneDX compatibile per l'immagine del contenitore.
4. Utilizzi l'API Amazon Inspector Scan sulla SBOM generata per produrre un report di vulnerabilità.

Per istruzioni sulla configurazione di un'integrazione personalizzata, consulta. Creazione di una propria integrazione di pipeline CI/CD personalizzata con Amazon Inspector Scan

Configurazione di un AWS account per utilizzare l'integrazione CI/CD di Amazon Inspector

È necessario registrarsi e Account AWS utilizzare l'integrazione CI/CD di Amazon Inspector. Account AWS Deve avere un ruolo IAM che consenta alla tua pipeline di accedere all'API Amazon Inspector Scan.

Completa le attività nei seguenti argomenti per registrarti Account AWS, creare un utente amministratore e configurare un ruolo IAM per l'integrazione CI/CD.

> **Note**
>
> Se ti sei già registrato per un Account AWS, puoi passare a. Configura un ruolo IAM per l'integrazione CI/CD

Argomenti

- Iscriviti a un Account AWS
- Creazione di un utente amministratore
- Configura un ruolo IAM per l'integrazione CI/CD

Iscriviti a un Account AWS

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

Per iscriverti a un Account AWS

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

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

   Quando ti iscrivi a un Account AWS, Utente root dell'account AWSviene creato un. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWS nell'account. Come best practice di sicurezza, assegna l'accesso amministrativo a un utente amministrativo e utilizza solo l'utente root per eseguire attività che richiedono l'accesso di un utente root.

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

Creazione di un utente amministratore

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

Proteggi i tuoi Utente root dell'account AWS

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

   Per informazioni sull'accesso utilizzando un utente root, consulta la pagina Signing in as the root user della Guida per l'utente di Accedi ad AWS .
2. Abilita l'autenticazione a più fattori (MFA) per l'utente root.

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

Creazione di un utente amministratore

1. Abilita Centro identità IAM.

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

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

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

Accesso come utente amministratore

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

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

Configura un ruolo IAM per l'integrazione CI/CD

Per integrare la scansione di Amazon Inspector nella tua pipeline CI/CD devi creare una policy IAM che consenta l'accesso all'API Amazon Inspector Scan che analizza la distinta base del software (SBOM). Quindi, puoi collegare tale policy a un ruolo IAM che il tuo account può assumere per eseguire l'API Amazon Inspector Scan.

1. Accedi AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM, scegli Policies, quindi scegli Create Policy.
3. In Policy Editor seleziona JSON e incolla la seguente dichiarazione:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
```

```
            "Effect": "Allow",
            "Action": "inspector-scan:ScanSbom",
            "Resource": "*"
        }
    ]
}
```

4. Seleziona Successivo.
5. Assegna un nome alla politica, ad esempio`InspectorCICDscan-policy`, e aggiungi una descrizione opzionale, quindi scegli Crea politica. Questa politica verrà allegata al ruolo che creerai nei passaggi successivi.
6. Nel riquadro di navigazione della console IAM, seleziona Ruoli, quindi seleziona Crea nuovo ruolo.
7. Per il tipo di entità affidabile, scegli Custom trust policy e incolla la seguente policy:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{ACCOUNT_ID}:root"
            },
            "Action": "sts:AssumeRole",
            "Condition": {}
        }
    ]
}
```

8. Seleziona Successivo.
9. In Aggiungi autorizzazioni cerca e seleziona la politica che hai creato in precedenza, quindi scegli Avanti.
10. Assegna un nome al ruolo, ad esempio`InspectorCICDscan-role`, e aggiungi una descrizione opzionale, quindi scegli`Create Role`.

Generatore SBOM Amazon Inspector

Amazon Inspector SBOM Generator (Sbomgen) è uno strumento binario che produce una distinta base del software (SBOM) per l'immagine di un contenitore. Un SBOM è un inventario raccolto del software installato su un sistema.

Sbomgenfunziona mediante la scansione dei file che notoriamente contengono informazioni sui pacchetti installati. Se viene trovato uno di questi file, lo strumento estrae i nomi dei pacchetti, le versioni e altri metadati. I metadati di questo pacchetto vengono quindi trasformati in un SBOM. CycloneDX

Sbomgenpuò essere usato come strumento autonomo per fornire CycloneDX SBOM come file o a STDOUT. Viene anche utilizzato come parte dell'integrazione CI/CD di Amazon Inspector, che esegue automaticamente la scansione delle immagini dei container come parte della pipeline di distribuzione. Per ulteriori informazioni, consulta Integrazione delle scansioni di Amazon Inspector nella tua pipeline CI/CD.

Pacchetti e formati di immagine supportati

Al momento, Sbomgen può raccogliere l'inventario per i seguenti tipi di pacchi:

- Alpine APK
- Debian / Ubuntu DPKG
- Red Hat RPM
- Gopacchi tramite `go.mod` e `go mod cache`
- Javapacchi tramite `pom.properties`
- Node.jspacchetti tramite `package.json` file all'interno `node_modules`
- Pacchetti C# tramite file Nuget (`.deps.json`,,, `csproj` packages.lock.json) `Packages.config`
- PHP `installed.json` tramite e `composer.lock`
- Pythonpacchetti tramite`requirements.txt`, `Pipfile.lock`poetry.lock, e file `egg/wheel`
- Rubypacchetti tramite `Gemfile.lock` `.gemspec` gems e installate globalmente
- Rustpacchetti tramite e `Cargo.lock` `Cargo.toml`

Sbomgensupporta i seguenti formati di manifesto di immagini di immagini di contenitori:

- manifesto di immagini OCI
- Dockermanifesto di immagini versione 2, schema 2
- Dockerimage manifest versione 2, schema 1
- Dockerimage manifest versione 1

> **Important**
>
> Sbomgennon può scansionare le immagini dei contenitori se hanno dimensioni superiori a 5 GB, hanno più di 60 livelli o più di 2.000 pacchetti installati.

Installazione di Amazon Inspector SBOM Generator () Sbomgen

Sbomgenè disponibile solo per i sistemi operativi Linux. Se lo si utilizza per analizzare le immagini dei container, è necessario che sia installato un servizio contenitore, ad esempio Docker Podman, ocontainerd.

Per prestazioni ottimali, consigliamo di eseguire il file binario da un sistema con queste specifiche hardware minime:

- CPU 4x core
- 8 GB RAM

Per installare Sbomgen

1. Scarica il file Sbomgen zip dall'URL corretto per la tua architettura:

   Linux AMD64:

   https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/amd64/inspector-sbomgen.zip

   Linux ARM64:

   https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/arm64/inspector-sbomgen.zip
2. Decomprimi il download usando il seguente comando:

```
unzip inspector-sbomgen.zip
```

3. Verifica la presenza dei seguenti file nell'archivio:

   - `inspector-sbomgen`— Questo è il file binario che eseguirete per generare gli SBOM.
   - `README.txt`— Questa è la documentazione per l'utilizzoSbomgen.
   - `LICENSE.txt`— Questo file contiene la licenza del software perSbomgen.
   - `licenses`— Questa cartella contiene informazioni sulla licenza per i pacchetti di terze parti utilizzati daSbomgen.
   - `checksums.txt`— Questo file fornisce gli hash del file Sbomgen binario.
   - `sbom.json`— Questo è un CycloneDX SBOM per il file binario. Sbomgen
4. (Facoltativo) Verificate l'autenticità e l'integrità del file binario utilizzando il seguente comando:

   ```
   sha256sum < inspector-sbomgen
   ```

   - Confronta i risultati con il contenuto del `checksums.txt` file.
5. Concedi le autorizzazioni eseguibili al file binario utilizzando il seguente comando:

   ```
   chmod +x inspector-sbomgen
   ```
6. Verificate che Sbomgen sia stato installato correttamente utilizzando il seguente comando:

   ```
   ./inspector-sbomgen --version
   ```

   L'output dovrebbe essere simile al seguente:

   ```
   Version: 1.X.X
   ```

Uso di Sbomgen

È possibile utilizzarlo Sbomgen per generare un SBOM per le immagini dei contenitori.

È inoltre possibile personalizzare i risultati della generazione SBOM tramite opzioni quali l'esclusione di file specifici o la definizione dei pacchetti ricercati dallo strumento. Per esempi di questi casi d'uso e altro ancora, esegui il comando seguente:

```
./inspector-sbomgen list-examples
```

Per generare un SBOM per un'immagine del contenitore e inviare il risultato in un file

Per questo esempio, *image:tag*sostituitelo con l'ID dell'immagine e *output_path.json*con il percorso in cui salvare l'output in:

```
./inspector-sbomgen container --image image:tag -o output_path.json
```

Autenticazione nei registri privati con Sbomgen

È possibile generare un SBOM dai contenitori ospitati in registri privati fornendo le credenziali di autenticazione del registro privato. È possibile fornire le credenziali in diversi modi: tramite credenziali memorizzate nella cache, tramite un metodo interattivo o tramite un metodo non interattivo in cui le credenziali vengono fornite come variabili di ambiente prima dell'esecuzione. Sbomgen

Autenticazione tramite credenziali memorizzate nella cache (scelta consigliata)

1. Sbomgenproverà a utilizzare le credenziali memorizzate nella cache, se disponibili sul tuo agente. Per questo metodo, esegui prima l'autenticazione nel registro dei contenitori. Ad esempio, se utilizziDocker, puoi autenticarti nel registro utilizzando il Docker `login` comando:

   ```
   docker login
   ```
2. Quindi, dopo aver effettuato con successo l'autenticazione nel registro privato, è possibile utilizzarla Sbomgen su un'immagine del contenitore in quel registro. Per utilizzare l'esempio seguente, sostituiscilo *image:tag*con il nome dell'immagine da scansionare:

   ```
   ./inspector-sbomgen container --image image:tag
   ```

Autenticazione mediante il metodo interattivo

- Per questo metodo, fornisci il tuo nome utente come parametro e ti Sbomgen verrà richiesto di inserire una password sicura quando necessario. Per utilizzare l'esempio seguente, *image:tag*sostituiscilo con il nome dell'immagine da scansionare e *your_username*con un nome utente che abbia accesso a quell'immagine:

  ```
  ./inspector-sbomgen container --image image:tag --username
  your_username
  ```

Autenticazione tramite metodo non interattivo

- Per utilizzare questo metodo, è necessario archiviare la password o il token di registro in un file.txt leggibile solo dall'utente corrente. Il file di testo deve contenere solo la password o il

token su un'unica riga. Per utilizzare l'esempio seguente, sostituiscilo *your_username*con il tuo nome utente, sostituiscilo *password.txt*con il file contenente la password o il token e *image:tag*sostituiscilo con il nome dell'immagine da scansionare:

```
INSPECTOR_SBOMGEN_USERNAME=your_username\
INSPECTOR_SBOMGEN_PASSWORD=`cat password.txt` \
./inspector-sbomgen container --image image:tag
```

Esempi di risultati da Sbomgen

Di seguito è riportato un esempio di SBOM per un'immagine di contenitore inventariata utilizzando. Sbomgen

Immagine del contenitore (SBOM)


```
{
  "bomFormat": "CycloneDX",
  "specVersion": "1.5",
  "serialNumber": "urn:uuid:828875ef-8c32-4777-b688-0af96f3cf619",
  "version": 1,
  "metadata": {
    "timestamp": "2023-11-17T21:36:38Z",
    "tools": [
      {
        "vendor": "Amazon Web Services, Inc. (AWS)",
        "name": "Amazon Inspector SBOM Generator",
        "version": "1.0.0",
        "hashes": [
          {
            "alg": "SHA-256",
            "content":
 "10ab669cfc99774786301a745165b5957c92ed9562d19972fbf344d4393b5eb1"
          }
        ]
      }
    ],
    "component": {
      "bom-ref": "comp-1",
      "type": "container",
      "name": "fedora:latest",
      "properties": [
```

```
        {
          "name": "amazon:inspector:sbom_generator:image_id",
          "value":
 "sha256:c81c8ae4dda7dedc0711daefe4076d33a88a69a28c398688090c1141eff17e50"
        },
        {
          "name": "amazon:inspector:sbom_generator:layer_diff_id",
          "value":
 "sha256:eddd0d48c295dc168d0710f70364581bd84b1dda6bb386c4a4de0b61de2f2119"
        }
      ]
    }
  },
  "components": [
    {
      "bom-ref": "comp-2",
      "type": "library",
      "name": "dnf",
      "version": "4.18.0",
      "purl": "pkg:pypi/dnf@4.18.0",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
          "value": "/usr/lib/python3.12/site-packages/dnf-4.18.0.dist-info/METADATA"
        },
        {
          "name": "amazon:inspector:sbom_generator:is_duplicate_package",
          "value": "true"
        },
        {
          "name": "amazon:inspector:sbom_generator:duplicate_purl",
          "value": "pkg:rpm/fedora/python3-dnf@4.18.0-2.fc39?
arch=noarch&distro=39&epoch=0"
        }
      ]
    },
```

```
    {
      "bom-ref": "comp-3",
      "type": "library",
      "name": "libcomps",
      "version": "0.1.20",
      "purl": "pkg:pypi/libcomps@0.1.20",
      "properties": [
        {
          "name": "amazon:inspector:sbom_generator:source_file_scanner",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_package_collector",
          "value": "python-pkg"
        },
        {
          "name": "amazon:inspector:sbom_generator:source_path",
          "value": "/usr/lib64/python3.12/site-packages/libcomps-0.1.20-py3.12.egg-
info/PKG-INFO"
        },
        {
          "name": "amazon:inspector:sbom_generator:is_duplicate_package",
          "value": "true"
        },
        {
          "name": "amazon:inspector:sbom_generator:duplicate_purl",
          "value": "pkg:rpm/fedora/python3-libcomps@0.1.20-1.fc39?
arch=x86_64&distro=39&epoch=0"
        }
      ]
    }
  ]
}
```


Creazione di una propria integrazione di pipeline CI/CD personalizzata con Amazon Inspector Scan

Ti consigliamo di utilizzare i plugin CI/CD di Amazon Inspector se sono disponibili nel tuo marketplace CI/CD. Per un elenco dei plugin disponibili, consulta. Soluzioni CI/CD supportate

Se Amazon Inspector non fornisce plug-in per la tua soluzione CI/CD, puoi creare un'integrazione CI/CD personalizzata utilizzando una combinazione di Amazon Inspector SBOM Generator e Amazon

Inspector Scan API. Puoi anche utilizzare un'integrazione personalizzata per ottimizzare le scansioni tramite le opzioni disponibili in Amazon Inspector SBOM Generator.

Per configurare la tua integrazione personalizzata

1. Configura un Account AWS file per consentire l'accesso all'API Amazon Inspector Scan. Per istruzioni, consulta Configurazione di un AWS account per utilizzare l'integrazione CI/CD di Amazon Inspector.
2. Installa e configura il binario Amazon Inspector SBOM Generator. Per istruzioni, consulta Installazione di Amazon Inspector SBOM Generator () Sbomgen.
3. Utilizza il generatore SBOM per creare un file SBOM per l'immagine di un contenitore che desideri scansionare. Per utilizzare l'esempio seguente, sostituitelo *image:id* con il nome dell'immagine da scansionare e *sbom_path.json* con la posizione in cui salvare l'output SBOM:

   ```
   ./inspector-sbomgen container –image image:id -o sbom_path.json
   ```
4. Chiamate l'`inspector-scan`API per scansionare l'SBOM generato e fornire un rapporto di vulnerabilità. Per utilizzare l'esempio seguente, sostituisci *sbom_path.json con il percorso del file di un file SBOM* compatibile con CyclonedX valido. *Quindi sostituisci ENDPOINT con l'endpoint API per la quale sei attualmente autenticato e sostituisci REGION con la regione corrispondente Regione AWS .* Endpoint per l'API Amazon Inspector ScanPer un elenco completo delle regioni e degli endpoint, consulta la sezione.

   ```
   aws inspector-scan scan-sbom --sbom file://sbom_path.json --endpoint
   "ENDPOINT" --region REGION
   ```

Formati di output delle API

L'API Amazon Inspector Scan può generare un report di vulnerabilità in formato CycloneDX 1.5 o Amazon Inspector che trova JSON. L'impostazione predefinita può essere modificata utilizzando il flag. `--output-format`

Esempio di output in formato CycloneDX 1.5

```
{
  "status": "SBOM parsed successfully, 1 vulnerabilities found",
  "sbom": {
    "bomFormat": "CycloneDX",
```

```
    "specVersion": "1.5",
    "serialNumber": "urn:uuid:0077b45b-ff1e-4dbb-8950-ded11d8242b1",
    "metadata": {
      "properties": [
        {
          "name": "amazon:inspector:sbom_scanner:critical_vulnerabilities",
          "value": "1"
        },
        {
          "name": "amazon:inspector:sbom_scanner:high_vulnerabilities",
          "value": "0"
        },
        {
          "name": "amazon:inspector:sbom_scanner:medium_vulnerabilities",
          "value": "0"
        },
        {
          "name": "amazon:inspector:sbom_scanner:low_vulnerabilities",
          "value": "0"
        }
      ],
      "tools": [
        {
          "name": "CycloneDX SBOM API",
          "vendor": "Amazon Inspector",
          "version": "empty:083c9b00:083c9b00:083c9b00"
        }
      ],
      "timestamp": "2023-06-28T14:15:53.760Z"
    },
    "components": [
      {
        "bom-ref": "comp-1",
        "type": "library",
        "name": "log4j-core",
        "purl": "pkg:maven/org.apache.logging.log4j/log4j-core@2.12.1",
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:path",
            "value": "/home/dev/foo.jar"
          }
        ]
      }
    ],
```

```
    "vulnerabilities": [
      {
        "bom-ref": "vuln-1",
        "id": "CVE-2021-44228",
        "source": {
          "name": "NVD",
          "url": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228"
        },
        "references": [
          {
            "id": "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            }
          },
          {
            "id": "GHSA-jfh8-c2jp-5v3q",
            "source": {
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            }
          }
        ],
        "ratings": [
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v3-1/"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          },
          {
            "source": {
              "name": "NVD",
              "url": "https://www.first.org/cvss/v2/"
            },
            "score": 9.3,
            "severity": "critical",
            "method": "CVSSv2",
```

```
            "vector": "AC:M/Au:N/C:C/I:C/A:C"
          },
          {
            "source": {
              "name": "EPSS",
              "url": "https://www.first.org/epss/"
            },
            "score": 0.97565,
            "severity": "none",
            "method": "other",
            "vector": "model:v2023.03.01,date:2023-06-27T00:00:00+0000"
          },
          {
            "source": {
              "name": "SNYK",
              "url": "https://security.snyk.io/vuln/SNYK-JAVA-
ORGAPACHELOGGINGLOG4J-2314720"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
          },
          {
            "source": {
              "name": "GITHUB",
              "url": "https://github.com/advisories/GHSA-jfh8-c2jp-5v3q"
            },
            "score": 10.0,
            "severity": "critical",
            "method": "CVSSv31",
            "vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
          }
        ],
        "cwes": [
          400,
          20,
          502
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
 releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
 and parameters do not protect against attacker controlled LDAP and other JNDI related
 endpoints. An attacker who can control log messages or log message parameters can
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
```

```
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "advisories": [
          {
            "url": "https://www.intel.com/content/www/us/en/security-center/advisory/
intel-sa-00646.html"
          },
          {
            "url": "https://support.apple.com/kb/HT213189"
          },
          {
            "url": "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/"
          },
          {
            "url": "https://logging.apache.org/log4j/2.x/security.html"
          },
          {
            "url": "https://www.debian.org/security/2021/dsa-5020"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf"
          },
          {
            "url": "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpujan2022.html"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf"
          },
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf"
          },
          {
            "url": "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf"
          },
```

```
          {
            "url": "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/"
          },
          {
            "url": "https://www.oracle.com/security-alerts/cpuapr2022.html"
          },
          {
            "url": "https://twitter.com/kurtseifried/status/1469345530182455296"
          },
          {
            "url": "https://tools.cisco.com/security/center/content/
CiscoSecurityAdvisory/cisco-sa-apache-log4j-qRuKNEbd"
          },
          {
            "url": "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html"
          },
          {
            "url": "https://www.kb.cert.org/vuls/id/930724"
          }
        ],
        "created": "2021-12-10T10:15:00Z",
        "updated": "2023-04-03T20:15:00Z",
        "affects": [
          {
            "ref": "comp-1"
          }
        ],
        "properties": [
          {
            "name": "amazon:inspector:sbom_scanner:exploit_available",
            "value": "true"
          },
          {
            "name": "amazon:inspector:sbom_scanner:exploit_last_seen_in_public",
            "value": "2023-03-06T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:cisa_kev_date_added",
            "value": "2021-12-10T00:00:00Z"
          },
          {
            "name": "amazon:inspector:sbom_scanner:cisa_kev_date_due",
            "value": "2021-12-24T00:00:00Z"
```

```
          },
          {
            "name": "amazon:inspector:sbom_scanner:fixed_version:comp-1",
            "value": "2.15.0"
          }
        ]
      }
    ]
  }
}
```

Esempio di output in formato Inspector

```
                      {
  "status": "SBOM parsed successfully, 1 vulnerability found",
  "inspector": {
    "messages": [
      {
        "name": "foo",
        "purl": "pkg:maven/foo@1.0.0", // Will not exist in output if missing in sbom
        "info": "Component skipped: no rules found."
      }
    ],
    "vulnerability_count": {
      "critical": 1,
      "high": 0,
      "medium": 0,
      "low": 0
    },
    "vulnerabilities": [
      {
        "id": "CVE-2021-44228",
        "severity": "critical",
        "source": "https://nvd.nist.gov/vuln/detail/CVE-2021-44228",
        "related": [
          "SNYK-JAVA-ORGAPACHELOGGINGLOG4J-2314720",
          "GHSA-jfh8-c2jp-5v3q"
        ],
        "description": "Apache Log4j2 2.0-beta9 through 2.15.0 (excluding security
  releases 2.12.2, 2.12.3, and 2.3.1) JNDI features used in configuration, log messages,
  and parameters do not protect against attacker controlled LDAP and other JNDI related
  endpoints. An attacker who can control log messages or log message parameters can
```

```
 execute arbitrary code loaded from LDAP servers when message lookup substitution is
 enabled. From log4j 2.15.0, this behavior has been disabled by default. From version
 2.16.0 (along with 2.12.2, 2.12.3, and 2.3.1), this functionality has been completely
 removed. Note that this vulnerability is specific to log4j-core and does not affect
 log4net, log4cxx, or other Apache Logging Services projects.",
        "references": [
          "https://www.intel.com/content/www/us/en/security-center/advisory/intel-
sa-00646.html",
          "https://support.apple.com/kb/HT213189",
          "https://msrc-blog.microsoft.com/2021/12/11/microsofts-response-to-
cve-2021-44228-apache-log4j2/",
          "https://logging.apache.org/log4j/2.x/security.html",
          "https://www.debian.org/security/2021/dsa-5020",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-479842.pdf",
          "https://www.oracle.com/security-alerts/alert-cve-2021-44228.html",
          "https://www.oracle.com/security-alerts/cpujan2022.html",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-714170.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/M5CSVUNV4HWZZXGOKNSK6L7RPM7BOKIB/",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-397453.pdf",
          "https://cert-portal.siemens.com/productcert/pdf/ssa-661247.pdf",
          "https://lists.fedoraproject.org/archives/list/package-
announce@lists.fedoraproject.org/message/VU57UJDCFIASIO35GC55JMKSRXJMCDFM/",
          "https://www.oracle.com/security-alerts/cpuapr2022.html",
          "https://twitter.com/kurtseifried/status/1469345530182455296",
          "https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-
sa-apache-log4j-qRuKNEbd",
          "https://lists.debian.org/debian-lts-announce/2021/12/msg00007.html",
          "https://www.kb.cert.org/vuls/id/930724"
        ],
        "created": "2021-12-10T10:15:00Z",
        "updated": "2023-04-03T20:15:00Z",
        "properties": {
          "cisa_kev_date_added": "2021-12-10T00:00:00Z",
          "cisa_kev_date_due": "2021-12-24T00:00:00Z",
          "cwes": [
            400,
            20,
            502
          ],
          "cvss": [
            {
              "source": "NVD",
              "severity": "critical",
```

```
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H",
              "cvss2_base_score": 9.3,
              "cvss2_base_vector": "AC:M/Au:N/C:C/I:C/A:C"
            },
            {
              "source": "SNYK",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H/E:H"
            },
            {
              "source": "GITHUB",
              "severity": "critical",
              "cvss3_base_score": 10.0,
              "cvss3_base_vector": "AV:N/AC:L/PR:N/UI:N/S:C/C:H/I:H/A:H"
            }
          ],
          "epss": 0.97565,
          "exploit_available": true,
          "exploit_last_seen_in_public": "2023-03-06T00:00:00Z"
        },
        "affects": [
          {
            "installed_version": "pkg:maven/org.apache.logging.log4j/log4j-
core@2.12.1",
            "fixed_version": "2.15.0",
            "path": "/home/dev/foo.jar"
          }
        ]
      }
    ]
  }
}
```


Utilizzo del plug-in Amazon Inspector Jenkins

Il Jenkins plug-in sfrutta il binario Amazon Inspector SBOM Generator e l'API Amazon Inspector Scan per produrre report dettagliati alla fine della build, in modo da poter analizzare e correggere i rischi prima della distribuzione.

Amazon Inspector è un servizio di gestione delle vulnerabilità che analizza le immagini dei container alla ricerca di vulnerabilità del sistema operativo e dei pacchetti del linguaggio di programmazione in base ai CVE.

Utilizzando il Jenkins plug-in Amazon Inspector, puoi aggiungere scansioni di vulnerabilità di Amazon Inspector alla tua pipeline. Jenkins

> **Note**
>
> Le scansioni delle vulnerabilità di Amazon Inspector possono essere configurate per superare o fallire le esecuzioni della pipeline in base al numero e alla gravità delle vulnerabilità rilevate.

Puoi visualizzare la versione più recente del Jenkins plug-in nel marketplace all'indirizzo https://plugins.jenkins.io//. Jenkins amazon-inspector-image-scanner

I passaggi seguenti descrivono come configurare il plug-in Amazon Inspector Jenkins.

> **Important**
>
> Prima di completare i seguenti passaggi, è necessario aggiornare Jenkins alla versione 2.387.3 o superiore per consentire l'esecuzione del plug-in.

Fase 1: Configura un Account AWS

Configura un Account AWS con un ruolo IAM che consenta l'accesso all'API Amazon Inspector Scan. Per istruzioni, consulta Configurazione di un AWS account per utilizzare l'integrazione CI/CD di Amazon Inspector.

Fase 2: Installa il plugin Amazon Inspector Jenkins

La procedura seguente descrive come installare il plug-in Amazon Inspector Jenkins dalla dashboard. Jenkins

1. Dalla dashboard di Jenkins, scegli Manage Jenkins, quindi scegli Manage Plugins.
2. Scegli Disponibile.
3. Dalla scheda Available, cerca Amazon Inspector Scans, quindi installa il plug-in.

(Facoltativo) Fase 3. Aggiungi le credenziali docker a Jenkins

> **Note**
>
> Aggiungi le credenziali docker solo se l'immagine docker si trova in un repository privato. In caso contrario, puoi ignorare questo passaggio.

La procedura seguente descrive come aggiungere credenziali docker Jenkins dalla dashboard. Jenkins

1. Dalla dashboard di Jenkins, scegli Gestisci Jenkins, Credenziali e quindi Sistema.
2. Scegli Credenziali globali, quindi Aggiungi credenziali.
3. Per Tipo, seleziona Nome utente con password.
4. Per Scope, seleziona Global (Jenkins, nodes, items, all child items, ecc.).
5. Inserisci i tuoi dati, quindi scegli OK.

(Facoltativo) Fase 4. Aggiungere AWS credenziali

> **Note**
>
> Aggiungi AWS le credenziali solo se desideri autenticarti in base a un utente IAM. In caso contrario, puoi ignorare questo passaggio.

La procedura seguente descrive come aggiungere AWS credenziali dalla dashboard. Jenkins

1. Dalla dashboard Jenkins, scegli Gestisci Jenkins, Credenziali e quindi Sistema.
2. Scegli Credenziali globali, quindi Aggiungi credenziali.
3. Per Tipo, seleziona AWS Credentials.
4. Inserisci i tuoi dati, tra cui l'ID della chiave di accesso e la chiave di accesso segreta, quindi scegli OK.

Fase 5. Aggiungi il supporto CSS in uno Jenkins script

La procedura seguente descrive come aggiungere il supporto CSS in uno Jenkikns script.

1. Riavvia Jenkins.
2. Dalla dashboard, scegli Manage Jenkins, Nodes, Built-In Node e quindi Script Console.
3. Nella casella di testo, aggiungi la rigaSystem.setProperty("hudson.model.DirectoryBrowserSupport.CSP", ""), quindi scegli Esegui.

Fase 6. Aggiungi Amazon Inspector Scan alla tua build

Puoi aggiungere Amazon Inspector Scan alla tua build aggiungendo una fase di compilazione nel tuo progetto o utilizzando la pipeline Jenkins dichiarativa.

Amazon Inspector Scansiona la tua build aggiungendo una fase di compilazione al tuo progetto

1. Nella pagina di configurazione, scorri verso il basso fino a Build Steps e scegli Aggiungi fase di compilazione. Quindi seleziona Amazon Inspector Scan.
2. Scegli tra due metodi di installazione di inspector-sbomgen: automatico o manuale.

   a. (Opzione 1) Scegli Automatico per scaricare l'ultima versione di inspector-sbomgen. Se scegli questo metodo, assicurati di selezionare l'architettura della CPU che corrisponde al sistema che esegue il plugin.

   b. (Opzione 2) Scegli Manuale se desideri configurare il binario Amazon Inspector SBOM Generator per la scansione. Se scegli questo metodo, assicurati di fornire il percorso completo di una versione di inspector-sbomgen scaricata in precedenza.

   Per ulteriori informazioni, consulta Installazione di Amazon Inspector SBOM Generator (Sbomgen) in Amazon Inspector SBOM Generator.
3. Completa quanto segue per completare la configurazione della fase di compilazione di Amazon Inspector Scan:

   a. Inserisci il tuo ID immagine. L'immagine può essere locale, remota o archiviata. I nomi delle immagini devono seguire la convenzione di Docker denominazione. Se state analizzando un'immagine esportata, fornite il percorso del file tar previsto. Vedi il seguente esempio di percorsi Image Id:

      i. Per contenitori locali o remoti: NAME[:TAG|@DIGEST]

ii. Per un file tar: `/path/to/image.tar`

b. Seleziona un tramite Regione AWSil quale inviare la richiesta di scansione.

c. (Facoltativo) Per le credenziali Docker, seleziona il tuo nome utenteDocker. Esegui questa operazione solo se l'immagine del contenitore si trova in un repository privato.

d. (Facoltativo) È possibile fornire i seguenti metodi di AWS autenticazione supportati:

i. (Facoltativo) Per il ruolo IAM, fornisci un ruolo ARN (arn:aws:iam: :role/). *`AccountNumberRoleName`*

ii. (Facoltativo) Per le credenziali AWS, seleziona Id per l'autenticazione in base a un utente IAM.

iii. (Facoltativo) Per il nome del AWS profilo, fornisci il nome di un profilo da autenticare utilizzando un nome di profilo.

e. (Facoltativo) Specificare le soglie di vulnerabilità per gravità. Se il numero specificato viene superato durante una scansione, la creazione dell'immagine avrà esito negativo. Se i valori sono tutti`0`, la compilazione avrà esito positivo, indipendentemente dal fatto che vengano rilevate eventuali vulnerabilità.

4. Selezionare Salva.

Aggiungi Amazon Inspector Scan alla tua build utilizzando la Jenkins pipeline dichiarativa

Puoi aggiungere Amazon Inspector Scan alla tua build utilizzando la pipeline dichiarativa Jenkins automaticamente o manualmente.

Per scaricare automaticamente la pipeline dichiarativa SBOMGen

- Per aggiungere Amazon Inspector Scan a una build, usa la seguente sintassi di esempio. In base all'architettura del sistema operativo preferita del download di Amazon Inspector SBOM Generator, sostituisci *`SBOMGEN_SOURCE con LinuxAMD64 o LinuxARM64`*. Sostituisci *`IMAGE_PATH`* con il percorso della tua immagine (ad esempio *`alpine:latest`*), IAM_ROLE *`con`* l'ARN del ruolo IAM che hai configurato nel passaggio 1 e *`ID con il tuo ID`* Docker credenziale se stai utilizzando un repository privato. Facoltativamente, puoi abilitare le soglie di vulnerabilità e specificare i valori per ogni gravità.

```
pipeline {
```

```
    agent any
    stages {
        stage('amazon-inspector-image-scanner') {
            steps {
                script {
                step([
                $class:
'com.amazon.inspector.jenkins.amazoninspectorbuildstep.AmazonInspectorBuilder',
                sbomgenSource: 'SBOMGEN_SOURCE', // this can be linuxAmd64 or linuxArm64
                archivePath: 'IMAGE_PATH',
                awsRegion: 'REGION',
                iamRole: 'IAM ROLE',
                credentialId: 'Id', // provide empty string if image not in private
repositories
                awsCredentialId: ''AWS ID;',
                awsProfileName: 'Profile Name',
                isThresholdEnabled: false,
                countCritical: 0,
                countHigh: 0,
                countLow: 10,
                countMedium: 5,
               ])
            }
          }
        }
    }
}
```

Per scaricare manualmente la pipeline dichiarativa SBOMGen

- Per aggiungere Amazon Inspector Scan a una build, usa la seguente sintassi di esempio. *Sostituisci SBOMGEN_PATH con il percorso dell'Amazon Inspector SBOM Generator che hai installato nella fase 3, IMAGE_PATH con il percorso dell'immagine (ad esempio alpine:latest), IAM_ROLE con l'ARN del ruolo IAM configurato nella fase 1 e ID con il tuo ID credenziale se utilizzi un repository privato.* Docker Facoltativamente, puoi abilitare le soglie di vulnerabilità e specificare i valori per ogni gravità.

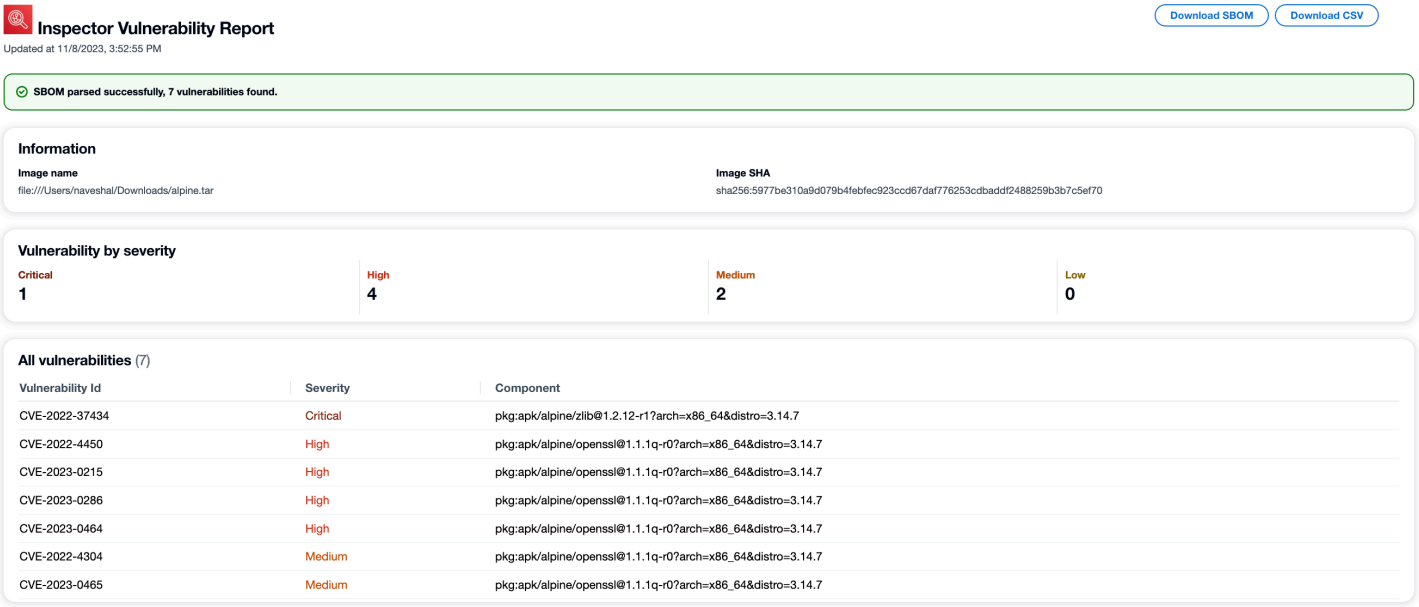
> **Note**
>
> *Inseriscilo Sbomgen nella directory Jenkins e fornisci il percorso della directory Jenkins nel plugin (ad esempio /opt/folder/arm64/inspector-sbomgen).*

```
pipeline {
    agent any
    stages {
        stage('amazon-inspector-image-scanner') {
            steps {
                script {
                step([
                $class:
 'com.amazon.inspector.jenkins.amazoninspectorbuildstep.AmazonInspectorBuilder',
                sbomgenPath: 'SBOMGEN_PATH',
                archivePath: 'IMAGE_PATH',
                awsRegion: 'REGION',
                iamRole: 'IAM ROLE',
                awsCredentialId: ''AWS ID;',
                credentialId: 'Id;', // provide empty string if image not in private
 repositories
                awsProfileName: 'Profile Name',
                isThresholdEnabled: false,
                countCritical: 0,
                countHigh: 0,
                countLow: 10,
                countMedium: 5,
               ])
            }
         }
       }
    }
 }
```

Fase 7. Visualizza il report sulla vulnerabilità di Amazon Inspector

1. Completa una nuova build del tuo progetto.

2. Al termine della compilazione, seleziona un formato di output dai risultati. Se selezioni HTML, hai la possibilità di scaricare una versione JSON SBOM o CSV del rapporto. Di seguito viene illustrato un esempio di report HTML:



Inspector Vulnerability Report

Updated at 11/8/2023, 3:52:55 PM

Download SBOM Download CSV

SBOM parsed successfully, 7 vulnerabilities found.

Information

Image name
file:///Users/naveshal/Downloads/alpine.tar

Image SHA
sha256:5977be310a9d079b4febfec923ccd67daf776253cdbaddf2488259b3b7c5ef70

Vulnerability by severity

Critical	High	Medium	Low
1	4	2	0

All vulnerabilities (7)

Vulnerability Id	Severity	Component
CVE-2022-37434	Critical	pkg:apk/alpine/zlib@1.2.12-r1?arch=x86_64&distro=3.14.7
CVE-2022-4450	High	pkg:apk/alpine/openssl@1.1.1q-r0?arch=x86_64&distro=3.14.7
CVE-2023-0215	High	pkg:apk/alpine/openssl@1.1.1q-r0?arch=x86_64&distro=3.14.7
CVE-2023-0286	High	pkg:apk/alpine/openssl@1.1.1q-r0?arch=x86_64&distro=3.14.7
CVE-2023-0464	High	pkg:apk/alpine/openssl@1.1.1q-r0?arch=x86_64&distro=3.14.7
CVE-2022-4304	Medium	pkg:apk/alpine/openssl@1.1.1q-r0?arch=x86_64&distro=3.14.7
CVE-2023-0465	Medium	pkg:apk/alpine/openssl@1.1.1q-r0?arch=x86_64&distro=3.14.7

Risoluzione dei problemi

Di seguito sono riportati gli errori più comuni che puoi riscontrare quando utilizzi il plug-in Amazon Inspector Scan per. Jenkins

Caricamento delle credenziali non riuscito o errore di eccezione

Errore:

```
InstanceProfileCredentialsProvider(): Failed to load credentials or sts exception.
```

Risoluzione

Ottieni `aws_access_key_id` e `aws_secret_access_key` per il tuo account. AWS Configura `aws_access_key_id` e `aws_secret_access_key` accedi`~/.aws/credentials`.

Errore di percorso Inspector-SBOMGen

Errore:

```
Exception:com.amazon.inspector.jenkins.amazoninspectorbuildstep.exception.Sbomge
There was an issue running inspector-sbomgen, is /opt/inspector/inspector-
sbomgen the correct path?
```

Risoluzione:

Completate la seguente procedura per risolvere il problema.

1. Inserisci l'architettura del sistema operativo corretta Inspector-SBOMGen nella Jenkins directory Per ulteriori informazioni, consulta Amazon Inspector SBOM Generator.
2. Concedi le autorizzazioni eseguibili al file binario utilizzando il seguente comando:. `chmod +x inspector-sbomgen`
3. Fornisci il percorso corretto del Jenkins computer nel plug-in, ad esempio`/opt/folder/arm64/inspector-sbomgen`.
4. Salva la configurazione ed esegui il Jenkins lavoro.

Utilizzo del plug-in Amazon Inspector TeamCity

Il TeamCity plug-in Amazon Inspector ti dà la possibilità di aggiungere scansioni di vulnerabilità di Amazon Inspector alla tua pipeline. TeamCity Il plug-in sfrutta il binario Amazon Inspector SBOM Generator e l'API Amazon Inspector Scan per produrre report dettagliati alla fine della build in modo da poter analizzare e correggere i rischi prima della distribuzione. Le scansioni possono anche essere configurate per dare esito positivo o negativo alle esecuzioni della pipeline in base al numero e alla gravità delle vulnerabilità rilevate.

Amazon Inspector è un servizio di gestione delle vulnerabilità offerto da Amazon Inspector AWS che analizza le immagini dei container alla ricerca di vulnerabilità del sistema operativo e dei pacchetti del linguaggio di programmazione in base ai CVE. Per ulteriori informazioni sull'integrazione CI/CD di Amazon Inspector, consulta. Integrazione delle scansioni di Amazon Inspector nella tua pipeline CI/CD

Per un elenco dei pacchetti e dei formati di immagine dei contenitori supportati dal plug-in Amazon Inspector, consulta,. Pacchetti e formati di immagine supportati

Puoi visualizzare la versione più recente del plug-in nel TeamCity marketplace all'indirizzo https://plugins.jetbrains.com/plugin/23236 - amazon-inspector-scanner. In alternativa, segui i passaggi indicati in ogni sezione di questo documento per configurare il plug-in Amazon Inspector TeamCity:

1. Configura un Account AWS.

   - Configura un Account AWS con un ruolo IAM che consenta l'accesso all'API Amazon Inspector Scan. Per istruzioni, consulta Configurazione di un AWS account per utilizzare l'integrazione CI/CD di Amazon Inspector.

2. Installa il plug-in Amazon InspectorTeamCity.

   a. Dalla dashboard, vai su Amministrazione > Plugin.

   b. Cerca le scansioni di Amazon Inspector.

   c. Installa il plugin .

3. Installa il generatore SBOM di Amazon Inspector.

   - Installa il binario Amazon Inspector SBOM Generator nella directory del tuo server Teamcity. Per istruzioni, consulta Installazione di Amazon Inspector SBOM Generator () Sbomgen.

4. Aggiungi una fase di compilazione di Amazon Inspector Scan al tuo progetto.

   a. Nella pagina di configurazione, scorri verso il basso fino a Build Steps, scegli Aggiungi fase di compilazione, quindi seleziona Amazon Inspector Scan.

   b. Configura la fase di compilazione di Amazon Inspector Scan inserendo i seguenti dettagli:

      - Aggiungi un nome per Step.
      - Scegli tra due metodi di installazione di Amazon Inspector SBOM Generator: automatico o manuale.
        - Scarica automaticamente la versione più recente di Amazon Inspector SBOM Generator in base all'architettura del sistema e della CPU.
        - Il manuale richiede di fornire un percorso completo a una versione precedentemente scaricata di Amazon Inspector SBOM Generator.

        Per ulteriori informazioni, consulta Installazione di Amazon Inspector SBOM Generator (Sbomgen) in Amazon Inspector SBOM Generator.
      - Inserisci il tuo ID immagine. L'immagine può essere locale, remota o archiviata. I nomi delle immagini devono seguire la convenzione di Docker denominazione. Se state analizzando un'immagine esportata, fornite il percorso del file tar previsto. Vedi il seguente esempio di percorsi Image Id:
        - Per contenitori locali o remoti: `NAME[:TAG|@DIGEST]`
        - Per un file tar: `/path/to/image.tar`

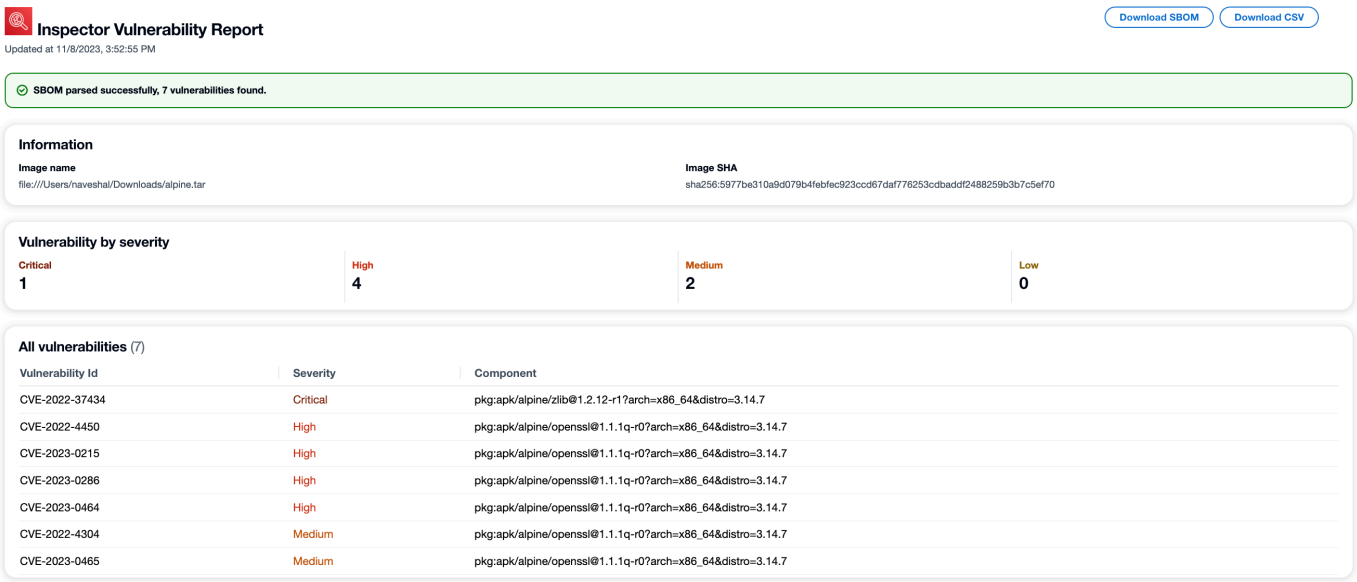
- Per IAM Role inserisci l'ARN per il ruolo che hai configurato nel passaggio 1.
- Seleziona un tramite Regione AWSil quale inviare la richiesta di scansione.
- (Facoltativo) Per l'autenticazione Docker, inserisci il tuo nome utente e la password Docker. Esegui questa operazione solo se l'immagine del contenitore si trova in un repository privato.
- (Facoltativo) Per AWS l'autenticazione, inserisci l'ID della chiave di AWS accesso e la chiave AWS segreta. Fatelo solo se desiderate autenticarvi in base alle AWS credenziali.
- (Facoltativo) Specificate le soglie di vulnerabilità per gravità. Se il numero specificato viene superato durante una scansione, la creazione dell'immagine avrà esito negativo. Se i valori sono tutti, `0` la compilazione avrà esito positivo indipendentemente dal numero di vulnerabilità rilevate.

c. Seleziona Salva.

5. Visualizza il report sulle vulnerabilità di Amazon Inspector.

a. Completa una nuova build del tuo progetto.

b. Una volta completata la build, seleziona un formato di output dai risultati. Quando selezioni HTML, hai la possibilità di scaricare una versione JSON SBOM o CSV del rapporto. Di seguito è riportato un esempio di report HTML:



Spazi dei nomi Amazon Inspector CycloneDX

Amazon Inspector dispone di CycloneDX namespace e nomi di proprietà riservati da utilizzare con SBOM prodotti da Amazon Inspector SBOM Generator e Amazon Inspector Scan API. Questa pagina documenta tutte le proprietà chiave/valore personalizzate che possono essere aggiunte ai componenti in CycloneDX SBOM creati utilizzando gli strumenti Amazon Inspector. Per ulteriori informazioni sulle tassonomie delle CycloneDX proprietà, consulta la documentazione ufficiale.

`amazon:inspector:sbom_scanner`tassonomia dei namespace

Lo spazio dei `amazon:inspector:sbom_scanner` nomi viene utilizzato dall'API Amazon Inspector Scan. Possiede le seguenti proprietà:

Proprietà	Descrizione
`amazon:inspector:sbom_scanner:critical_vulnerabilities`	Conteggio del numero totale di vulnerabilità di gravità critica rilevate nella SBOM.
`amazon:inspector:sbom_scanner:high_vulnerabilities`	Conteggio del numero totale di vulnerabilità ad alta gravità rilevate nello SBOM.
`amazon:inspector:sbom_scanner:medium_vulnerabilities`	Conteggio del numero totale di vulnerabilità di media gravità rilevate nello SBOM.
`amazon:inspector:sbom_scanner:low_vulnerabilities`	Conteggio del numero totale di vulnerabilità di bassa gravità rilevate nello SBOM.
`amazon:inspector:sbom_scanner:info`	Fornisce il contesto di scansione per un determinato componente, ad esempio: «Componente scansionato: nessuna vulnerabilità trovata».
`amazon:inspector:sbom_scanner:warning`	Fornisce il contesto del motivo per cui un determinato componente non è stato analizzato, ad esempio: «Componente ignorato: nessun purl fornito».

Proprietà	Descrizione
`amazon:inspector:sbom_scanner:fixed_version: component_bom_ref`	Fornisce la versione fissa del componente indicato per la vulnerabilità specificata.
`amazon:inspector:sbom_scanner:exploit_available`	Indica se è disponibile un exploit per la vulnerabilità specificata.
`amazon:inspector:sbom_scanner:exploit_last_seen_in_public`	Indica quando un exploit è stato visto l'ultima volta in pubblico per una determinata vulnerabilità.
`amazon:inspector:sbom_scanner:cisa_kev_date_added`	Indica quando la vulnerabilità è stata aggiunta al catalogo CISA Known Exploited Vulnerabilities.
`amazon:inspector:sbom_scanner:cisa_kev_date_due`	Indica quando è necessaria la correzione della vulnerabilità in base al catalogo CISA Known Exploited Vulnerabilities.
`amazon:inspector:sbom_scanner:path`	Il percorso del file che ha fornito le informazioni sull'oggetto del pacchetto.

`amazon:inspector:sbom_generator`tassonomia dei namespace

Lo spazio dei `amazon:inspector:sbom_generator` nomi viene utilizzato da Amazon Inspector SBOM Generator. Possiede le seguenti proprietà:

Proprietà	Descrizione
`amazon:inspector:sbom_generator:os_hostname`	Il nome host del sistema da inventariare.
`amazon:inspector:sbom_generator:kernel_name`	Il nome del kernel del sistema da inventariare.

Proprietà	Descrizione
`amazon:inspector:sbom_generator:kernel_version`	La versione del kernel del sistema da inventariare.
`amazon:inspector:sbom_generator:cpu_architecture`	L'architettura della CPU del sistema da inventariare, ad esempio x86_64.
`amazon:inspector:sbom_generator:image_id`	L'hash del file di configurazione dell'immagine del contenitore, noto anche come ID immagine.
`amazon:inspector:sbom_generator:layer_diff_id`	L'hash del livello di immagine del contenitore non compresso.
`amazon:inspector:sbom_generator:source_file_scanner`	Lo scanner che ha trovato il file che contiene le informazioni sul pacchetto, ad esempio:. `/var/lib/dpkg/status`
`amazon:inspector:sbom_generator:source_package_collector`	Il raccoglitore che ha estratto il nome e la versione del pacchetto da un file specifico.
`amazon:inspector:sbom_generator:source_path`	Il percorso del file da cui sono state estratte le informazioni del pacchetto oggetto.
`amazon:inspector:sbom_generator:is_duplicate_package`	Indica che il pacchetto oggetto è stato trovato da più di uno scanner di file.
`amazon:inspector:sbom_generator:go_toolchain`	Indica la versione del Go compilatore o della toolchain utilizzata per produrre un eseguibile Go.
`amazon:inspector:sbom_generator:expires_before`	la data precedente alla validità del certificato SSL.
`amazon:inspector:sbom_generator:expires_after`	la data dopo la quale il certificato SSL non è più valido.
`amazon:inspector:sbom_generator:is_expired`	un valore booleano che indica se il certificato SSL è scaduto.

Scansione automatizzata delle risorse con Amazon Inspector

La scansione senza agenti di Amazon Inspector per Amazon EC2 è disponibile in anteprima. L'utilizzo della funzionalità di scansione senza agenti di Amazon EC2 è soggetto alla Sezione 2 dei Termini di AWS servizio («Beta e anteprime»).

Amazon Inspector utilizza il proprio motore di scansione appositamente progettato. Questo motore monitora le risorse alla ricerca di vulnerabilità del software o percorsi di rete aperti che possono comportare carichi di lavoro compromessi, uso improprio delle risorse o accesso non autorizzato ai dati. Quando Amazon Inspector rileva una vulnerabilità, crea una scoperta. I risultati includono dettagli associati al rilevamento per aiutarti a correggere la vulnerabilità. Puoi esaminare i risultati sulla console Amazon Inspector e utilizzando l'API Amazon Inspector. Per ulteriori informazioni, consulta Gestione dei risultati in Amazon Inspector.

Una volta attivato, Amazon Inspector rileva automaticamente tutte le risorse idonee e avvia scansioni continue di tali risorse. Amazon Inspector analizza le vulnerabilità del software e l'esposizione involontaria della rete. Amazon Inspector esegue anche scansioni in risposta a eventi, come l'installazione di una nuova applicazione o patch.

Quando attivi Amazon Inspector per la prima volta, il tuo account viene registrato automaticamente a tutti i tipi di scansione. I seguenti argomenti coprono dettagli specifici sui tipi di scansione forniti da Amazon Inspector. Amazon Inspector classifica i tipi di scansione in base al tipo di risorsa interessata da una vulnerabilità. I seguenti argomenti illustrano le risorse scansionate da Amazon Inspector, cosa avvia nuove scansioni per tali risorse e come configurare le scansioni per ogni tipo di risorsa.

Argomenti

Quando attivi Amazon Inspector per la prima volta, il tuo account viene registrato automaticamente nei seguenti tipi di scansione: scansione Amazon Amazon EC2, scansione Amazon ECR, scansione standard Lambda. La scansione del codice Lambda è un livello opzionale di scansione delle funzioni Lambda che puoi attivare in qualsiasi momento.

Panoramica dei tipi di scansione di Amazon Inspector

Amazon Inspector offre una gamma di diversi tipi di scansione incentrati su tipi di risorse specifici nel tuo AWS ambiente.

Scansione Amazon EC2

Quando attivi la scansione Amazon EC2, Amazon Inspector analizza le tue istanze Amazon EC2 alla ricerca di vulnerabilità dei pacchetti del sistema operativo e del linguaggio di programmazione e della raggiungibilità della rete. Amazon Inspector analizza l'istanza EC2 alla ricerca di vulnerabilità ed esposizioni comuni (CVE) e problemi di esposizione della rete. Amazon Inspector esegue le scansioni utilizzando l'agente SSM installato sull'istanza o tramite istantanee delle istanze di Amazon EBS. Per ulteriori informazioni sulle scansioni per Amazon EC2, consulta. Scansione delle istanze Amazon EC2 con Amazon Inspector

Scansione Amazon ECR

Quando attivi la scansione Amazon ECR, Amazon Inspector converte tutti i repository di container con scansione di base nel tuo registro privato in scansione avanzata con scansione continua. Puoi anche configurare facoltativamente questa impostazione per eseguire la scansione solo in modalità push o per scansionare determinati repository tramite regole di inclusione. Tutte le immagini inviate negli ultimi 30 giorni o recuperate negli ultimi 90 giorni vengono inizialmente scansionate. Amazon Inspector continua a monitorare le immagini per una durata di 90 giorni per impostazione predefinita, questa impostazione può essere modificata in qualsiasi momento. Per ulteriori informazioni sulle scansioni per Amazon ECR, consulta. Scansione delle immagini dei container Amazon ECR con Amazon Inspector

Scansione standard Lambda

Quando attivi la scansione standard Lambda, Amazon Inspector rileva le funzioni Lambda nel tuo account e avvia immediatamente la scansione per individuare eventuali vulnerabilità. Amazon Inspector analizza nuove funzioni e layer Lambda quando vengono distribuiti e li scansiona nuovamente quando vengono aggiornati o quando vengono pubblicati nuovi Common Vulnerabilities and Exposures (CVE). Per ulteriori informazioni sulla scansione della funzione Lambda, vedere. AWS Lambda Funzioni di scansione con Amazon Inspector

Scansione standard Lambda + scansione del codice Lambda

Questa opzione può combinare la scansione standard Lambda con la scansione del codice Lambda. Quando la scansione del codice Lambda è attivata, Amazon Inspector rileva le funzioni e i livelli Lambda nel tuo account e analizza le vulnerabilità del codice e le dipendenze del pacchetto applicativo. La scansione del codice Lambda analizza il codice dell'applicazione personalizzato nelle funzioni Lambda alla ricerca di vulnerabilità del codice. Questi due tipi di scansione devono essere attivati insieme. Per ulteriori informazioni, consulta Scansione del codice Amazon Inspector Lambda.

Attivazione di un tipo di scansione

Puoi attivare un nuovo tipo di scansione Amazon Inspector in qualsiasi momento. Una volta attivato un tipo di scansione, Amazon Inspector inizierà immediatamente a scansionare le risorse idonee per quel tipo di scansione. Per una panoramica dei tipi di scansione disponibili, consultaPanoramica dei tipi di scansione di Amazon Inspector. Di seguito viene descritto cosa succede quando si attiva per la prima volta ogni tipo di scansione:

- Scansione Amazon EC2: quando attivi la scansione Amazon Inspector Amazon EC2 per un account, Amazon Inspector analizza tutte le istanze idonee nel tuo account alla ricerca di vulnerabilità dei pacchetti e problemi di raggiungibilità della rete. Il plug-in Amazon Inspector SSM è installato su tutti gli host gestiti da SSM. Windows Per ulteriori informazioni, consulta Scansione Windows delle istanze. Inoltre, Amazon Inspector crea le seguenti associazioni SSM nel tuo account:
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`
  - `InvokeInspectorSsmPlugin-do-not-delete`.
- Scansione Amazon ECR: quando attivi la scansione delle immagini dei contenitori Amazon ECR per un account, il tipo di scansione Amazon ECR per gli archivi privati in quell'account cambia da Scansione di base con Amazon ECR a scansione avanzata con Amazon Inspector. Quindi tutte le immagini di container Amazon ECR idonee inviate negli ultimi 30 giorni o recuperate negli ultimi 90 giorni vengono scansionate per individuare eventuali vulnerabilità dei pacchetti. Inoltre, la durata di una nuova scansione di Amazon ECR è impostata su 90 giorni per le date push e pull delle immagini.

- Scansione Lambda standard: quando attivi la scansione Lambda standard in un account, tutte le funzioni Lambda dell'account che sono state richiamate o aggiornate negli ultimi 90 giorni vengono analizzate alla ricerca di vulnerabilità dei pacchetti. Inoltre, nel tuo account viene CloudTrail creato un canale collegato al servizio.
- Scansione standard Lambda + scansione del codice Lambda: questi tipi di scansione della funzione Lambda vengono attivati insieme. Quando attivi la scansione del codice Lambda in un account, tutte le funzioni Lambda del tuo account che sono state richiamate o aggiornate negli ultimi 90 giorni vengono scansionate alla ricerca di vulnerabilità del codice.

Attivazione delle scansioni

Se sei l'amministratore delegato di Amazon Inspector in AWS un'organizzazione, puoi abilitare automaticamente diversi tipi di scansione di Amazon Inspector per più account in più regioni utilizzando uno script di shell sviluppato da Amazon Inspector inspector2- on. enablement-with-cli GitHub Altrimenti, per completare questa procedura per un ambiente con più account tramite la console, completa i seguenti passaggi dopo aver effettuato l'accesso come amministratore delegato di Amazon Inspector.

Console

Per attivare le scansioni

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri attivare un nuovo tipo di scansione.
3. Nel riquadro di navigazione, scegli Gestione account.
4. Nella pagina Gestione dell'account, seleziona gli account per i quali desideri attivare un tipo di scansione.
5. Scegli Attiva e seleziona il tipo di scansione che desideri attivare.
6. (Consigliato) Ripeti questi passaggi Regione AWS per ognuno dei quali desideri attivare quel tipo di scansione.

API

Esegui l'operazione Enable API. Nella richiesta, fornisci gli ID dell'account per cui stai attivando le scansioni, il token di idempotenza e uno o più di`EC2`, `ECR`, `LAMBDA`, o `LAMBDA_CODE` `resourceTypes` per attivare scansioni di quel tipo.

Scansione delle istanze Amazon EC2 con Amazon Inspector

La scansione senza agenti di Amazon Inspector per Amazon EC2 è disponibile in anteprima. L'utilizzo della funzionalità di scansione senza agenti di Amazon EC2 è soggetto alla Sezione 2 dei Termini di AWS servizio («Beta e anteprime»).

La scansione di Amazon Inspector EC2 estrae i metadati dall'istanza EC2, quindi confronta questi metadati con le regole raccolte dagli avvisi di sicurezza per produrre i risultati. Amazon Inspector analizza le istanze alla ricerca di vulnerabilità dei pacchetti e problemi di raggiungibilità della rete. Per informazioni sui tipi di risultati prodotti per questi problemi, consulta. Ricerca dei tipi in Amazon Inspector

Amazon Inspector esegue scansioni di raggiungibilità della rete una volta ogni 24 ore, mentre le scansioni di vulnerabilità dei pacchetti vengono eseguite con cadenza variabile a seconda del metodo di scansione associato all'istanza.

Metodi di scansione

Le scansioni delle vulnerabilità dei pacchetti possono essere eseguite utilizzando un metodo di scansione basato su agenti o senza agente. Questi metodi di scansione determinano come e quando Amazon Inspector raccoglie l'inventario software da un'istanza EC2 per le scansioni delle vulnerabilità dei pacchetti. Il metodo basato su agenti si basa sull'agente SSM per raccogliere l'inventario del software, mentre il metodo agentless utilizza le istantanee di Amazon EBS anziché un agente.

I metodi di scansione utilizzati da Amazon Inspector dipendono dall'impostazione della modalità di scansione del tuo account. Per ulteriori informazioni, consulta,. Gestione della modalità di scansione

Per attivare le scansioni di Amazon EC2, consulta. Attivazione di un tipo di scansione

Scansione basata su agenti

Le scansioni basate su agenti vengono eseguite continuamente utilizzando l'agente SSM su tutte le istanze idonee. Per le scansioni basate su agenti, Amazon Inspector utilizza le associazioni SSM e i plug-in installati tramite queste associazioni per raccogliere l'inventario software dalle tue istanze. Oltre alle scansioni delle vulnerabilità dei pacchetti dei sistemi operativi, la scansione basata su agenti di Amazon Inspector può anche rilevare le vulnerabilità dei pacchetti per i pacchetti del linguaggio di programmazione delle applicazioni nelle istanze basate su Linux tramite. Ispezione approfondita di Amazon Inspector per istanze Amazon EC2 Linux

Il seguente processo spiega come Amazon Inspector utilizza SSM per raccogliere l'inventario ed eseguire scansioni basate su agenti:

1. Amazon Inspector crea associazioni SSM nel tuo account per raccogliere l'inventario dalle tue istanze. Per alcuni tipi di istanze (Windows e Linux), queste associazioni installano plug-in su singole istanze per raccogliere l'inventario.
2. Utilizzando SSM, Amazon Inspector estrae l'inventario dei pacchetti da un'istanza.
3. Amazon Inspector valuta l'inventario estratto e genera risultati per eventuali vulnerabilità rilevate.

Istanze idonee

Amazon Inspector utilizzerà il metodo basato su agenti per scansionare un'istanza se soddisfa le seguenti condizioni:

- L'istanza ha un sistema operativo supportato. Per un elenco dei sistemi operativi supportati, consulta la colonna di supporto per la scansione basata su agenti di. the section called “Sistemi operativi supportati per la scansione di Amazon EC2”
- L'istanza non è esclusa dalle scansioni tramite i tag di esclusione di Amazon Inspector EC2.
- L'istanza è gestita tramite SSM. Per istruzioni sulla verifica e la configurazione dell'agente, consulta. Configurazione dell'agente SSM

Comportamenti di scansione basati su agenti

Quando si utilizza il metodo di scansione basato su agenti, Amazon Inspector avvia nuove scansioni di vulnerabilità delle istanze EC2 nelle seguenti situazioni:

- Quando avvii una nuova istanza EC2.

- Quando installi un nuovo software su un'istanza EC2 esistente (Linux e Mac).
- Quando Amazon Inspector aggiunge un nuovo elemento CVE (Common Vulnerabilities and Exposures) al suo database e tale CVE è rilevante per la tua istanza EC2 (Linux e Mac).

Amazon Inspector aggiorna il campo Ultima scansione per un'istanza EC2 quando viene completata una scansione iniziale. Successivamente, il campo Ultima scansione viene aggiornato quando Amazon Inspector valuta l'inventario SSM (per impostazione predefinita ogni 30 minuti) o quando un'istanza viene nuovamente scansionata perché al database Amazon Inspector è stato aggiunto un nuovo CVE che ha un impatto su quell'istanza.

Puoi verificare quando un'istanza EC2 è stata analizzata l'ultima volta per individuare eventuali vulnerabilità dalla scheda Istanze nella pagina di gestione dell'account o utilizzando il comando. ListCoverage

Configurazione dell'agente SSM

Affinché Amazon Inspector rilevi le vulnerabilità del software per un'istanza Amazon EC2 utilizzando il metodo di scansione basato su agenti, l'istanza deve essere un'istanza gestita in Amazon EC2 Systems Manager (SSM). Un'istanza gestita da SSM ha l'agente SSM installato e in esecuzione e SSM è autorizzato a gestire l'istanza. Se stai già utilizzando SSM per gestire le tue istanze, non sono necessari altri passaggi per le scansioni basate su agenti.

L'agente SSM è installato per impostazione predefinita sulle istanze EC2 create da alcune Amazon Machine Images (AMI). Per ulteriori informazioni, consulta Informazioni su SSM Agent nella Guida per l'utente.AWS Systems Manager Tuttavia, anche se è installato, potrebbe essere necessario attivare l'agente SSM manualmente e concedere l'autorizzazione SSM per gestire l'istanza.

La procedura seguente descrive come configurare un'istanza Amazon EC2 come istanza gestita utilizzando un profilo di istanza IAM. La procedura fornisce anche collegamenti a informazioni più dettagliate nella Guida per l'AWS Systems Manager utente.

AmazonSSMManagedInstanceCoreè la politica consigliata da utilizzare quando si collega un profilo di istanza. Questa policy dispone di tutte le autorizzazioni necessarie per la scansione di Amazon Inspector EC2.

> **Note**
>
> Puoi anche automatizzare la gestione SSM di tutte le tue istanze EC2, senza l'uso di profili di istanza IAM, utilizzando SSM Default Host Management Configuration. Per ulteriori informazioni, consulta la pagina Configurazione di gestione host predefinita.

Per configurare SSM per un'istanza Amazon EC2

1. Se non è già installato dal fornitore del sistema operativo, installa l'agente SSM. Per ulteriori informazioni, consulta Working with SSM Agent.
2. Utilizzare il AWS CLI per verificare che l'agente SSM sia in esecuzione. Per ulteriori informazioni, consulta Verifica dello stato dell'agente SSM e avvio dell'agente.
3. Concedi l'autorizzazione a SSM per gestire la tua istanza. Puoi concedere l'autorizzazione creando un profilo di istanza IAM e collegandolo alla tua istanza. Ti consigliamo di utilizzare la AmazonSSMManagedInstanceCorepolicy, poiché questa policy ha le autorizzazioni per SSM Distributor, SSM Inventory e SSM State manager, di cui Amazon Inspector ha bisogno per le scansioni. Per istruzioni sulla creazione di un profilo di istanza con queste autorizzazioni e sul collegamento di un'istanza, vedere Configurare le autorizzazioni dell'istanza per Systems Manager Systems Manager.
4. (Facoltativo) Attiva gli aggiornamenti automatici per l'agente SSM. Per ulteriori informazioni, consulta Automazione degli aggiornamenti all'agente SSM.
5. (Facoltativo) Configura Systems Manager per utilizzare un endpoint Amazon Virtual Private Cloud (Amazon VPC). Per ulteriori informazioni, consulta Creazione di endpoint Amazon VPC.

> **Important**
>
> Amazon Inspector richiede un'associazione Systems Manager State Manager nel tuo account per raccogliere l'inventario delle applicazioni software. Amazon Inspector crea automaticamente un'associazione chiamata `InspectorInventoryCollection-do-not-delete` se non ne esiste già una.
> Amazon Inspector richiede anche una sincronizzazione dei dati delle risorse e ne crea automaticamente una chiamata `InspectorResourceDataSync-do-not-delete` se non ne esiste già una. Per ulteriori informazioni, consulta Configurazione della sincronizzazione dei dati delle risorse per Inventory nella Guida per l'AWS Systems Manager utente. Ogni account può avere un determinato numero di sincronizzazioni dei dati delle risorse per

regione. Per ulteriori informazioni, consulta Numero massimo di sincronizzazioni dei dati delle risorse (Account AWS per regione) negli endpoint e nelle quote SSM. Se hai raggiunto questo numero massimo, dovrai eliminare la sincronizzazione dei dati di una risorsa, vedi Gestione della sincronizzazione dei dati delle risorse.

Risorse SSM create per la scansione

Amazon Inspector richiede una serie di risorse SSM nel tuo account per eseguire le scansioni di Amazon EC2. Le seguenti risorse vengono create quando attivi per la prima volta la scansione di Amazon Inspector EC2:

> **Note**
>
> Se una di queste risorse SSM viene eliminata mentre la scansione Amazon Inspector Amazon EC2 è attivata per il tuo account, Amazon Inspector tenterà di ricrearla all'intervallo di scansione successivo.

`InspectorInventoryCollection-do-not-delete`

Si tratta di un'associazione Systems Manager State Manager (SSM) che Amazon Inspector utilizza per raccogliere l'inventario delle applicazioni software dalle istanze Amazon EC2. Se il tuo account dispone già di un'associazione SSM per la raccolta dell'inventario`InstanceIds*`, Amazon Inspector la utilizzerà invece di crearne una propria.

`InspectorResourceDataSync-do-not-delete`

Si tratta di una sincronizzazione dei dati delle risorse che Amazon Inspector utilizza per inviare i dati di inventario raccolti dalle istanze Amazon EC2 a un bucket Amazon S3 di proprietà di Amazon Inspector. Per ulteriori informazioni, consulta Configurazione della sincronizzazione dei dati delle risorse per l'inventario nella Guida per l'utente.AWS Systems Manager

`InspectorDistributor-do-not-delete`

Si tratta di un'associazione SSM utilizzata da Amazon Inspector per la scansione delle istanze di Windows. Questa associazione installa il plug-in Amazon Inspector SSM sulle tue istanze Windows. Se il file del plug-in viene eliminato inavvertitamente, questa associazione lo reinstallerà all'intervallo di associazione successivo.

`InvokeInspectorSsmPlugin-do-not-delete`

Si tratta di un'associazione SSM utilizzata da Amazon Inspector per la scansione delle istanze di Windows. Questa associazione consente ad Amazon Inspector di avviare scansioni utilizzando il plug-in, inoltre puoi utilizzarlo per impostare intervalli personalizzati per le scansioni delle istanze di Windows. Per ulteriori informazioni, consulta [WindowsImpostazione di pianificazioni personalizzate, ad esempio scansioni].

`InspectorLinuxDistributor-do-not-delete`

Si tratta di un'associazione SSM utilizzata da Amazon Inspector per l'ispezione approfondita di Amazon EC2 Linux. Questa associazione installa il plug-in Amazon Inspector SSM sulle tue istanze Linux.

`InvokeInspectorLinuxSsmPlugin-do-not-delete`

Si tratta di un'associazione SSM utilizzata da Amazon Inspector per l'ispezione approfondita di Amazon EC2 Linux. Questa associazione consente ad Amazon Inspector di avviare scansioni utilizzando il plug-in.

> **Note**
>
> Quando disattivi la scansione o l'ispezione approfondita di Amazon Inspector Amazon EC2, tutte le risorse SSM verranno disinstallate automaticamente dagli host Linux corrispondenti.

Scansione senza agenti

Amazon Inspector utilizza un metodo di scansione senza agente su istanze idonee quando l'account è in modalità di scansione ibrida (che include scansioni basate su agenti e senza agente). Per le scansioni senza agenti, Amazon Inspector utilizza le istantanee EBS per raccogliere un inventario software dalle tue istanze. Le istanze scansionate utilizzando il metodo agentless vengono analizzate alla ricerca di vulnerabilità sia del pacchetto del sistema operativo che del pacchetto del linguaggio di programmazione dell'applicazione.

> **Note**
>
> Durante la scansione delle istanze Linux alla ricerca delle vulnerabilità dei pacchetti del linguaggio di programmazione delle applicazioni, il metodo agentless analizza tutti i percorsi disponibili, mentre la scansione basata su agenti analizza solo i percorsi predefiniti e i

percorsi aggiuntivi specificati come parte di. Ispezione approfondita di Amazon Inspector per istanze Amazon EC2 Linux Ciò può comportare che la stessa istanza abbia risultati diversi a seconda che venga scansionata utilizzando il metodo basato su agenti o il metodo senza agenti.

Il seguente processo spiega come Amazon Inspector utilizza gli snapshot EBS per raccogliere l'inventario ed eseguire scansioni senza agenti:

1. Amazon Inspector crea uno snapshot EBS di tutti i volumi collegati all'istanza. Mentre Amazon Inspector lo utilizza, lo snapshot viene archiviato nel tuo account e contrassegnato `InspectorScan` come chiave di tag e un ID di scansione univoco come valore del tag.
2. Amazon Inspector recupera i dati dagli snapshot utilizzando le API dirette di EBS e li valuta per individuare eventuali vulnerabilità. I risultati vengono generati per tutte le vulnerabilità rilevate.
3. Amazon Inspector elimina gli snapshot EBS creati nel tuo account.

Istanze idonee

Amazon Inspector utilizzerà il metodo agentless per scansionare un'istanza se soddisfa le seguenti condizioni:

- L'istanza ha un sistema operativo supportato. Per un elenco dei sistemi operativi supportati, consulta la colonna di supporto per la scansione basata su agenti di. the section called “Sistemi operativi supportati per la scansione di Amazon EC2”
- L'istanza non è esclusa dalle scansioni tramite i tag di esclusione di Amazon Inspector EC2.
- L'istanza ha lo stato di`Unmanaged EC2 instance`, o. `Stale inventory` `No inventory`
- L'istanza è supportata da EBS e ha uno dei seguenti formati di file system:
  - `ext3`
  - `ext4`
  - `xfs`

Comportamenti di scansione senza agenti

Quando il tuo account è configurato per la scansione ibrida, Amazon Inspector esegue scansioni senza agente su istanze idonee ogni 24 ore. Amazon Inspector rileva e analizza le nuove istanze

idonee ogni ora, incluse nuove istanze senza agenti SSM o istanze preesistenti con stato modificato in. `SSM_UNMANAGED`

Amazon Inspector aggiorna il campo Ultima scansione per un'istanza Amazon EC2 ogni volta che esegue la scansione degli snapshot estratti da un'istanza dopo una scansione senza agente.

Puoi verificare quando un'istanza EC2 è stata analizzata l'ultima volta per individuare eventuali vulnerabilità dalla scheda Istanze nella pagina di gestione dell'account o utilizzando il comando. ListCoverage

Gestione della modalità di scansione

La modalità di scansione EC2 determina i metodi di scansione che Amazon Inspector utilizzerà per eseguire le scansioni EC2 nel tuo account. Puoi visualizzare la modalità di scansione del tuo account dalla pagina delle impostazioni di scansione EC2 in Impostazioni generali. Gli account autonomi o gli amministratori delegati di Amazon Inspector possono modificare la modalità di scansione. Quando imposti la modalità di scansione come amministratore delegato di Amazon Inspector, tale modalità di scansione viene impostata per tutti gli account membri della tua organizzazione. Amazon Inspector offre le seguenti modalità di scansione:

Scansione basata su agenti: in questa modalità di scansione, Amazon Inspector utilizzerà esclusivamente il metodo di scansione basato su agenti per la scansione delle vulnerabilità dei pacchetti. Questa modalità di scansione analizza solo le istanze gestite da SSM nel tuo account, ma ha il vantaggio di fornire scansioni continue in risposta a nuovi CVE o modifiche alle istanze. La scansione basata su agenti fornisce anche un'ispezione approfondita di Amazon Inspector per le istanze idonee. Questa è la modalità di scansione predefinita per gli account appena attivati.

Scansione ibrida: in questa modalità di scansione, Amazon Inspector utilizza una combinazione di metodi basati su agenti e senza agenti per individuare le vulnerabilità dei pacchetti. Per le istanze EC2 idonee su cui è installato e configurato l'agente SSM, Amazon Inspector utilizza il metodo basato su agenti. Per le istanze idonee che non sono gestite tramite SSM, Amazon Inspector utilizzerà il metodo agentless per le istanze idonee supportate da EBS.

Per modificare la modalità di scansione

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri modificare la modalità di scansione EC2.

3. Dal pannello di navigazione laterale, in Impostazioni generali, seleziona Impostazioni di scansione EC2.
4. In Modalità di scansione, seleziona Modifica.
5. Scegli una modalità di scansione, quindi seleziona Salva modifiche.

Esclusione delle istanze dalle scansioni di Amazon Inspector

Puoi etichettare determinate istanze per escluderle dalle scansioni di Amazon Inspector. L'esclusione delle istanze dalle scansioni può aiutare a prevenire avvisi non utilizzabili. Non ti viene addebitato alcun costo per le istanze escluse.

Per escludere un'istanza EC2 dalle scansioni, contrassegna quell'istanza con la seguente chiave:

- `InspectorEc2Exclusion`

Il valore è facoltativo.

Per ulteriori informazioni sull'aggiunta di tag, consulta Etichettare le risorse Amazon EC2.

Inoltre, puoi escludere un volume EBS crittografato dalle scansioni senza agenti etichettando la AWS KMS chiave utilizzata per crittografare quel volume con il tag. `InspectorEc2Exclusion` Per ulteriori informazioni, consulta Etichettatura delle chiavi

Sistemi operativi supportati

Amazon Inspector analizza le istanze EC2 Mac, Windows e Linux supportate alla ricerca di vulnerabilità nei pacchetti del sistema operativo. Per le istanze Linux, Amazon Inspector può produrre risultati per i pacchetti di linguaggi di programmazione delle applicazioni che utilizzano. Ispezione approfondita di Amazon Inspector per istanze Amazon EC2 Linux Per le istanze Mac e Windows vengono scansionati solo i pacchetti del sistema operativo.

Per informazioni sui sistemi operativi supportati, incluso il sistema operativo che può essere scansionato senza un agente SSM, consulta. Sistemi operativi supportati per la scansione di Amazon EC2

Ispezione approfondita di Amazon Inspector per istanze Amazon EC2 Linux

Amazon Inspector amplia la copertura di scansione di Amazon EC2 per includere l'ispezione approfondita. Con un'ispezione approfondita, Amazon Inspector rileva le vulnerabilità dei pacchetti

per i pacchetti di linguaggi di programmazione delle applicazioni nelle istanze Amazon EC2 basate su Linux.

Amazon Inspector analizza i percorsi predefiniti per individuare le librerie di pacchetti dei linguaggi di programmazione. Puoi anche configurare percorsi personalizzati oltre ai percorsi predefiniti. Per ulteriori informazioni, consulta Percorsi personalizzati per l'ispezione approfondita di Amazon Inspector.

Amazon Inspector esegue scansioni di ispezione approfondita utilizzando i dati raccolti con il plug-in Amazon Inspector SSM. Per gestire il plug-in ed eseguire un'ispezione approfondita per Linux, Amazon Inspector crea automaticamente la seguente associazione SSM `InvokeInspectorLinuxSsmPlugin-do-not-delete` nel tuo account. Ciò si verifica quando Amazon Inspector attiva l'ispezione approfondita.

Amazon Inspector raccoglie l'inventario aggiornato delle applicazioni dalle istanze per un'ispezione approfondita ogni 6 ore.

Per un elenco dei linguaggi di programmazione supportati da Amazon Inspector per l'ispezione approfondita, consulta,. Linguaggi di programmazione supportati: Amazon EC2 deep inspection

> **Note**
>
> L'ispezione approfondita non è supportata per le istanze Windows o Mac.

Attivazione o disattivazione dell'ispezione approfondita

> **Note**
>
> L'ispezione approfondita viene attivata automaticamente come parte della scansione di Amazon EC2 per gli account che attivano Amazon Inspector dopo il 17 aprile 2023.

Puoi verificare se l'ispezione approfondita è attiva per un account nella console Amazon Inspector dalla colonna di scansione di Amazon EC2 nella pagina di gestione dell'account. Se l'ispezione approfondita non è attiva, questa colonna riporterà la dicitura Attivata (ispezione approfondita disattivata). Per verificare lo stato di attivazione a livello di codice, utilizza l'API. GetEc2DeepInspectionConfiguration Oppure, per più account, usa l'BatchGetMemberEc2DeepInspectionStatusAPI.

Se hai attivato Amazon Inspector prima del 17 aprile 2023, puoi attivare l'ispezione approfondita tramite il banner della console o l'UpdateEc2DeepInspectionConfigurationAPI. Se sei l'amministratore delegato di un'organizzazione in Amazon Inspector, puoi utilizzare BatchUpdateMemberEc2DeepInspectionStatusl'API per attivarla per te e per i tuoi account membro.

Puoi disattivare l'ispezione approfondita tramite l'API. UpdateEc2DeepInspectionConfiguration Gli account dei membri di un'organizzazione non possono disattivare l'ispezione approfondita. Invece, l'account membro deve essere disattivato dall'amministratore delegato utilizzando l'API. BatchUpdateMemberEc2DeepInspectionStatus

Informazioni sul plug-in Amazon Inspector SSM per Linux

Amazon Inspector utilizza il plug-in Amazon Inspector SSM per eseguire un'ispezione approfondita delle istanze Linux. Il plug-in Amazon Inspector SSM viene installato automaticamente sulle tue istanze Linux nella seguente directory:. `/opt/aws/inspector/bin` Il nome dell'eseguibile è. `inspectorssmplugin`

> **Note**
>
> Amazon Inspector utilizza Systems Manager Distributor per distribuire il plug-in nella tua istanza Amazon EC2. Systems Manager Distributor supporta i sistemi operativi elencati come Piattaforme e architetture di pacchetti supportate nella guida Systems Manager. Il sistema operativo dell'istanza Amazon EC2 deve essere supportato da Systems Manager Distributor e Amazon Inspector for Amazon Inspector per Amazon Inspector per eseguire scansioni di ispezione approfondite.

Amazon Inspector crea le seguenti directory di file per gestire i dati raccolti per l'ispezione approfondita dal plug-in Amazon Inspector SSM:

- `/opt/aws/inspector/var/input`
- `/opt/aws/inspector/var/output`
  - `packages.txt`In questa directory vengono memorizzati i percorsi completi dei pacchetti scoperti da Deep Inspection. Se Amazon Inspector ha rilevato lo stesso pacchetto più volte sulla tua istanza, questo file elenca ogni posizione in cui è stato trovato il pacchetto.

Amazon Inspector archivia i log del plug-in nella directory. `/var/log/amazon/inspector`

Disinstallazione del plug-in Amazon Inspector SSM

Se il `inspectorssmplugin` file viene eliminato inavvertitamente, l'associazione `InspectorLinuxDistributor-do-not-delete` SSM proverà a reinstallare il plug-in all'intervallo di scansione successivo.

Se disattivi la scansione di Amazon EC2, il plug-in verrà disinstallato automaticamente da tutti gli host Linux.

Percorsi personalizzati per l'ispezione approfondita di Amazon Inspector

Puoi configurare percorsi personalizzati per la ricerca di Amazon Inspector quando esegue un'ispezione approfondita delle tue istanze Linux Amazon EC2. Quando aggiungi un percorso personalizzato, Amazon Inspector cerca i pacchetti in quella directory e in tutte le sottodirectory al suo interno.

Tutti gli account possono definire fino a 5 percorsi personalizzati per il proprio account individuale. Se sei l'amministratore delegato della tua organizzazione, puoi definire 5 percorsi aggiuntivi da applicare all'intera organizzazione. Ciò equivale a un totale di un massimo di 10 percorsi personalizzati scansionati per account dell'organizzazione.

Amazon Inspector analizza tutti i percorsi personalizzati oltre ai seguenti percorsi predefiniti che vengono analizzati per tutti gli account:

- `/usr/lib`
- `/usr/lib64`
- `/usr/local/lib`
- `/usr/local/lib64`

> **Note**
>
> I percorsi personalizzati devono essere percorsi locali. Amazon Inspector non esegue la scansione di percorsi di rete mappati come supporti Network File System (NFS) o supporti di file system Amazon S3.

Formattazione per percorsi personalizzati

Di seguito è riportato un esempio del formato per un percorso personalizzato: `/home/usr1/project01`

I percorsi personalizzati non possono superare i 256 caratteri.

È previsto un limite di 5.000 pacchi per istanza e un limite massimo di 15 minuti per la raccolta dell'inventario dei pacchi. Ti consigliamo di provare a scegliere percorsi personalizzati per aiutarti a evitare questi limiti.

Imposta un percorso personalizzato nella console

Console

Accedi come amministratore delegato di Amazon Inspector e segui i passaggi seguenti per aggiungere percorsi personalizzati per la tua organizzazione.

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, selezionate la regione in cui desiderate attivare la scansione standard Lambda.
3. Dal pannello di navigazione laterale, in Impostazioni generali, seleziona Impostazioni di scansione EC2.
4. In Percorsi personalizzati per il tuo account, seleziona Modifica per aggiungere percorsi per il tuo account individuale. Se sei l'amministratore delegato, puoi scegliere Modifica nel riquadro Percorsi personalizzati per la tua organizzazione per aggiungere percorsi personalizzati per tutti gli account all'interno dell'organizzazione.
5. Inserisci i percorsi personalizzati nelle caselle di testo.
6. Scegli Salva per salvare i percorsi personalizzati. Amazon Inspector includerà questi percorsi nella sua prossima ispezione approfondita.

API

Esegui il comando UpdateEc2DeepInspectionConfiguration. Per `packagePaths` specificare una serie di percorsi da scansionare.

Linguaggi di programmazione compatibili

Per le istanze Linux, l'ispezione approfondita di Amazon Inspector può produrre risultati per i pacchetti di linguaggi di programmazione delle applicazioni oltre alle vulnerabilità nei pacchetti del sistema operativo. Per le istanze Mac e Windows vengono analizzati solo i pacchetti del sistema operativo.

Per informazioni sui linguaggi di programmazione supportati, vedere. Linguaggi di programmazione supportati per l'ispezione approfondita di Amazon Inspector

Scansione Windows delle istanze EC2 con Amazon Inspector

> **Note**
>
> Il 31 agosto 2022, Amazon Inspector ha ampliato la copertura di scansione di Amazon EC2 per includere le istanze EC2 in esecuzione. Windows

Amazon Inspector rileva automaticamente tutte le Windows istanze supportate e le include nella scansione continua senza azioni aggiuntive. Per informazioni sulle istanze supportate, consulta. Sistemi operativi supportati per la scansione di Amazon EC2

A differenza delle scansioni per le istanze basate su Linux, Amazon Inspector Windows esegue le scansioni a intervalli regolari. Windowsle istanze vengono inizialmente scansionate al momento del rilevamento e poi scansionate ogni 6 ore. Tuttavia, l'intervallo di scansione predefinito di 6 ore è regolabile. Per ulteriori informazioni, consulta WindowsImpostazione di pianificazioni personalizzate, ad esempio scansioni. Di seguito è riportata una panoramica di come Amazon Inspector esegue la scansione Windows delle istanze:

1. Quando la scansione di Amazon EC2 è attivata, Amazon Inspector crea nuove associazioni SSM per le Windows tue risorse`InspectorDistributor-do-not-delete`:, e. `InspectorInventoryCollection-do-not-delete` `InvokeInspectorSsmPlugin-do-not-delete`
2. L'associazione `InspectorDistributor-do-not-delete` SSM utilizza il documento `AWS-ConfigureAWSPackage` SSM e il pacchetto `AmazonInspector2-InspectorSsmPlugin` SSM Distributor per installare il plug-in Amazon Inspector SSM sulle tue istanze. Windows Per ulteriori informazioni, consulta Informazioni sul plug-in Amazon Inspector SSM per Windows.

3. L'associazione `InvokeInspectorSsmPlugin-do-not-delete` SSM esegue il plug-in Amazon Inspector SSM a intervalli regolari per raccogliere dati sulle istanze e generare risultati di Amazon Inspector. Per impostazione predefinita, l'intervallo è ogni 6 ore. Tuttavia, è possibile personalizzarlo impostando un'espressione cron o un'espressione di frequenza per l'associazione utilizzando SSM. Per ulteriori informazioni, vedere Reference: Cron and rate expressions for Systems Manager nella Guida per l'AWS Systems Manager utente.

> **Note**
>
> Amazon Inspector inserisce i file di definizione Open Vulnerability and Assessment Language (OVAL) aggiornati nel bucket S3. `inspector2-oval-prod-REGION` Questo bucket S3 contiene le definizioni OVAL utilizzate nelle scansioni e non deve essere modificato. La modifica di questa impostazione impedirà ad Amazon Inspector di cercare nuovi CVE non appena vengono rilasciati.

Requisiti di scansione di Amazon Inspector per le istanze Windows

Per eseguire la scansione di un'Windowsistanza, Amazon Inspector richiede che l'istanza soddisfi i seguenti criteri:

- L'istanza è un'istanza gestita da SSM. Per istruzioni sulla configurazione dell'istanza per la scansione, consultaConfigurazione dell'agente SSM.
- Il sistema operativo dell'istanza è uno dei sistemi Windows operativi supportati. Per un elenco completo dei sistemi operativi supportati, vedereSistemi operativi supportati per la scansione di Amazon EC2.
- Nell'istanza è installato il plug-in Amazon Inspector SSM. Amazon Inspector installa automaticamente il plug-in Amazon Inspector SSM per le istanze gestite al momento del rilevamento. Per informazioni dettagliate sul plug-in, consulta l'argomento successivo.

> **Note**
>
> Se l'host è in esecuzione su un Amazon VPC senza accesso a Internet in uscita, Windows la scansione richiede che l'host sia in grado di accedere agli endpoint Amazon S3 regionali. Per informazioni su come configurare un endpoint Amazon VPC Amazon S3, consulta Creare un endpoint gateway nella Amazon Virtual Private Cloud User Guide. Se la tua policy sugli

endpoint di Amazon VPC limita l'accesso ai bucket S3 esterni, devi specificamente consentire l'accesso al bucket gestito da Amazon Inspector nel Regione AWS tuo che memorizza le definizioni OVAL utilizzate per valutare l'istanza. Questo bucket ha il seguente formato:. `inspector2-oval-prod-REGION`

Informazioni sul plug-in Amazon Inspector SSM per Windows

Il plug-in Amazon Inspector SSM è necessario per consentire ad Amazon Inspector di scansionare le istanze. Windows Il plug-in Amazon Inspector SSM viene installato automaticamente sulle Windows istanze in `C:\Program Files\Amazon\Inspector` e il file binario eseguibile viene denominato. `InspectorSsmPlugin.exe`

I seguenti percorsi di file vengono creati per archiviare i dati raccolti dal plug-in Amazon Inspector SSM:

- `C:\ProgramData\Amazon\Inspector\Input`
- `C:\ProgramData\Amazon\Inspector\Output`
- `C:\ProgramData\Amazon\Inspector\Logs`

> **Note**
>
> Per impostazione predefinita, il plug-in Amazon Inspector SSM viene eseguito con una priorità inferiore a quella normale.

Disinstallazione del plug-in Amazon Inspector SSM

Se il `InspectorSsmPlugin.exe` file viene eliminato inavvertitamente, l'associazione `InspectorDistributor-do-not-delete` SSM reinstallerà il plug-in al successivo intervallo di scansione. Windows Se desideri disinstallare il plug-in Amazon Inspector SSM, puoi utilizzare l'azione di disinstallazione sul documento. `AmazonInspector2-ConfigureInspectorSsmPlugin`

Inoltre, il plug-in Amazon Inspector SSM verrà disinstallato automaticamente da tutti gli Windows host se disattivi la scansione di Amazon EC2.

> **Note**
>
> Se disinstalli l'agente SSM prima di disattivare Amazon Inspector, il plug-in Amazon Inspector SSM rimarrà sull'Windowshost ma non invierà più dati al plug-in Amazon Inspector SSM. Per ulteriori informazioni, consulta Disattivazione di Amazon Inspector.

WindowsImpostazione di pianificazioni personalizzate, ad esempio scansioni

Puoi personalizzare l'intervallo tra le scansioni delle tue istanze Windows Amazon EC2 impostando un'espressione cron o un'espressione rate per l'`InvokeInspectorSsmPlugin-do-not-delete`associazione tramite SSM. Per ulteriori informazioni, consultate Reference: Cron and rate expressions for Systems Manager nella Guida per l'AWS Systems Manager utente o utilizzate le seguenti istruzioni.

Seleziona uno dei seguenti esempi di codice per modificare la cadenza di scansione Windows delle istanze da 6 ore predefinita a 12 ore utilizzando un'espressione rate o un'espressione cron.

Gli esempi seguenti richiedono l'utilizzo di AssociationIdfor l'associazione denominata. `InvokeInspectorSsmPlugin-do-not-delete` È possibile recuperare il file AssociationIdeseguendo il seguente AWS CLI comando:

```
$ aws ssm list-associations --association-filter-list
 "key=AssociationName,value=InvokeInspectorSsmPlugin-do-not-delete" --region us-east-1
```

> **Note**
>
> AssociationIdÈ regionale, quindi devi prima recuperare un ID univoco per ciascuno. Regione AWSÈ quindi possibile eseguire il comando per modificare la cadenza di scansione in ciascuna regione in cui si desidera impostare una pianificazione di scansione personalizzata per Windows le istanze.

Example rate expression

```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "rate(12 hours)"
```

Example cron expression

```
$ aws ssm update-association \
--association-id "YourAssociationId" \
--association-name "InvokeInspectorSsmPlugin-do-not-delete" \
--schedule-expression "cron(0 0/12 * * ? *)"
```

Scansione delle immagini dei container Amazon ECR con Amazon Inspector

Amazon Inspector analizza le immagini dei container archiviate in Amazon ECR alla ricerca di vulnerabilità del software per generare risultati di Package Vulnerability. Per informazioni sui tipi di risultati prodotti per questi problemi, consulta. Ricerca dei tipi in Amazon Inspector

Quando attivi le scansioni Amazon Inspector per Amazon ECR, imposti Amazon Inspector come servizio di scansione preferito per il tuo registro privato. Ciò sostituisce la scansione di base predefinita, fornita gratuitamente da Amazon ECR, con la scansione avanzata, fornita e fatturata tramite Amazon Inspector.

La scansione avanzata fornita da Amazon Inspector offre il vantaggio della scansione delle vulnerabilità sia per il sistema operativo che per i pacchetti di linguaggi di programmazione a livello di registro. Puoi esaminare i risultati scoperti utilizzando la scansione avanzata a livello di immagine, per ogni livello dell'immagine, sulla console Amazon ECR. Inoltre, puoi esaminare e utilizzare questi risultati in altri servizi non disponibili per le scansioni di base, AWS Security Hub tra cui Amazon EventBridge. Puoi visualizzare i risultati rilevati dalle scansioni sulla console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home. Per informazioni su come utilizzare i risultati, consulta. Gestione dei risultati in Amazon Inspector

Per istruzioni sull'attivazione delle scansioni Amazon ECR, consulta. Attivazione di un tipo di scansione

Comportamenti di scansione per la scansione Amazon ECR

Quando attivi per la prima volta la scansione ECR e il tuo repository è configurato per la scansione continua, Amazon Inspector rileva tutte le immagini idonee che hai inviato entro 30 giorni o recuperato negli ultimi 90 giorni. Quindi Amazon Inspector esegue la scansione delle immagini rilevate e ne imposta lo stato di scansione su. `active` Amazon Inspector continua a monitorare le

immagini purché siano state inviate o recuperate negli ultimi 90 giorni (per impostazione predefinita) o entro la durata della nuova scansione ECR configurata. Per ulteriori informazioni, consulta Configurazione della durata della nuova scansione ECR.

Per la scansione continua, Amazon Inspector avvia nuove scansioni di vulnerabilità delle immagini dei container nelle seguenti situazioni:

- Ogni volta che viene inserita una nuova immagine del contenitore.
- Ogni volta che Amazon Inspector aggiunge un nuovo elemento CVE (Common Vulnerabilities and Exposures) al suo database e tale CVE è rilevante per l'immagine del contenitore (solo scansione continua).

Se configuri il tuo repository per la scansione on push, le immagini vengono scansionate solo quando vengono inviate.

Puoi verificare l'ultima volta in cui è stata verificata la presenza di vulnerabilità in un'immagine del contenitore dalla scheda Immagini del contenitore nella pagina di gestione dell'account o utilizzando l'API. ListCoverage Amazon Inspector aggiorna il campo Last scanned at di un'immagine Amazon ECR in risposta ai seguenti eventi:

- Quando Amazon Inspector completa una scansione iniziale dell'immagine di un contenitore.
- Quando Amazon Inspector esegue nuovamente la scansione di un'immagine del contenitore, è stato aggiunto al database Amazon Inspector un nuovo elemento CVE (Common Vulnerabilities and Exposures) che influisce sull'immagine del contenitore.

Sistemi operativi e tipi di supporti supportati

Per informazioni sui sistemi operativi supportati, vedereSistemi operativi supportati per la scansione Amazon ECR.

Le scansioni di Amazon Inspector dei repository Amazon ECR coprono i seguenti tipi di supporti supportati:

- `"application/vnd.docker.distribution.manifest.v1+json"`
- `"application/vnd.docker.distribution.manifest.v1+prettyjws"`
- `"application/vnd.oci.image.manifest.v1+json"`
- `"application/vnd.docker.distribution.manifest.v2+json"`

> **Note**
>
> Le immagini e le immagini Scratch non sono `DockerV2ListMediaType` supportate.

Configurazione della scansione avanzata per i repository Amazon ECR

Quando attivi le scansioni di Amazon Inspector per le immagini dei contenitori Amazon ECR, modifichi l'impostazione di configurazione della scansione per il tuo registro privato. Il tipo di scansione per il registro viene modificato dalla scansione di base alla scansione avanzata fornita da Amazon Inspector. Per ulteriori informazioni, consulta la sezione Scansione delle immagini nella guida per l'utente di Amazon ECR.

Puoi gestire le impostazioni per una scansione avanzata a livello di repository in ECR. È possibile scegliere la scansione continua o la scansione immediata per i propri archivi. La scansione continua include scansioni istantanee e scansioni automatiche. La scansione on-push esegue la scansione solo quando inizialmente si invia un'immagine. Per entrambe le opzioni, è possibile affinare l'ambito di scansione tramite filtri di inclusione. Per impostazione predefinita, quando si attiva per la prima volta la scansione avanzata, le impostazioni sono impostate su Scansione continua di tutti gli archivi.

Per configurare le impostazioni di scansione avanzate

1. Apri la console Amazon ECR all'indirizzo https://console.aws.amazon.com/ecr/.
2. Nel Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione contenente i repository da scansionare.
3. Nel pannello di navigazione, scegli Registro privato, quindi scegli Scansione.
4. In Tipo di scansione, assicurati che sia selezionata l'opzione Scansione avanzata. In caso contrario, seleziona Scansione avanzata.

   Per impostazione predefinita, è selezionata l'opzione Scansione continua di tutti i repository che attiva la copertura di scansione completa di Amazon Inspector per tutti i repository.
5. Deseleziona Scansiona continuamente tutti i repository per filtrare quali repository vengono scansionati in modo continuo o istantaneo.

Per ulteriori informazioni sulla configurazione delle scansioni avanzate, consulta Using enhanced scanning nella guida per l'utente di Amazon ECR.

Configurazione della durata della nuova scansione ECR

L'impostazione della durata della nuova scansione ECR determina per quanto tempo Amazon Inspector monitora continuamente le immagini dei container nei repository. Puoi configurare la durata della nuova scansione per la data di invio e la data di recupero dell'immagine. La durata di scansione predefinita per i nuovi account, inclusi i nuovi account aggiunti a un'organizzazione, è di 90 giorni.

Durata della data di invio dell'immagine

La durata della data di invio delle immagini determina per quanto tempo Amazon Inspector monitora continuamente le immagini dopo che sono state trasferite nei repository dopo l'ultima data di aggiornamento. Le seguenti opzioni sono disponibili come durate di nuova scansione:

- 14 giorni
- 30 giorni
- 60 giorni
- 90 giorni (impostazione predefinita)
- 180 giorni
- Durata

Durata della data di recupero dell'immagine

La durata della data di recupero dell'immagine determina per quanto tempo Amazon Inspector monitora continuamente le immagini dopo l'ultima data di recupero. Le seguenti opzioni sono disponibili come durate di nuova scansione:

- 14 giorni
- 30 giorni
- 60 giorni
- 90 giorni (impostazione predefinita)
- 180 giorni

Amazon Inspector continuerà a monitorare e scansionare nuovamente un'immagine purché sia stata inserita o recuperata entro le date push e pull configurate. Se l'immagine non è stata inserita o recuperata entro le date push e pull configurate, Amazon Inspector interrompe il monitoraggio.

> **Note**
>
> Quando Amazon Inspector interrompe il monitoraggio di un'immagine, imposta il codice di stato della scansione dell'immagine `inactive` e il codice motivo su. `expired` Quindi pianifica la chiusura di tutti i risultati associati alle immagini.

Imposta la durata della nuova scansione in base al tuo ambiente. Ad esempio, se crei immagini spesso, scegli una durata di scansione più breve. Allo stesso modo, se utilizzate le immagini per lunghi periodi di tempo, scegliete una durata di scansione più lunga.

Quando configuri la durata della nuova scansione da un account amministratore delegato, Amazon Inspector applica l'impostazione a tutti gli account membri dell'organizzazione.

Per configurare la durata della nuova scansione ECR

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Dal pannello di navigazione, scegli Impostazioni generali, quindi scegli Impostazioni di scansione ECR.
3. Nelle impostazioni di scansione ECR, in Durata della nuova scansione ECR, scegli la durata della data di invio dell'immagine e la durata della data di estrazione dell'immagine che desideri impostare.
4. Selezionare Salva. Le nuove impostazioni vengono applicate immediatamente.

> **Note**
>
> Se aumenti la durata della data push, Amazon Inspector applica la modifica a tutte le immagini scansionate attivamente nei repository configurati per la scansione continua. Tuttavia, le immagini inattive rimangono inattive, anche se le hai inserite entro la nuova durata.

AWS Lambda Funzioni di scansione con Amazon Inspector

Il supporto di Amazon Inspector per AWS Lambda le funzioni fornisce valutazioni continue e automatizzate delle vulnerabilità di sicurezza per le funzioni e i livelli Lambda. Amazon Inspector offre due tipi di scansione per Lambda. Questi tipi di scansione cercano diversi tipi di vulnerabilità.

Scansione standard Amazon Inspector Lambda

Questo è il tipo di scansione Lambda predefinito. La scansione standard Lambda analizza le dipendenze delle applicazioni all'interno di una funzione Lambda e dei relativi livelli alla ricerca di vulnerabilità dei pacchetti. Per ulteriori informazioni, consulta Scansione standard Lambda.

Scansione del codice Amazon Inspector Lambda

Questo tipo di scansione analizza il codice dell'applicazione personalizzato nelle funzioni e nei livelli alla ricerca di vulnerabilità del codice. Puoi attivare la scansione standard Lambda da sola o insieme alla scansione del codice Lambda. Per ulteriori informazioni, consulta Scansione del codice Amazon Inspector Lambda.

Quando attivi la scansione Lambda, Amazon Inspector crea i AWS CloudTrail seguenti canali collegati ai servizi nel tuo account:

- `cloudtrail:CreateServiceLinkedChannel`
- `cloudtrail:DeleteServiceLinkedChannel`

Amazon Inspector gestisce questi canali e li utilizza per monitorare i tuoi CloudTrail eventi per le scansioni. Per ulteriori informazioni sui canali collegati ai servizi, consulta Visualizzazione dei canali collegati ai servizi CloudTrail utilizzando la CLI. AWS

> **Note**
>
> I canali collegati ai servizi creati da Amazon Inspector ti consentono di CloudTrail visualizzare gli eventi nel tuo account come se avessi CloudTrail una traccia, tuttavia ti consigliamo di crearne di CloudTrail personalizzati per gestire gli eventi del tuo account.

Per istruzioni sull'attivazione delle scansioni della funzione Lambda, vedere. Attivazione di un tipo di scansione

Comportamenti di scansione per la scansione della funzione Lambda

Al momento dell'attivazione, Amazon Inspector analizza tutte le funzioni Lambda richiamate o aggiornate negli ultimi 90 giorni nel tuo account. Amazon Inspector avvia scansioni di vulnerabilità delle funzioni Lambda nelle seguenti situazioni:

- Non appena Amazon Inspector rileva una funzione Lambda esistente.
- Quando si distribuisce una nuova funzione Lambda nel servizio Lambda.
- Quando si implementa un aggiornamento al codice dell'applicazione o alle dipendenze di una funzione Lambda esistente o dei relativi livelli.
- Ogni volta che Amazon Inspector aggiunge un nuovo elemento di vulnerabilità ed esposizioni comuni (common vulnerabilities and exposures, CVE) al suo database e tale CVE è pertinente alla funzione.

Amazon Inspector monitora ogni funzione Lambda per tutta la sua durata fino a quando non viene eliminata o esclusa dalla scansione.

Puoi verificare quando una funzione Lambda è stata verificata l'ultima volta per verificare la presenza di vulnerabilità dalla scheda Funzioni Lambda nella pagina Gestione dell'account o utilizzando l'API. ListCoverage Amazon Inspector aggiorna il campo Last scanned at per una funzione Lambda in risposta ai seguenti eventi:

- Quando Amazon Inspector completa una scansione iniziale di una funzione Lambda.
- Quando viene aggiornata una funzione Lambda.
- Quando Amazon Inspector esegue nuovamente la scansione di una funzione Lambda perché un nuovo elemento CVE che influisce su tale funzione è stato aggiunto al database Amazon Inspector.

Runtime e funzioni idonee supportati

Amazon Inspector supporta diversi runtime per la scansione standard Lambda e la scansione del codice Lambda. Per un elenco dei runtime supportati per ogni tipo di scansione, consulta e. Runtime supportati: scansione standard di Amazon Inspector Lambda Runtime supportati: scansione del codice Amazon Inspector Lambda

Oltre a disporre di un runtime supportato, una funzione Lambda deve soddisfare i seguenti criteri per essere idonea alle scansioni di Amazon Inspector:

- La funzione è stata richiamata o aggiornata negli ultimi 90 giorni.
- La funzione è contrassegnata `$LATEST`.
- La funzione non è esclusa dalle scansioni per tag.

> **Note**
>
> Le funzioni Lambda che non sono state richiamate o modificate negli ultimi 90 giorni vengono automaticamente escluse dalle scansioni. Amazon Inspector riprenderà la scansione di una funzione esclusa automaticamente se viene richiamata nuovamente o se vengono apportate modifiche al codice della funzione Lambda.

Scansione standard Amazon Inspector Lambda

La scansione standard di Amazon Inspector Lambda identifica le vulnerabilità del software nelle dipendenze dei pacchetti applicativi che aggiungi al codice e ai livelli della funzione Lambda. Ad esempio, se la funzione Lambda utilizza una versione del `python-jwt` pacchetto con una vulnerabilità nota, la scansione standard Lambda genererà un risultato per quella funzione.

Se Amazon Inspector rileva una vulnerabilità nelle dipendenze dei pacchetti applicativi della funzione Lambda, Amazon Inspector fornisce una ricerca dettagliata del tipo di vulnerabilità del pacchetto.

Per istruzioni sull'attivazione di un tipo di scansione, consulta. Attivazione di un tipo di scansione

> **Note**
>
> La scansione standard Lambda non analizza la dipendenza AWS SDK installata per impostazione predefinita nell'ambiente di runtime Lambda. Amazon Inspector analizza solo le dipendenze caricate con il codice della funzione o ereditate da un livello.

> **Note**
>
> La disattivazione della scansione standard di Amazon Inspector Lambda disattiverà anche la scansione del codice Amazon Inspector Lambda.

Esclusione delle funzioni dalla scansione standard Lambda

Puoi etichettare determinate funzioni per escluderle dalle scansioni standard di Amazon Inspector Lambda. L'esclusione di funzioni dalle scansioni può aiutare a prevenire avvisi non utilizzabili.

Per escludere una funzione Lambda dalla scansione standard Lambda, contrassegna la funzione con la seguente coppia chiave-valore:

- Chiave: `InspectorExclusion`
- Valore: `LambdaStandardScanning`

Per escludere una funzione dalla scansione standard Lambda

1. Apri la console Lambda all'indirizzo https://console.aws.amazon.com/lambda/.
2. Seleziona Funzioni.
3. Dalla tabella delle funzioni, seleziona il nome di una funzione che desideri escludere dalla scansione standard di Amazon Inspector Lambda.
4. Seleziona Configurazione e scegli Tag dal menu.
5. Seleziona Gestisci tag, quindi Aggiungi nuovo tag.
6. Nel campo Chiave, inserisci`InspectorExclusion`, quindi nel campo Valore, inserisci`LambdaStandardScanning`.
7. Seleziona Salva per aggiungere il tag ed escludere la funzione dalla scansione standard di Amazon Inspector Lambda.

Per ulteriori informazioni sull'aggiunta di tag in Lambda, consulta Uso dei tag nelle funzioni Lambda.

Scansione del codice Amazon Inspector Lambda

> **Important**
>
> La scansione del codice acquisisce frammenti di codice dalle funzioni Lambda per evidenziare le vulnerabilità rilevate. Questi frammenti possono mostrare credenziali codificate o altri materiali sensibili in testo non crittografato.

La scansione del codice Lambda di Amazon Inspector analizza il codice applicativo personalizzato all'interno di una funzione Lambda alla ricerca di vulnerabilità del codice in base alle best practice

di sicurezza. AWS La scansione del codice Lambda può rilevare difetti di iniezione, fughe di dati, crittografia debole o crittografia mancante nel codice. Per informazioni sulle regioni disponibili, consulta. Disponibilità di funzionalità specifiche per ogni regione

La scansione standard Lambda è una funzionalità che valuta le dipendenze del pacchetto applicativo utilizzate in una funzione per vulnerabilità ed esposizioni comuni (CVE). È possibile attivare la scansione del codice Lambda insieme alla scansione standard Lambda.

Amazon Inspector valuta il codice applicativo della funzione Lambda utilizzando il ragionamento automatico e l'apprendimento automatico che analizza il codice dell'applicazione per una conformità di sicurezza complessiva. Identifica le violazioni delle politiche e le vulnerabilità sulla base di rilevatori interni sviluppati in collaborazione con Amazon. CodeGuru Per un elenco dei possibili rilevamenti, consulta la Detector Library. CodeGuru

Se Amazon Inspector rileva una vulnerabilità nel codice dell'applicazione della funzione Lambda, Amazon Inspector fornisce una ricerca dettagliata del tipo di vulnerabilità del codice. Questo tipo di risultato include la posizione esatta del problema nel codice, un frammento di codice che mostra il problema e la soluzione suggerita. La correzione suggerita include blocchi di plug-and-play codice che è possibile utilizzare per sostituire le righe di codice vulnerabili. Queste correzioni di codice suggerite vengono fornite in aggiunta alle indicazioni generali sulla correzione del codice per tale risultato.

> **Important**
>
> I suggerimenti per la correzione del codice si basano su servizi di ragionamento automatico e intelligenza artificiale generativa e pertanto potrebbero non funzionare come previsto. L'utente è responsabile dei suggerimenti per la correzione del codice che adotta. Esamina sempre i suggerimenti per la correzione del codice prima di adottarli. Potrebbe essere necessario apportare modifiche ai suggerimenti di correzione del codice per garantire che il codice funzioni come previsto. Consulta la Politica sull'IA responsabile.

Crittografia del codice nei risultati delle vulnerabilità del codice

I frammenti di codice rilevati in relazione alla rilevazione di una vulnerabilità del codice mediante la scansione del codice Lambda vengono archiviati dal servizio. CodeGuru Per impostazione predefinita, CodeGuru viene utilizzata una chiave di AWS proprietà controllata da per crittografare il codice, tuttavia, puoi utilizzare la tua chiave gestita dal cliente per la crittografia tramite l'API Amazon

Inspector. Per ulteriori informazioni, consulta Crittografia inattiva per il codice contenuto nei tuoi risultati.

La scansione del codice Lambda può essere attivata insieme alla scansione standard Lambda. Per istruzioni sull'attivazione di un tipo di scansione, vedere. Attivazione di un tipo di scansione

Esclusione delle funzioni dalla scansione del codice Lambda

Puoi etichettare determinate funzioni per escluderle dalle scansioni del codice di Amazon Inspector Lambda. L'esclusione di funzioni dalle scansioni può aiutare a prevenire avvisi non utilizzabili.

Per escludere una funzione Lambda da Amazon Inspector, Lambda code scan contrassegna la funzione con la seguente coppia chiave-valore:

- Chiave: `InspectorCodeExclusion`
- Valore: `LambdaCodeScanning`

Per escludere una funzione dalla scansione del codice Lambda

1. Accedi alla console Lambda all'indirizzo https://console.aws.amazon.com/lambda/.
2. Seleziona Funzioni.
3. Dalla tabella delle funzioni, seleziona il nome di una funzione che desideri escludere dalla scansione del codice di Amazon Inspector Lambda.
4. Seleziona Configurazione e scegli Tag dal menu.
5. Seleziona Gestisci tag, quindi Aggiungi nuovo tag.
6. Nel campo Chiave, inserisci`InspectorCodeExclusion`, quindi nel campo Valore, inserisci`LambdaCodeScanning`.
7. Seleziona Salva per aggiungere il tag ed escludere la funzione dalla scansione del codice Amazon Inspector Lambda.

Per ulteriori informazioni sull'aggiunta di tag in Lambda, consulta Uso dei tag nelle funzioni Lambda.

Disattivazione di un tipo di scansione

Puoi disattivare un nuovo tipo di scansione Amazon Inspector in qualsiasi momento. Quando disattivi un tipo di scansione, perdi l'accesso a tutti i risultati esistenti prodotti da quel tipo di scansione. Se

riattivi il tipo di scansione, le tue risorse idonee vengono scansionate e Amazon Inspector produrrà nuove scoperte. Per tenere traccia dei dati relativi ai risultati, puoi esportare i risultati prima della disattivazione. Per ulteriori informazioni, consulta Esportazione dei report dei risultati da Amazon Inspector.

Quando si disattiva un tipo di scansione, possono verificarsi alcune modifiche in quell' AWS account a seconda del tipo di scansione disattivato. Di seguito sono riportate le modifiche che si verificheranno quando si disattivano questi tipi di scansione:

- Scansione Amazon EC2: quando disattivi la scansione di Amazon Inspector Amazon EC2 per un account, vengono eliminate le seguenti associazioni SSM utilizzate da Amazon Inspector:
  - `InspectorDistributor-do-not-delete`
  - `InspectorInventoryCollection-do-not-delete`
  - `InspectorLinuxDistributor-do-not-delete`
  - `InvokeInspectorLinuxSsmPlugin-do-not-delete`
  - `InvokeInspectorSsmPlugin-do-not-delete`. Inoltre, il plug-in Amazon Inspector SSM installato tramite questa associazione viene rimosso da tutti i tuoi host. Windows Per ulteriori informazioni, consulta Scansione Windows delle istanze.
- Scansione Amazon ECR: quando disattivi la scansione delle immagini dei container Amazon ECR per un account, il tipo di scansione Amazon ECR per quell'account cambia da Scansione avanzata con Amazon Inspector a scansione di base con Amazon ECR.
- Scansione Lambda standard: quando si disattiva la scansione standard Lambda in un account, viene disattivata la scansione del codice Lambda se era attiva anche la scansione del codice. Inoltre, il canale collegato al CloudTrail servizio creato quando la scansione era abilitata viene eliminato.

Disattivazione delle scansioni

La disattivazione di tutti i tipi di scansione per un account disattiva Amazon Inspector per quell'account. Regione AWS Per ulteriori informazioni, consulta Disattivazione di Amazon Inspector.

Per completare questa procedura per un ambiente con più account, segui questi passaggi dopo aver effettuato l'accesso come amministratore delegato di Amazon Inspector.

Console

Per disattivare le scansioni

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri disattivare le scansioni.
3. Nel riquadro di navigazione, scegli Gestione account.
4. Scegli la scheda Account per mostrare lo stato di scansione di un account.
5. Seleziona la casella di controllo di ogni account per il quale desideri disattivare le scansioni.
6. Scegli Azioni e, tra le opzioni Disattiva, seleziona il tipo di scansione che desideri disattivare.
7. (Consigliato) Ripeti questi passaggi Regione AWS per ognuno dei quali desideri disattivare quel tipo di scansione.

API

Esegui l'operazione Disable API. Nella richiesta, fornisci gli ID dell'account per cui stai disattivando le scansioni e per `resourceTypes` fornire uno o più di`EC2`, `ECR`, `LAMBDA`, o `LAMBDA_CODE` per disattivare le scansioni.

Scansioni del Center for Internet Security (CIS) per le istanze EC2

Quando abiliti la scansione Amazon Inspector EC2 per un account, consenti ad Amazon Inspector di eseguire o pianificare scansioni CIS. Amazon Inspector CIS esegue una scansione comparativa dei sistemi operativi delle istanze Amazon EC2 per verificare se sono configurate in base alle raccomandazioni sulle best practice stabilite dal Center for Internet Security. Il programma CIS Security Benchmarks fornisce linee guida di configurazione standard del settore e best practice per configurare in modo sicuro un sistema. Per ulteriori informazioni, consulta Cosa sono i benchmark CIS?

Amazon Inspector esegue scansioni CIS su istanze Amazon EC2 di destinazione in base ai tag dell'istanza e alla pianificazione di scansione definiti in una configurazione di scansione. Per ogni istanza mirata, Amazon Inspector esegue una serie di controlli sull'istanza. Ogni controllo valuta se la configurazione del sistema soddisfa una raccomandazione specifica di CIS Benchmark. Ogni controllo ha un ID e un titolo di controllo CIS, che sono direttamente correlati a una raccomandazione CIS Benchmark per quella piattaforma. Al termine di una scansione, è possibile visualizzare i risultati e vedere quali controlli l'istanza ha superato, non è riuscito o ignorato per quel sistema.

Requisiti delle istanze EC2 per le scansioni CIS di Amazon Inspector

Per eseguire una scansione CIS sulla tua istanza, Amazon Inspector richiede che l'istanza soddisfi i seguenti criteri:

- Il sistema operativo dell'istanza è uno dei sistemi operativi supportati per le scansioni CIS. Per un elenco completo dei sistemi operativi supportati, vedere. Sistemi operativi supportati: scansione CIS
- L'istanza è un'istanza gestita di Amazon EC2 Systems Manager (SSM). Per ulteriori informazioni, consulta Working with SSM Agent.
- Nell'istanza è installato il plug-in Amazon Inspector SSM. Amazon Inspector installa automaticamente questo plug-in per le istanze gestite SSM.
- L'istanza ha un profilo di istanza che concede le autorizzazioni a SSM per gestire l'istanza e Amazon Inspector per eseguire scansioni CIS per quell'istanza. Per concedere queste autorizzazioni, collega le ManagedCispolicy politiche AmazonInspector2FullAccess, AmazonSSM

ManagedInstanceCore e 2 a un ruolo IAM e associa AmazonInspectorquel ruolo alla tua istanza come profilo di istanza. Per istruzioni sulla creazione e il collegamento di un profilo di istanza, consulta Work with IAM roles nella Amazon EC2 User Guide.

> **Note**
>
> L'abilitazione dell'ispezione approfondita di Amazon Inspector non è più un requisito quando si esegue una scansione CIS su un'istanza. Se disabiliti l'ispezione approfondita, Amazon Inspector continua a installare l'agente SSM, ma il plug-in non verrà più richiamato per eseguire l'ispezione approfondita. Ciò significa che nel tuo account sarà presente la seguente associazione:. `InspectorLinuxDistributor-do-not-delete`

Esecuzione di scansioni CIS

È possibile eseguire una scansione CIS una volta su richiesta o come scansione periodica pianificata. Per eseguire una scansione, è innanzitutto necessario creare una configurazione di scansione.

Quando si crea una configurazione di scansione, si specificano le coppie chiave-valore di tag da utilizzare per indirizzare le istanze. Se sei l'amministratore delegato di Amazon Inspector di un'organizzazione, puoi specificare più account nella configurazione di scansione e Amazon Inspector cercherà le istanze con i tag specificati in ciascuno di questi account. Scegli il livello CIS Benchmark per la scansione. Per ogni benchmark, CIS supporta un profilo di livello 1 e di livello 2 progettato per fornire linee di base per i diversi livelli di sicurezza richiesti da ambienti diversi.

- Livello 1: consiglia le impostazioni di sicurezza di base essenziali che possono essere configurate su qualsiasi sistema. L'implementazione di queste impostazioni dovrebbe causare interruzioni del servizio minime o nulle. L'obiettivo di queste raccomandazioni è ridurre il numero di punti di ingresso nei sistemi, riducendo i rischi complessivi per la sicurezza informatica.
- Livello 2: consiglia impostazioni di sicurezza più avanzate per ambienti ad alta sicurezza. L'implementazione di queste impostazioni richiede pianificazione e coordinamento per ridurre al minimo il rischio di impatto aziendale. L'obiettivo di queste raccomandazioni è aiutarti a raggiungere la conformità normativa.

Il livello 2 estende il livello 1. Quando scegli il livello 2, Amazon Inspector verifica tutte le configurazioni consigliate per il livello 1 e il livello 2.

Dopo aver definito i parametri per la scansione, puoi scegliere se eseguirla come scansione singola, che viene eseguita dopo aver completato la configurazione, o come scansione ricorrente. Le scansioni ricorrenti possono essere eseguite giornalmente, settimanalmente o mensilmente, in un momento a scelta.

> **Tip**
>
> Ti consigliamo di scegliere un giorno e un'ora che abbiano meno probabilità di influire sul sistema mentre la scansione è in esecuzione.

Per creare una configurazione di scansione CIS

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona il Regione AWS punto in cui desideri eseguire una scansione CIS.
3. Dal pannello di navigazione, in Scansioni su richiesta, seleziona Scansioni CIS.
4. Scegli Crea nuova scansione.
    a. Inserisci un nome di configurazione della scansione.
    b. Per la risorsa Target, inserisci la chiave e il valore corrispondente di un tag sulle istanze che desideri scansionare. È possibile specificare un totale di 25 tag da includere nella scansione e per ogni chiave è possibile specificare fino a cinque valori diversi.
    c. Scegliete un livello CIS Benchmark. È possibile selezionare il livello 1 per le configurazioni di sicurezza di base o il livello 2 per le configurazioni di sicurezza avanzate.
5. Per gli account Target, specifica quali account includere nella scansione. Un account indipendente o un membro di un'organizzazione può selezionare Self per creare una configurazione di scansione per il proprio account. Un amministratore delegato di Amazon Inspector può selezionare Tutti gli account per scegliere come target tutti gli account all'interno dell'organizzazione oppure selezionare Specificare gli account e specificare un sottoinsieme di account membri da scegliere come target. L'amministratore delegato può inserire `SELF` invece di un ID account per creare una configurazione di scansione per il proprio account. Per ulteriori informazioni, consulta Considerazioni sulla gestione delle scansioni CIS di Amazon Inspector in un'organizzazione AWS.

6. Scegli una pianificazione per le scansioni. Scegli tra Scansione singola, che verrà eseguita non appena avrai finito di creare la configurazione di scansione, o Scansioni ricorrenti, che verranno eseguite all'ora pianificata che scegli fino all'eliminazione.
7. Scegli Crea per completare la creazione della configurazione di scansione.

Visualizzazione e modifica delle configurazioni di scansione CIS

È possibile visualizzare o modificare le scansioni precedentemente pianificate in qualsiasi momento.

Per visualizzare o modificare una configurazione di scansione CIS

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la posizione in Regione AWS cui hai creato la configurazione di scansione CIS.
3. Dal pannello di navigazione, in Scansioni su richiesta, seleziona Scansioni CIS.
4. Scegli Pianificato per visualizzare le configurazioni di scansione pianificate.
5. Seleziona un elemento dalla colonna Nome della configurazione di scansione per aprire i dettagli di quella configurazione di scansione.
6. (Facoltativo) Scegliete Modifica per modificare i parametri di questa scansione.

Visualizzazione dei risultati delle scansioni CIS

Amazon Inspector crea un processo di scansione ogni volta che viene eseguita una configurazione di scansione e raccoglie i risultati della scansione con un ID di scansione univoco.

I risultati della scansione sono disponibili per 90 giorni dopo il completamento della scansione. È possibile visualizzare i risultati della scansione aggregati per assegno o per risorsa di destinazione.

Risultati della scansione aggregati per controlli

I risultati della scansione sono raggruppati in base a ogni singolo controllo eseguito durante la scansione. Per ogni controllo, viene visualizzato un rapporto su quante risorse sono state superate, non riuscite o sono state ignorate.

Risultati della scansione aggregati per risorsa

I risultati della scansione sono raggruppati per ogni risorsa a cui è destinata la configurazione di scansione. Per ogni risorsa, viene visualizzato un rapporto contenente i controlli relativi a una risorsa che ha superato, ha avuto esito negativo o è stata ignorata per quella risorsa.

Per visualizzare i risultati della scansione

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona il punto in Regione AWS cui desideri visualizzare i risultati della scansione.
3. Dal pannello di navigazione, in Scansioni su richiesta, seleziona Scansioni CIS.
4. Seleziona l'ID della scansione di cui desideri visualizzare i risultati nella colonna Scan ID.
5. Scegli come visualizzare i risultati della scansione:
    - Seleziona la scheda Controlli per visualizzare i risultati della scansione aggregati per controlli.
        - Per un controllo elencato, seleziona un numero tra superato, ignorato o non riuscito nella colonna Stato della risorsa per aprire una visualizzazione delle risorse filtrate in base a quello stato e a quel controllo.
    - Seleziona la scheda Risorse scansionate per visualizzare i risultati della scansione aggregati per risorsa.
        - Seleziona una risorsa per aprire un pannello dei dettagli che elenca i controlli che la risorsa ha superato, non riuscito o ignorato.
6. (Facoltativo) Utilizzate la barra dei filtri in entrambe le visualizzazioni per affinare i risultati.

È possibile scaricare i risultati di una scansione CIS utilizzando la console o l'API.

Per scaricare i risultati della scansione

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona il punto in Regione AWS cui desideri visualizzare i risultati della scansione.
3. Dal pannello di navigazione, in Scansioni su richiesta, seleziona Scansioni CIS.
4. Seleziona l'ID della scansione di cui desideri visualizzare i risultati nella colonna Scan ID.

5. Scegli Download (Scarica). Se sei l'amministratore delegato, puoi scegliere di scaricare i risultati per account membri specifici.

Considerazioni sulla gestione delle scansioni CIS di Amazon Inspector in un'organizzazione AWS

Quando si eseguono scansioni CIS all'interno di un'organizzazione, gli account dei membri e gli amministratori delegati di Amazon Inspector interagiscono con le configurazioni e i risultati delle scansioni CIS in modi diversi.

Quando un amministratore delegato crea una configurazione di scansione CIS per tutti gli account o un elenco di ID di account membri, l'organizzazione è proprietaria di tale configurazione di scansione. Indipendentemente dall'account, l'attuale amministratore delegato può gestire le configurazioni di scansione di proprietà dell'organizzazione, anche se sono state create da un account diverso. Le configurazioni di scansione CIS di proprietà dell'organizzazione avranno un ARN che elenca l'ID dell'organizzazione come proprietario, seguendo lo schema:. `arn:aws:inspector2:`*`Region`*`:`*`111122223333`*`:owner/`*`OrganizationId`*`/cis-configuration/`*`scanId` L'ID dell'account sarà l'ID dell'account di gestione Organizations.

> **Important**
>
> Non è possibile aggiungere tag alle configurazioni di scansione CIS di proprietà dell'organizzazione.

Quando un amministratore delegato crea una configurazione di scansione e la specifica `SELF` come account di destinazione, il suo account possiede quella configurazione di scansione. Anche se lasciano la propria organizzazione, possono comunque gestire quella configurazione di scansione.

> **Note**
>
> Un amministratore delegato non può modificare gli obiettivi di una configurazione di scansione destinata. `SELF`

Le configurazioni di scansione create da account membri, account autonomi o amministratori delegati con `SELF` come destinazione sono di proprietà dell'account che le ha create. Queste

configurazioni di scansione CIS hanno un ARN che elenca quell'account come proprietario seguendo lo schema:. `arn:aws:inspector2:Region:111122223333:owner/111122223333/cis-configuration/scanId` L'ID account sarà l'account che ha creato la scansione.

Un account membro di un'organizzazione può creare configurazioni di scansione per il proprio account. L'amministratore delegato può visualizzare le configurazioni di scansione create dai membri ma non può modificarle o eliminarle. Se un account membro lascia l'organizzazione, l'amministratore delegato non sarà più in grado di vedere le configurazioni di scansione create da quell'account.

L'amministratore delegato può visualizzare i risultati delle scansioni di qualsiasi account dell'organizzazione, compresi quelli pianificati dai membri. Un account membro può visualizzare i risultati di qualsiasi scansione CIS delle risorse del proprio account, incluse quelle pianificate dall'amministratore delegato.

Bucket Amazon S3 di proprietà di Amazon Inspector utilizzati per le scansioni CIS di Amazon Inspector

Amazon Inspector fornisce i file di definizione Open Vulnerability and Assessment Language (OVAL) aggiornati necessari per le scansioni CIS. La tabella seguente elenca tutti i bucket Amazon S3 di proprietà di Amazon Inspector con definizioni OVAL utilizzati dalla scansione CIS per ogni supporto. Regione AWS Se necessario, i bucket devono essere consentiti nell'elenco dei VPC.

> **Note**
>
> I dettagli per ciascuno dei seguenti bucket Amazon S3 di proprietà di Amazon Inspector non sono soggetti a modifiche. Tuttavia, l'elenco potrebbe essere aggiornato in base alle nuove novità di supporto. Regioni AWS Non puoi usare questi bucket per altre operazioni Amazon S3 o nei tuoi bucket Amazon S3.

Bucket CIS	Regione AWS
`cis-datasets-prod-arn-5908f6f`	Europa (Stoccolma)
`cis-datasets-prod-bah-8f88801`	Medio Oriente (Bahrein)
`cis-datasets-prod-bjs-0f40506`	Cina (Pechino)

Bucket CIS	Regione AWS
cis-datasets-prod-bom-435a167	Asia Pacifico (Mumbai)
cis-datasets-prod-cdg-f3a9c58	Europa (Parigi)
cis-datasets-prod-cgk-09eb12f	Asia Pacifico (Giacarta)
cis-datasets-prod-cmh-63030b9	Stati Uniti orientali (Ohio)
cis-datasets-prod-cpt-02c5c6f	Africa (Città del Capo)
cis-datasets-prod-dub-984936f	Europa (Irlanda)
cis-datasets-prod-fra-6eb96eb	Europa (Francoforte)
cis-datasets-prod-gru-de69f99	Sud America (San Paolo)
cis-datasets-prod-hkg-8e30800	Asia Pacifico (Hong Kong)
cis-datasets-prod-iad-8438411	Stati Uniti orientali (Virginia settentrionale)
cis-datasets-prod-icn-f4eff1c	Asia Pacifico (Seoul)
cis-datasets-prod-kix-5743b21	Asia Pacifico (Osaka-Locale)
cis-datasets-prod-lhr-8b1fbd0	Europa (Londra)
cis-datasets-prod-mxp-7b1bbce	Europa (Milano)
cis-datasets-prod-nrt-464f684	Asia Pacifico (Tokyo)
cis-datasets-prod-osu-5bead6f	AWS GovCloud (Stati Uniti orientali)
cis-datasets-prod-pdt-adadf9c	AWS GovCloud (Stati Uniti occidentali)
cis-datasets-prod-pdx-acfb052	US West (Oregon)
cis-datasets-prod-sfo-1515ba8	Stati Uniti occidentali (California settentrionale)
cis-datasets-prod-sin-309725b	Asia Pacifico (Singapore)

Bucket CIS	Regione AWS
`cis-datasets-prod-syd-f349107`	Asia Pacifico (Sydney)
`cis-datasets-prod-yul-5e0c95e`	Canada (Centrale)
`cis-datasets-prod-zhy-5a8eacb`	Cina (Ningxia)
`cis-datasets-prod-zrh-67e0e3d`	Europa (Zurigo)

Valutazione della copertura di Amazon Inspector del tuo ambiente AWS

Per aiutarti a valutare e interpretare la copertura di Amazon Inspector del tuo AWS ambiente, la pagina di gestione degli account sulla console Amazon Inspector fornisce statistiche e dettagli sullo stato della scansione di account e risorse da parte di Amazon Inspector. Con questa pagina, puoi esaminare le statistiche aggregate e altri dati relativi alle tue risorse. Puoi anche eseguire un'analisi approfondita della copertura di Amazon Inspector per le singole risorse e approfondire i risultati per risorse specifiche. Se sei l'amministratore delegato di Amazon Inspector di un'organizzazione, i dati includono statistiche e dettagli per tutti gli account dell'organizzazione.

Per valutare la copertura di Amazon Inspector del tuo ambiente AWS

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Nel riquadro di navigazione, scegli Gestione dell'account.
3. Nella pagina Gestione dell'account, scegli la scheda per una delle cinque diverse visualizzazioni di copertura:

   - Account, per una copertura a livello di account.
   - Istanze, per la copertura delle istanze Amazon Elastic Compute Cloud (Amazon EC2).
   - Repository, per la copertura dei repository Amazon Elastic Container Registry (Amazon ECR).
   - Immagini, per la copertura delle immagini dei container Amazon ECR.
   - Lambda, per la copertura delle funzioni Lambda.

Gli argomenti di questa sezione descrivono le informazioni fornite da ciascuna scheda, incluso lo stato di scansione che può avere una singola risorsa.

Argomenti

Valutazione della copertura a livello di account

Se il tuo account non fa parte di un'organizzazione o non è l'account amministratore delegato di Amazon Inspector di un'organizzazione, la scheda Account fornisce informazioni sul tuo account e sullo stato della scansione delle risorse per il tuo account. In questa scheda, puoi attivare o disattivare la scansione di tutti o solo tipi specifici di risorse per il tuo account. Per ulteriori informazioni, consulta Scansione automatizzata delle risorse con Amazon Inspector.

Se il tuo account è l'account amministratore delegato di Amazon Inspector per un'organizzazione, la scheda Account fornisce le impostazioni di attivazione automatica per gli account della tua organizzazione ed elenca tutti gli account dell'organizzazione. Per ogni account, l'elenco indica se Amazon Inspector è attivato per l'account e, in caso affermativo, i tipi di scansione delle risorse attivati per l'account. In qualità di amministratore delegato, puoi utilizzare questa scheda per modificare le impostazioni di attivazione automatica per la tua organizzazione. È inoltre possibile attivare o disattivare tipi specifici di scansione delle risorse per gli account dei singoli membri. Per ulteriori informazioni, consulta Attivazione delle scansioni Amazon Inspector per gli account dei membri.

Valutazione della copertura delle istanze Amazon EC2

La scheda Istanze mostra le istanze Amazon EC2 nel tuo ambiente. AWS Gli elenchi sono organizzati in gruppi nelle seguenti schede:

- Tutto: mostra tutte le istanze presenti nell'ambiente. La colonna Stato indica lo stato di scansione corrente di un'istanza.
- Scansione: mostra tutte le istanze che Amazon Inspector monitora e analizza attivamente nel tuo ambiente.
- Nessuna scansione: mostra tutte le istanze che Amazon Inspector non monitora e non analizza nel tuo ambiente. La colonna Reason indica perché Amazon Inspector non monitora e analizza un'istanza.

  Un'istanza EC2 può apparire nella scheda Not scanning per diversi motivi. Amazon Inspector utilizza AWS Systems Manager (SSM) e l'agente SSM per monitorare e scansionare automaticamente le istanze EC2 alla ricerca di vulnerabilità. Se un'istanza non ha l'agente SSM in esecuzione, non ha un ruolo AWS Identity and Access Management (IAM) che supporti Systems Manager o non esegue un sistema operativo o un'architettura supportati, Amazon Inspector non

può monitorare e scansionare l'istanza. Per ulteriori informazioni, consulta Scansione delle istanze Amazon EC2.

In ogni scheda, la colonna Account specifica chi possiede un' Account AWS istanza.

Tag dell'istanza EC2: questa colonna mostra i tag associati all'istanza e può essere utilizzata per determinare se l'istanza è stata esclusa dalle scansioni per tag.

Sistema operativo: questa colonna mostra il tipo di sistema operativo, che può essere`WINDOWS`, `MACLINUX`, o. `UNKNOWN`

Monitorato tramite: questa colonna mostra se Amazon Inspector utilizza il metodo di scansione basato su agenti o senza agente su questa istanza.

Ultima scansione: questa colonna mostra l'ultima volta che Amazon Inspector ha verificato la presenza di vulnerabilità nella risorsa. La frequenza con cui Amazon Inspector esegue le scansioni dipende dal metodo di scansione utilizzato per eseguire la scansione dell'istanza.

Per visualizzare ulteriori dettagli su un'istanza EC2, scegli il link nella colonna delle istanze EC2. Amazon Inspector visualizza quindi i dettagli sull'istanza e i risultati correnti relativi all'istanza. Per esaminare i dettagli di un risultato, scegli il link nella colonna Titolo. Per informazioni su questi dettagli, consultaInformazioni sulla ricerca di Amazon Inspector.

Valori dello stato di scansione per le istanze Amazon EC2

Per un'istanza Amazon Elastic Compute Cloud (Amazon EC2) Elastic Compute EC2, i valori Status possibili sono:

- Monitoraggio attivo: Amazon Inspector monitora e analizza continuamente l'istanza.
- Istanza EC2 interrotta: Amazon Inspector ha sospeso la scansione dell'istanza perché l'istanza si trova in uno stato interrotto. Tutti i risultati esistenti persisteranno fino alla chiusura dell'istanza. Se l'istanza viene riavviata, Amazon Inspector riprenderà automaticamente la scansione dell'istanza.
- Errore interno: si è verificato un errore interno quando Amazon Inspector ha tentato di scansionare l'istanza. Amazon Inspector risolverà automaticamente l'errore e riprenderà la scansione il prima possibile.
- Nessun inventario: Amazon Inspector non è riuscito a trovare l'inventario delle applicazioni software da scansionare per l'istanza. Le associazioni Amazon Inspector per l'istanza potrebbero essere state eliminate o potrebbero non essere state eseguite.

Per risolvere questo problema, usa AWS Systems Manager per assicurarti che l'`InspectorInventoryCollection-do-not-delete`associazione esista e che il suo stato di associazione abbia esito positivo. Inoltre, utilizzate AWS Systems Manager Fleet Manager per verificare l'inventario delle applicazioni software per l'istanza.

- Disattivazione in sospeso: Amazon Inspector ha interrotto la scansione dell'istanza. L'istanza viene disabilitata, in attesa del completamento delle attività di pulizia.
- Scansione iniziale in sospeso: Amazon Inspector ha messo in coda l'istanza per una scansione iniziale.
- Risorsa terminata: l'istanza è stata terminata. Amazon Inspector sta attualmente ripulendo i risultati e i dati di copertura esistenti per l'istanza.
- Inventario obsoleto: Amazon Inspector non è stato in grado di raccogliere un inventario aggiornato delle applicazioni software acquisito negli ultimi 7 giorni per l'istanza.

  Per risolvere questo problema, assicurati che AWS Systems Manager le associazioni Amazon Inspector richieste esistano e siano in esecuzione per l'istanza. Inoltre, utilizza AWS Systems Manager Fleet Manager per verificare l'inventario delle applicazioni software per l'istanza.
- Istanza EC2 non gestita: Amazon Inspector non monitora o analizza l'istanza. L'istanza non è gestita da. AWS Systems Manager

  Per risolvere questo problema, puoi utilizzare il AWSSupport-TroubleshootManagedInstance runbookservizio fornito da AWS Systems Manager Automation. Dopo la configurazione AWS Systems Manager per la gestione dell'istanza, Amazon Inspector inizierà automaticamente a monitorare e scansionare continuamente l'istanza.
- Sistema operativo non supportato: Amazon Inspector non monitora o scansiona l'istanza. L'istanza utilizza un sistema operativo o un'architettura che Amazon Inspector non supporta. Per un elenco dei sistemi operativi supportati da Amazon Inspector, consulta. Sistemi operativi supportati per la scansione di Amazon EC2
- Monitoraggio attivo con errori parziali: questo stato indica che la scansione EC2 è attiva, ma sono presenti errori associati. Ispezione approfondita di Amazon Inspector per istanze Amazon EC2 Linux I possibili errori nelle ispezioni approfondite sono:
  - Limite di raccolta dei pacchetti con ispezione approfondita superato: l'istanza ha superato il limite di 5000 pacchetti per l'ispezione approfondita di Amazon Inspector. Per riprendere l'ispezione approfondita per questa istanza, puoi provare a modificare i percorsi personalizzati associati all'account.

- Superato il limite di inventario SSM giornaliero di Deep Inspector: l'agente SSM non è riuscito a inviare l'inventario ad Amazon Inspector perché la quota SSM per i dati di inventario raccolti per istanza al giorno è già stata raggiunta per questa istanza. Per ulteriori informazioni, consulta Endpoint e quote di Amazon EC2 Systems Manager.
- Superato il limite di ritiro per l'ispezione approfondita: Amazon Inspector non è riuscito a estrarre l'inventario del pacco perché il tempo di ritiro del pacco ha superato la soglia massima di 15 minuti.
- L'ispezione approfondita non ha un inventario: il plug-in Amazon Inspector SSM non è ancora stato in grado di raccogliere un inventario dei pacchetti per questo caso. Di solito è il risultato di una scansione in sospeso, tuttavia, se questo stato persiste dopo 6 ore, usa Amazon EC2 Systems Manager per assicurarti che le associazioni Amazon Inspector richieste esistano e siano in esecuzione per l'istanza.

Per dettagli sulla configurazione delle impostazioni di scansione per un'istanza EC2, consulta. Scansione delle istanze Amazon EC2

Valutazione della copertura dei repository Amazon ECR

La scheda Repositories mostra i repository Amazon ECR nel tuo ambiente. AWS Gli elenchi sono organizzati in gruppi nelle seguenti schede:

- Tutti: mostra tutti i repository presenti nell'ambiente. La colonna Stato indica lo stato di scansione corrente di un repository.
- Attivato: mostra tutti i repository che Amazon Inspector è configurato per monitorare e scansionare nel tuo ambiente. La colonna Status indica lo stato di scansione corrente di un repository.
- Non attivato: mostra tutti i repository che Amazon Inspector non monitora e non analizza nel tuo ambiente. La colonna Reason indica perché Amazon Inspector non monitora e scansiona un repository.

In ogni scheda, la colonna Account specifica il Account AWS proprietario di un repository.

Per esaminare ulteriori dettagli su un repository, scegli il nome del repository. Amazon Inspector visualizza quindi un elenco di immagini dei container nel repository e i dettagli per ogni immagine. I dettagli includono il tag dell'immagine, l'image digest e lo stato della scansione. Includono anche statistiche chiave sui risultati, come il numero di risultati critici per l'immagine. Per approfondire ed esaminare i dati di supporto per la ricerca di statistiche, scegli il tag dell'immagine.

Valori dello stato di scansione per i repository Amazon ECR

Per un repository Amazon Elastic Container Registry (Amazon ECR), i valori Status possibili sono:

- Attivato (continuo): per un repository, Amazon Inspector monitora continuamente le immagini in questo repository. L'impostazione di scansione avanzata per il repository è impostata sulla scansione continua. Amazon Inspector esegue inizialmente la scansione di nuove immagini quando vengono inviate e scansiona nuovamente le immagini se viene pubblicato un nuovo CVE relativo a quell'immagine. Amazon Inspector continuerà a monitorare le immagini in questo repository per la durata della scansione ECR configurata.
- Attivato (in modalità push): Amazon Inspector analizza automaticamente le immagini dei singoli container nel repository quando viene inviata una nuova immagine. La scansione avanzata è attivata per il repository e impostata per la scansione in modalità push.
- Accesso negato: Amazon Inspector non è autorizzato ad accedere al repository o alle immagini dei container in esso contenute.

  Per risolvere questo problema, assicurati che le policy AWS Identity and Access Management (IAM) per il repository consentano ad Amazon Inspector di accedere al repository.
- Disattivato (manuale): Amazon Inspector non monitora o scansiona le immagini dei container nel repository. L'impostazione di scansione Amazon ECR per il repository è impostata sulla scansione manuale di base.

  Per iniziare a scansionare le immagini nel repository con Amazon Inspector, modifica l'impostazione di scansione del repository su Scansione avanzata, quindi scegli se scansionare le immagini in modo continuo o solo quando viene inviata una nuova immagine.
- Attivato (in modalità push): Amazon Inspector analizza automaticamente le immagini dei singoli container nel repository quando viene inviata una nuova immagine. L'impostazione di scansione avanzata per il repository è impostata per la scansione in modalità push.
- Errore interno: si è verificato un errore interno quando Amazon Inspector ha tentato di scansionare il repository. Amazon Inspector risolverà automaticamente l'errore e riprenderà la scansione il prima possibile.

Per informazioni dettagliate sulla configurazione delle impostazioni di scansione per gli archivi. Scansione delle immagini dei container Amazon ECR

Valutazione della copertura delle immagini dei container Amazon ECR

La scheda Immagini mostra le immagini dei container Amazon ECR nel tuo AWS ambiente. Gli elenchi sono organizzati in gruppi nelle seguenti schede:

- Tutto: mostra tutte le immagini dei contenitori presenti nell'ambiente. La colonna Stato indica lo stato di scansione corrente di un'immagine.
- Scansione: mostra tutte le immagini dei container che Amazon Inspector è configurato per monitorare e scansionare nel tuo ambiente. La colonna Status indica lo stato di scansione corrente di un'immagine.
- Nessuna scansione: mostra tutte le immagini dei container che Amazon Inspector non monitora e non analizza nel tuo ambiente. La colonna Reason indica perché Amazon Inspector non monitora e scansiona un'immagine.

  L'immagine di un contenitore può apparire nella scheda Non attivato per diversi motivi. L'immagine potrebbe essere archiviata in un repository per il quale le scansioni di Amazon Inspector non sono attivate oppure le regole di filtro di Amazon ECR impediscono la scansione di tale repository. Oppure l'immagine non è stata spostata o recuperata entro il numero di giorni configurato per la durata della nuova scansione ECR. Per ulteriori informazioni, consulta Configurazione della durata della nuova scansione ECR.

In ogni scheda, la colonna Repository name specifica il nome del repository che memorizza l'immagine del contenitore. La colonna Account specifica il proprietario del Account AWS repository. La colonna Ultima scansione mostra quando Amazon Inspector ha controllato l'ultima volta la risorsa per individuare eventuali vulnerabilità. Ciò può includere controlli in caso di aggiornamento della ricerca dei metadati, di aggiornamento dell'inventario delle applicazioni della risorsa o di esecuzione di una nuova scansione in risposta a un nuovo CVE. Per ulteriori informazioni, consulta Comportamenti di scansione per la scansione Amazon ECR.

Per visualizzare ulteriori dettagli sull'immagine di un contenitore, scegliete il link nella colonna Immagine del contenitore ECR. Amazon Inspector visualizza quindi i dettagli sull'immagine e i risultati attuali relativi all'immagine. Per esaminare i dettagli di un risultato, scegli il link nella colonna Titolo. Per informazioni su questi dettagli, consultaInformazioni sulla ricerca di Amazon Inspector.

Valori dello stato di scansione per le immagini dei container Amazon ECR

Per un'immagine del contenitore Amazon Elastic Container Registry, i possibili valori Status sono:

- Monitoraggio attivo (continuo): Amazon Inspector monitora continuamente e l'immagine e le nuove scansioni vengono eseguite su di essa ogni volta che viene pubblicato un nuovo CVE pertinente. La durata della nuova scansione di Amazon ECR per l'immagine viene aggiornata ogni volta che l'immagine viene spinta o estratta. La scansione avanzata è abilitata per l'archivio che memorizza l'immagine e l'impostazione di scansione avanzata per il repository è impostata sulla scansione continua.
- Attivato (in modalità push): Amazon Inspector esegue automaticamente la scansione dell'immagine ogni volta che viene inviata una nuova immagine. La scansione avanzata è attivata per l'archivio che memorizza l'immagine e l'impostazione di scansione avanzata per il repository è impostata per la scansione in modalità push.
- Errore interno: si è verificato un errore interno quando Amazon Inspector ha tentato di scansionare l'immagine del contenitore. Amazon Inspector risolverà automaticamente l'errore e riprenderà la scansione il prima possibile.
- Scansione iniziale in sospeso: Amazon Inspector ha messo in coda l'immagine per una scansione iniziale.
- Idoneità alla scansione scaduta (continua): Amazon Inspector ha sospeso la scansione dell'immagine. L'immagine non è stata aggiornata entro la durata specificata per le scansioni automatiche delle immagini nel repository. È possibile premere o tirare l'immagine per riprendere la scansione.
- Idoneità alla scansione scaduta (in fase di invio): Amazon Inspector ha sospeso la scansione dell'immagine. L'immagine non è stata aggiornata entro la durata specificata per le scansioni automatiche delle immagini nel repository. È possibile premere l'immagine per riprendere la scansione.
- Frequenza di scansione manuale (manuale): Amazon Inspector non esegue la scansione dell'immagine del contenitore Amazon ECR. L'impostazione di scansione Amazon ECR per il repository che memorizza l'immagine è impostata sulla scansione manuale di base. Per avviare la scansione automatica dell'immagine con Amazon Inspector, modifica l'impostazione del repository su Enhanced Scanning, quindi scegli se scansionare le immagini in modo continuo o solo quando viene inviata una nuova immagine.
- Sistema operativo non supportato: Amazon Inspector non monitora o scansiona l'immagine. L'immagine è basata su un sistema operativo non supportato da Amazon Inspector o utilizza un tipo di supporto non supportato da Amazon Inspector.

Per un elenco dei sistemi operativi supportati da Amazon Inspector, consulta. Sistemi operativi supportati per la scansione Amazon ECR Per un elenco dei tipi di file multimediali supportati da Amazon Inspector, consulta Tipi di file multimediali supportati.

Per dettagli sulla configurazione delle impostazioni di scansione per archivi e immagini, consulta. Scansione delle immagini dei container Amazon ECR

Valutazione della copertura delle funzioni AWS Lambda

La scheda Lambda mostra le funzioni Lambda nel tuo ambiente. AWS Questa pagina contiene due tabelle, una che mostra i dettagli della copertura delle funzioni per la scansione standard Lambda e l'altra per la scansione del codice Lambda. È possibile raggruppare le funzioni in base alle seguenti schede:

- Tutte: mostra tutte le funzioni Lambda nel tuo ambiente. La colonna Status indica lo stato di scansione corrente per una funzione Lambda.
- Scansione: mostra le funzioni Lambda che Amazon Inspector è configurato per scansionare. La colonna Status indica lo stato di scansione corrente per ogni funzione Lambda.
- Nessuna scansione: mostra le funzioni Lambda che Amazon Inspector non è configurato per scansionare. La colonna Reason indica perché Amazon Inspector non monitora e analizza una funzione.

  Una funzione Lambda può apparire nella scheda Not scanning per diversi motivi. La funzione Lambda potrebbe appartenere a un account che non è stato aggiunto ad Amazon Inspector o le regole di filtro impediscono la scansione di questa funzione. Per ulteriori informazioni, consulta Funzioni di scansione AWS Lambda .

In ogni scheda, la colonna Nome funzione specifica il nome della funzione Lambda. La colonna Account specifica il proprietario della Account AWS funzione. Runtime specifica il runtime della funzione. La colonna Status indica lo stato di scansione corrente per ogni funzione Lambda. I tag delle risorse mostrano i tag che sono stati applicati alla funzione. La colonna Ultima scansione mostra quando Amazon Inspector ha controllato l'ultima volta la risorsa per individuare eventuali vulnerabilità. Ciò può includere controlli in caso di aggiornamento della ricerca dei metadati, di aggiornamento dell'inventario delle applicazioni della risorsa o di esecuzione di una nuova scansione in risposta a un nuovo CVE. Per ulteriori informazioni, consulta Comportamenti di scansione per la scansione della funzione Lambda.

Scansione dei valori di stato delle funzioni AWS Lambda

Per una funzione Lambda, i possibili valori Status sono:

- Monitoraggio attivo: Amazon Inspector monitora e analizza continuamente le funzioni Lambda. La scansione continua include una scansione iniziale delle nuove funzioni quando vengono inserite nell'archivio e una nuova scansione automatica delle funzioni quando vengono aggiornate o quando vengono rilasciate nuove vulnerabilità ed esposizioni comuni (CVE).
- Esclusa per tag: Amazon Inspector non analizza questa funzione perché è stata esclusa dalle scansioni tramite tag.
- Idoneità alla scansione scaduta: Amazon Inspector non monitora questa funzione perché sono trascorsi 90 giorni o più dall'ultima volta che è stata richiamata o aggiornata.
- Errore interno: si è verificato un errore interno quando Amazon Inspector ha tentato di scansionare la funzione. Amazon Inspector risolverà automaticamente l'errore e riprenderà la scansione il prima possibile.
- Scansione iniziale in sospeso: Amazon Inspector ha messo in coda la funzione per una scansione iniziale.
- Non supportato: la funzione Lambda ha un runtime non supportato.

Gestione di più account in Amazon Inspector with Organizations

Puoi utilizzare Amazon Inspector per gestire più account associati tramite Organizations AWS . Per gestire più account Amazon Inspector, l'account di gestione Organizations designa un account all'interno dell'organizzazione come account amministratore delegato per Amazon Inspector. L'amministratore delegato gestisce Amazon Inspector per l'organizzazione e riceve autorizzazioni speciali per eseguire attività per conto dell'organizzazione. Queste attività includono l'attivazione o la disattivazione delle scansioni degli account dei membri, la visualizzazione di dati aggregati relativi alle ricerche dell'intera organizzazione e la creazione e la gestione di regole di soppressione.

> **Note**
>
> Per abilitare a livello di codice Amazon Inspector per più account in Regioni AWS più account, puoi utilizzare uno script di shell sviluppato da Amazon Inspector. Per ulteriori informazioni sull'uso di questo script, consulta inspector2 - sul sito Web. enablement-with-cli GitHub

Argomenti

Comprendere la relazione tra account amministratore e account membro in Amazon Inspector

Quando utilizzi Amazon Inspector in un ambiente con più account, l'account amministratore delegato di Amazon Inspector ha accesso a determinati metadati. Questi metadati includono i dati di configurazione di Amazon EC2 e Amazon ECR e i risultati dei risultati dei risultati dei risultati relativi alla sicurezza per gli account dei membri. L'account amministratore può anche creare regole di soppressione dei risultati da applicare agli account dei membri. Per ulteriori informazioni, consulta Eliminazione dei risultati di Amazon Inspector con regole di soppressione.

Azioni dell'amministratore delegato

In genere, quando l'amministratore delegato applica impostazioni al proprio account, tali impostazioni vengono applicate a tutti gli altri account dell'organizzazione. L'amministratore delegato può inoltre visualizzare e recuperare informazioni relative al proprio account e a qualsiasi membro associato. Un account amministratore delegato di Amazon Inspector può eseguire le seguenti azioni:

- Visualizza e gestisci lo stato di Amazon Inspector per gli account associati, inclusa l'attivazione e la disattivazione di Amazon Inspector.
- Attiva o disattiva i tipi di scansione per tutti gli account membri dell'organizzazione.
- Visualizza i dati di ricerca aggregati in tutta l'organizzazione e i dettagli di ricerca per tutti gli account dei membri all'interno dell'organizzazione.
- Crea e gestisci regole di soppressione che si applicano ai risultati per tutti gli account dell'organizzazione.
- Attiva la scansione avanzata di Amazon ECR per tutti i membri dell'organizzazione.
- Visualizza la copertura delle risorse per l'intera organizzazione.
- Definisci la durata delle scansioni automatiche delle immagini dei contenitori ECR per tutti gli account membri dell'organizzazione. L'impostazione della durata della scansione dell'amministratore delegato sostituisce qualsiasi impostazione precedentemente impostata dall'account membro. Tutti gli account dell'organizzazione condividono la durata di risanamento automatico di Amazon ECR degli amministratori delegati. Non è possibile impostare durate di risanamento diverse per singoli account.
- Specificate cinque percorsi personalizzati per l'ispezione approfondita di Amazon Inspector per Amazon EC2 che verranno utilizzati in tutti gli account dell'organizzazione. Questo si aggiunge ai cinque percorsi personalizzati che un amministratore delegato può impostare per il proprio account individuale. Per ulteriori informazioni sulla configurazione dei percorsi personalizzati di Deep Inspection, vedere. Percorsi personalizzati per l'ispezione approfondita di Amazon Inspector
- Attiva e disattiva l'ispezione approfondita di Amazon Inspector per gli account dei membri.
- Esporta gli SBOM per tutti gli account dei membri dell'organizzazione.
- Imposta la modalità di scansione di Amazon EC2 per tutti gli account membri dell'organizzazione. Per ulteriori informazioni, consulta Gestione della modalità di scansione.
- Crea e gestisci configurazioni di scansione CIS per tutti gli account dell'organizzazione, ad eccezione delle configurazioni di scansione create dagli account dei membri.

> **Note**
>
> Se un account membro lascia l'organizzazione, l'amministratore delegato non sarà più in grado di vedere le configurazioni di scansione pianificate da quell'account.

- Visualizza i risultati della scansione CIS per tutti gli account dell'organizzazione.

Azioni relative agli account dei membri

Un account membro può visualizzare e recuperare informazioni sul proprio account in Amazon Inspector, mentre le impostazioni dell'account sono gestite dall'amministratore delegato. Gli account dei membri all'interno di un'organizzazione possono eseguire le seguenti azioni in Amazon Inspector:

- Attiva Amazon Inspector per il proprio account.
- Visualizza la copertura delle risorse per il proprio account.
- Visualizza i dettagli dei risultati per il proprio account.
- Visualizza l'impostazione della durata della nuova scansione automatica dell'immagine del contenitore ECR per il proprio account.
- Specificate cinque percorsi personalizzati per l'ispezione approfondita di Amazon Inspector per EC2 che verranno utilizzati per il loro account individuale. Questi percorsi vengono analizzati in aggiunta a tutti i percorsi personalizzati che l'amministratore delegato ha specificato per l'organizzazione. Per ulteriori informazioni sulla configurazione dei percorsi di ispezione approfondita, vedere. Percorsi personalizzati per l'ispezione approfondita di Amazon Inspector
- Visualizza i percorsi personalizzati impostati dal tuo amministratore delegato per l'ispezione approfondita di Amazon Inspector.
- Esporta gli SBOM per tutte le risorse associate al loro account.
- Visualizza la modalità di scansione del loro account.
- Crea e gestisci le configurazioni di scansione CIS per il loro account.
- Visualizza i risultati di tutte le scansioni CIS relative alle risorse del relativo account, incluse quelle pianificate dall'amministratore delegato.

> **Note**
>
> Dopo l'attivazione, Amazon Inspector può essere disattivato solo da un account amministratore delegato.

Designazione di un amministratore delegato per Amazon Inspector

Considerazioni importanti per gli amministratori delegati

Prendi nota dei seguenti fattori che definiscono il modo in cui l'amministratore delegato opera in Amazon Inspector:

Un amministratore delegato può gestire un massimo di 5.000 membri.

Ogni amministratore delegato di Amazon Inspector ha una quota di 5.000 account membri. Tuttavia, la tua organizzazione potrebbe includere più di 5.000 account. Se superi i 5.000 account membro, riceverai una notifica tramite Amazon CloudWatch Personal Health Dashboard e un'e-mail all'account amministratore delegato.

Un amministratore delegato è regionale.

Al contrario AWS Organizations, Amazon Inspector è un servizio regionale. Ciò significa che devi designare un amministratore delegato, aggiungere account membro e attivare i tipi di scansione in ognuno dei quali Regione AWS desideri utilizzare Amazon Inspector.

Un'organizzazione può avere un solo amministratore delegato.

Puoi avere un solo amministratore delegato per Amazon Inspector per un'organizzazione. Se hai designato un account come amministratore delegato in una regione, quell'account deve essere il tuo amministratore delegato in tutte le altre regioni.

La modifica di un amministratore delegato non disattiva Amazon Inspector per gli account dei membri.

Se rimuovi l'amministratore delegato, Amazon Inspector non verrà disattivato in quegli account e le impostazioni di scansione non ne risentiranno.

La tua AWS organizzazione deve avere tutte le funzionalità attivate.

Questa è l'impostazione predefinita per AWS Organizations. Se non è attivata, vedi Attivazione di tutte le funzionalità nell'organizzazione.

Autorizzazioni necessarie per designare un amministratore delegato

È necessario disporre dell'autorizzazione per attivare Amazon Inspector e designare un amministratore delegato di Amazon Inspector.

Aggiungi la seguente dichiarazione alla fine di una policy IAM per concedere queste autorizzazioni.

```
{
    "Sid": "PermissionsForInspectorAdmin",
    "Effect": "Allow",
    "Action": [
        "inspector2:EnableDelegatedAdminAccount",
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators",
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganizationalUnit",
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization"
    ],
    "Resource": "*"
}
```

Designazione di un amministratore delegato per l'organizzazione AWS

La procedura seguente mostra come designare un amministratore delegato per l'organizzazione. AWS Una volta completata questa designazione, Amazon Inspector viene attivato sia per l'account di gestione Organizations che per l'account amministratore delegato scelto.

> **Note**
>
> Solo l'account di gestione Organizations può designare un amministratore delegato.

La prima attivazione di Amazon Inspector crea il ruolo collegato al servizio (`AWSServiceRoleForAmazonInspectorSLR`) per l'account. Per ulteriori informazioni su come Amazon Inspector utilizza i ruoli collegati ai servizi, consulta. Utilizzo di ruoli collegati ai servizi per Amazon Inspector Per informazioni sui ruoli collegati ai servizi in generale, consulta Using service-linked roles nella IAM User Guide.

Per designare un amministratore delegato per Amazon Inspector

Console

Designare un amministratore delegato nella console

1. Accedi all'account di gestione AWS Management Console utilizzando l'account di AWS Organizations gestione.
2. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home, quindi utilizza il Regione AWS selettore in alto a destra per specificare la regione in cui desideri designare un amministratore.
3. Nel riquadro Amministratore delegato, inserisci l'ID account a dodici cifre dell'account Account AWS che desideri designare come amministratore delegato di Amazon Inspector per la tua organizzazione. Quindi scegli Amministrazione delegata.
4. (Consigliato) Ripeti i passaggi precedenti per ciascuno Regione AWS di essi.

API

Designare un amministratore delegato utilizzando l'API

- Esegui l'operazione EnableDelegatedAdminAccountAPI utilizzando le credenziali dell'account Account AWS di gestione Organizations. Puoi anche usare AWS Command Line Interface per farlo eseguendo il seguente comando CLI:. `aws inspector2 enable-delegated-admin-account --delegated-admin-account-id 11111111111`

  > **Note**
  >
  > Assicurati di specificare l'ID dell'account che desideri rendere amministratore delegato di Amazon Inspector.

Dopo aver specificato l'amministratore delegato, devi utilizzare l'account di AWS Organizations gestione solo per modificare o rimuovere l'account amministratore delegato.

Attivazione delle scansioni Amazon Inspector per gli account dei membri

In qualità di amministratore delegato della tua organizzazione, puoi attivare la scansione Amazon EC2, la scansione Amazon ECR o entrambe per qualsiasi membro associato AWS Organizations

all'account di gestione. Quando attivi le scansioni per un account membro, tale account viene associato all'amministratore delegato, Amazon Inspector viene attivato automaticamente e le scansioni del tipo scelto vengono avviate immediatamente. Per informazioni su quali risorse possono essere scansionate e su come configurare le scansioni, consulta. Scansione automatizzata delle risorse con Amazon Inspector

Amazon Inspector offre diverse opzioni per la gestione e l'attivazione delle scansioni per gli account dei membri, inclusa l'attivazione di Amazon Inspector. Utilizza una delle seguenti opzioni per avviare le scansioni dei tuoi account membri.

Per attivare automaticamente la scansione di tutti gli account dei membri

1. Accedi all'account amministratore delegato.
2. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home. Utilizza quindi il Regione AWS selettore in alto a destra per specificare la regione in cui desideri attivare la scansione di tutti gli account membri.
3. Nel pannello di navigazione, in Impostazioni, scegli Gestione account. La tabella degli account mostra tutti gli account dei membri associati all'account AWS Organizations di gestione.
4. Seleziona la casella di controllo nella parte superiore della tabella per selezionare tutti gli account in questa pagina. Quindi scegli Attiva e seleziona l'opzione del tipo di scansione preferito dal menu.

   > **Note**
   >
   > Vengono selezionati solo gli account attualmente visibili nella pagina. Se hai più pagine di account, devi ripetere questa procedura su ogni pagina. Per modificare il numero di account visualizzati nella pagina, seleziona l'icona a forma di ingranaggio.

5. Attiva l'impostazione Attiva automaticamente Inspector per gli account dei nuovi membri, quindi seleziona i tipi di scansione per attivare tutti i nuovi membri aggiunti alla tua organizzazione.
6. (Consigliato) Ripeti questi passaggi in ogni regione in cui desideri scansionare gli account dei membri.

L'impostazione Attiva automaticamente Inspector per gli account dei nuovi membri attiva Amazon Inspector per tutti i futuri membri della tua organizzazione. Ciò consente all'amministratore delegato di Amazon Inspector di gestire tutti i nuovi membri aggiunti all'organizzazione. Quando il numero di account membri raggiunge la quota di 5.000, questa impostazione viene disattivata automaticamente.

Se un account viene rimosso e il numero totale di membri scende a meno di 5.000, l'impostazione viene riattivata automaticamente.

Per attivare selettivamente gli account dei membri

1. Accedi all'account amministratore delegato.
2. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home, quindi utilizza il Regione AWS selettore in alto a destra per specificare la regione in cui desideri attivare la scansione per determinati account membro.
3. Nel pannello di navigazione, in Impostazioni, scegli Gestione account. La tabella degli account mostra tutti gli account dei membri associati all'account AWS Organizations di gestione.
4. Nella pagina Gestione dell'account, seleziona la casella di controllo per ogni account membro per cui desideri attivare la scansione.
5. Seleziona Attiva.
6. Dal menu Attiva, scegli i tipi di scansione da attivare per gli account selezionati. È possibile scegliere tra le seguenti opzioni di scansione:
   - Tutte le scansioni: per attivare tutti i tipi di scansione.
   - Scansione EC2: per attivare le scansioni delle istanze Amazon EC2.
   - Scansione dei contenitori ECR: per attivare le scansioni delle immagini dei contenitori ECR.
   - AWS Lambda scansione standard: per attivare le scansioni delle funzioni Lambda.
7. (Consigliato) Ripeti questi passaggi in ogni regione in cui desideri attivare le scansioni per determinati membri.

Se il tuo account di AWS Organizations gestione ha delegato un amministratore per Amazon Inspector, puoi attivare il tuo account come membro e visualizzare i dettagli di scansione del tuo account.

Per attivare la scansione come account membro

1. Accedi al tuo account.
2. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home, quindi utilizza il Regione AWS selettore in alto a destra per specificare la regione in cui desideri attivare la scansione.
3. Nel pannello di navigazione, in Impostazioni, scegli Gestione account.

4. Nella pagina Gestione dell'account, seleziona la casella di controllo relativa al tuo account.
5. Dal menu Attiva, scegli i tipi di scansione da attivare. È possibile scegliere tra le seguenti opzioni di scansione:
   - Tutte le scansioni: per attivare tutti i tipi di scansione.
   - Scansione EC2: per attivare le scansioni delle istanze Amazon EC2.
   - Scansione dei contenitori ECR: per attivare le scansioni delle immagini dei contenitori ECR.
   - AWS Lambda scansione standard: per attivare le scansioni delle funzioni Lambda.
6. (Consigliato) Ripeti questi passaggi in ogni regione in cui desideri attivare le scansioni.

Dissociazione degli account dei membri in Amazon Inspector

La procedura seguente mostra come dissociare gli account dei membri. Gli account dei membri non associati rimangono nell' AWS Organizations organizzazione come account Amazon Inspector autonomi. L'amministratore delegato di Amazon Inspector non è più autorizzato ad attivare e gestire Amazon Inspector per questi account. Puoi aggiungere nuovamente account dissociati come membri in un secondo momento.

> **Note**
>
> La dissociazione di un account non disattiva le scansioni di Amazon Inspector per quell'account.

Console

Per dissociare gli account dei membri utilizzando la console

1. Accedere all'account amministratore delegato.
2. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home, quindi utilizza il Regione AWS selettore in alto a destra per specificare la regione in cui desideri dissociare uno o più account membro.
3. Nel pannello di navigazione, in Impostazioni, scegli Gestione account.
4. Nella pagina Gestione dell'account, seleziona la casella di controllo per ogni account da cui desideri dissociare.
5. Dal menu Azioni, scegli Dissocia account.

6. (Consigliato) Ripeti questi passaggi in ogni regione in cui desideri dissociare gli account.

API

Per dissociare gli account dei membri utilizzando l'API

Esegui l'operazione DisassociateMember API. Nella richiesta, fornisci gli ID dell'account da dissociare.

Rimozione di un amministratore delegato di Amazon Inspector

Se devi assegnare un nuovo amministratore delegato di Amazon Inspector, puoi rimuovere un amministratore delegato esistente come account di gestione. AWS Organizations

Quando rimuovi un amministratore delegato, Amazon Inspector non viene disattivato in quell'account o negli account dei membri dell'organizzazione. Gli account all'interno dell'organizzazione vengono convertiti in account autonomi e mantengono le impostazioni di scansione che avevano prima di essere gestiti da un amministratore delegato.

Per rimuovere l'amministratore delegato

1. Accedere all'account di gestione AWS Management Console utilizzando l'account AWS Organizations di gestione.
2. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home, quindi utilizza il Regione AWS selettore in alto a destra per specificare la regione in cui desideri rimuovere l'amministratore delegato.
3. Nel pannello di navigazione, in Impostazioni, scegli Gestione account.
4. Nella sezione Amministratore delegato, scegli Rimuovi, quindi conferma l'azione.
5. Ripeti questi passaggi in ogni regione in cui hai registrato questo amministratore delegato.

Quando aggiungi un nuovo amministratore delegato di Amazon Inspector, devi associare manualmente i membri dell'organizzazione al nuovo account amministratore. Utilizza i seguenti passaggi per associare i membri dell'organizzazione al nuovo account amministratore.

Per associare i membri a un nuovo amministratore delegato

1. Accedere all'account di amministratore delegato AWS Management Console utilizzando l'account amministratore delegato.

2. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home, quindi utilizza il Regione AWS selettore in alto a destra per specificare la regione in cui desideri associare i membri al nuovo amministratore delegato.
3. Nel pannello di navigazione, in Impostazioni, scegli Gestione account.
4. Seleziona tutti gli account elencati nella tua organizzazione utilizzando la casella di controllo in alto.
5. Dal menu Azioni, scegli Aggiungi membro.
6. Ripeti questi passaggi in ogni regione in cui desideri associare i membri al nuovo amministratore delegato.

Monitoraggio dell'utilizzo e dei costi in Amazon Inspector

Puoi utilizzare la console Amazon Inspector e le operazioni API per proiettare i costi mensili dell'utilizzo di Amazon Inspector nel tuo ambiente. Se sei l'amministratore di Amazon Inspector per un ambiente con più account, puoi visualizzare il costo totale per l'intero ambiente e le metriche di costo per ciascuno dei tuoi account membro.

Utilizzo della console di utilizzo

Puoi valutare l'utilizzo e il costo previsto per Amazon Inspector dalla console.

Per accedere alle statistiche di utilizzo

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, seleziona la regione in cui desideri monitorare i costi.
3. Nel riquadro di navigazione, scegli Utilizzo.

Nella scheda Per account vedrai il costo totale previsto in base al periodo di 30 giorni elencato nella sezione Utilizzo dell'account. Nella tabella sotto la colonna Costo previsto, seleziona un valore per visualizzare una suddivisione dell'utilizzo per tipo di scansione per quell'account. In questo riquadro dei dettagli puoi anche vedere per quali tipi di scansione è attiva una versione di prova gratuita per quell'account.

Se sei l'amministratore delegato di un'organizzazione, vedrai una riga nella tabella per ogni account all'interno dell'organizzazione. Se un account dell'organizzazione non è associato, la console mostra il costo previsto come -.

Nella scheda Per tipo di scansione è possibile visualizzare una suddivisione dell'utilizzo effettivo finora nell'attuale periodo di 30 giorni per tipo di scansione. Queste sono le informazioni utilizzate per calcolare i costi previsti nella scheda Per account.

Se sei l'amministratore delegato di un'organizzazione, puoi vedere l'utilizzo per ogni account dell'organizzazione.

In questa scheda, puoi espandere uno dei seguenti riquadri per le statistiche di utilizzo:

Scansione Amazon EC2

La console di utilizzo di Amazon Inspector tiene traccia delle seguenti metriche per la scansione basata su agenti e la scansione senza agente:

- Istanze (media): Amazon Inspector utilizza le ore di copertura per calcolare il numero medio di risorse per la scansione delle istanze EC2. La media è il totale delle ore di copertura divise per 720 ore (il numero di ore in un periodo di 30 giorni).
- Ore di copertura: per la scansione di Amazon EC2 si tratta del numero totale di ore negli ultimi 30 giorni in cui Amazon Inspector ha fornito copertura attiva per ogni istanza EC2 in un account. Per le istanze EC2, le ore di copertura sono le ore che intercorrono tra il momento in cui Amazon Inspector ha scoperto l'istanza fino alla sua chiusura o arresto o all'esclusione dalle scansioni tramite tag. (quando riavvii un'istanza interrotta o rimuovi un tag di esclusione, Amazon Inspector riprende la copertura e le ore di copertura per quell'istanza continueranno ad accumularsi).

Scansioni delle istanze CIS: il numero totale di scansioni CIS eseguite per le istanze dell'account.

Scansione Amazon ECR

Scansioni iniziali: il totale delle prime scansioni delle immagini nell'account negli ultimi 30 giorni.

Scansioni ripetute: la somma totale delle scansioni ripetute delle immagini nell'account negli ultimi 30 giorni. Una nuova scansione è qualsiasi scansione eseguita su un'immagine ECR precedentemente scansionata da Amazon Inspector. Se hai configurato il tuo repository ECR per la scansione continua, le scansioni vengono eseguite automaticamente quando Amazon Inspector aggiunge un nuovo Common Vulnerabilities and Exposures (CVE) al database.

Scansione Lambda

La console di utilizzo di Amazon Inspector tiene traccia delle seguenti metriche per la scansione standard Lambda e la scansione del codice Lambda:

- Numero di funzioni Lambda (media): Amazon Inspector utilizza le ore di copertura per calcolare il numero medio di funzioni per la scansione della funzione Lambda. La media è il totale delle ore di copertura diviso per 720 ore (il numero di ore in un periodo di 30 giorni).
- Ore di copertura: per la scansione della funzione Lambda, si tratta del numero totale di ore negli ultimi 30 giorni in cui Amazon Amazon Inspector ha fornito la copertura attiva per ogni funzione Lambda in un account. Per quanto riguarda AWS Lambda le funzioni, le ore di copertura vengono calcolate dal momento in cui Amazon Inspector rileva una funzione fino a quando

questa viene eliminata o esclusa dalle scansioni. Se una funzione esclusa viene nuovamente inclusa, le ore di copertura per quella funzione continueranno a maturare.

Scopri come Amazon Inspector calcola i costi di utilizzo

I costi forniti da Amazon Inspector sono stime, non costi effettivi, pertanto possono differire da quelli indicati nella tua AWS Billing console.

Tieni presente quanto segue su come Amazon Inspector calcola i costi nella pagina Utilizzo:

- Il costo di utilizzo riflette solo la regione corrente. I prezzi per tipo di scansione variano in base alla AWS regione, per verificare i prezzi esatti per regione, consulta la pagina Prezzi di Amazon Inspector
- Tutte le proiezioni di utilizzo sono arrotondate al dollaro USA più vicino.
- Gli sconti non sono inclusi nei costi previsti.
- Il costo previsto rappresenta il costo totale per il periodo di utilizzo di 30 giorni per tipo di scansione. Se un account è stato utilizzato per meno di 30 giorni, Amazon Inspector prevede il costo dopo 30 giorni come se le risorse attualmente coperte restassero coperte per il resto del periodo di 30 giorni.
- Il costo per tipo di scansione viene calcolato in base a quanto segue:
  - Scansione EC2: il costo riflette il numero medio di istanze EC2 coperte da Amazon Inspector negli ultimi 30 giorni.
  - Scansione dei contenitori ECR: il costo riflette la somma del numero di scansioni iniziali e scansioni di immagini ripetute negli ultimi 30 giorni.
  - Scansione standard Lambda: il costo riflette il numero medio di funzioni Lambda coperte da Amazon Inspector negli ultimi 30 giorni.
  - Scansione del codice Lambda: il costo riflette il numero medio di funzioni Lambda coperte da Amazon Inspector negli ultimi 30 giorni.

Informazioni sulla versione di prova gratuita di Amazon Inspector

Quando attivi un tipo di scansione Amazon Inspector, ti iscrivi automaticamente a una prova gratuita di 15 giorni per quel tipo di scansione. Ogni tipo di scansione ha una traccia gratuita indipendente, che include: scansione EC2, scansione ECR, scansione standard Lambda e scansione codice Lambda.

> **Note**
>
> La versione di prova gratuita non si applica alla scansione CIS.

Se si disattiva un tipo di scansione durante la prova gratuita, la versione di prova gratuita verrà messa in pausa per quel tipo di scansione. Se riattivi quel servizio, la prova gratuita riprenderà e avrai a disposizione i giorni rimanenti di tale prova gratuita.

Sicurezza in Amazon Inspector

La sicurezza del cloud AWS è la massima priorità. In qualità di AWS cliente, puoi beneficiare di data center e architetture di rete progettati per soddisfare i requisiti delle organizzazioni più sensibili alla sicurezza.

La sicurezza è una responsabilità condivisa tra te e te. AWS Il modello di responsabilità condivisa descrive questo aspetto come sicurezza del cloud e sicurezza nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che gestisce AWS i servizi in Cloud AWS. AWS fornisce inoltre servizi che è possibile utilizzare in modo sicuro. I revisori esterni testano e verificano regolarmente l'efficacia della nostra sicurezza nell'ambito dei AWS Programmi di AWS conformità dei Programmi di conformità dei di . Per ulteriori informazioni sui programmi di conformità applicabili ad Amazon Inspector, consulta AWS Services in Scope by Compliance Program Program.
- Sicurezza nel cloud: la tua responsabilità è determinata dal AWS servizio che utilizzi. Sei anche responsabile di altri fattori, tra cui la riservatezza dei dati, i requisiti della tua azienda e le leggi e normative vigenti.

Questa documentazione ti aiuta a capire come applicare il modello di responsabilità condivisa quando usi Amazon Inspector. I seguenti argomenti mostrano come configurare Amazon Inspector per soddisfare i tuoi obiettivi di sicurezza e conformità. Scopri anche come utilizzare altri AWS servizi che ti aiutano a monitorare e proteggere le tue risorse Amazon Inspector.

Argomenti

Protezione dei dati in Amazon Inspector

Il modello di responsabilità AWS condivisa Modello si applica alla protezione dei dati in Amazon Inspector. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura globale che gestisce tutti i Cloud AWS. L'utente è responsabile del controllo dei contenuti ospitati su questa infrastruttura. L'utente è inoltre responsabile della configurazione della protezione e delle attività di gestione per i Servizi AWS utilizzati. Per ulteriori informazioni sulla privacy dei dati, vedi le Domande frequenti sulla privacy dei dati. Per informazioni sulla protezione dei dati in Europa, consulta il post del blog relativo al Modello di responsabilità condivisa AWS e GDPR nel Blog sulla sicurezza AWS .

Ai fini della protezione dei dati, consigliamo di proteggere Account AWS le credenziali e configurare i singoli utenti con AWS IAM Identity Center or AWS Identity and Access Management (IAM). In tal modo, a ogni utente verranno assegnate solo le autorizzazioni necessarie per svolgere i suoi compiti. Ti suggeriamo, inoltre, di proteggere i dati nei seguenti modi:

- Utilizza l'autenticazione a più fattori (MFA) con ogni account.
- Usa SSL/TLS per comunicare con le risorse. AWS È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con. AWS CloudTrail
- Utilizza soluzioni di AWS crittografia, insieme a tutti i controlli di sicurezza predefiniti all'interno Servizi AWS.
- Utilizza i servizi di sicurezza gestiti avanzati, come Amazon Macie, che aiutano a individuare e proteggere i dati sensibili archiviati in Amazon S3.
- Se hai bisogno di moduli crittografici convalidati FIPS 140-2 per l'accesso AWS tramite un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-2.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Ciò include quando lavori con Amazon Inspector o altri utenti Servizi AWS utilizzando la console, l'API o AWS gli AWS CLI SDK. I dati inseriti nei tag o nei campi di testo in formato libero utilizzati per i nomi possono essere utilizzati per i la fatturazione o i log di diagnostica. Quando fornisci un URL a un server esterno, ti suggeriamo vivamente di non includere informazioni sulle credenziali nell'URL per convalidare la tua richiesta al server.

Argomenti

Crittografia dei dati a riposo

Amazon Inspector archivia in modo sicuro i dati inattivi utilizzando soluzioni di AWS crittografia predefinite. Amazon Inspector crittografa i dati, come l'inventario delle risorse raccolto utilizzando AWS Systems Manager, l'inventario delle risorse analizzato dalle immagini di Amazon ECR e i risultati di sicurezza generati, AWS utilizzando chiavi AWS di crittografia di proprietà di Key Management Service ().AWS KMS Non puoi visualizzare, gestire o utilizzare chiavi di AWS proprietà o verificarne l'utilizzo. Tuttavia, non è necessario intraprendere alcuna azione o modificare alcun programma per proteggere le chiavi che crittografano i dati. Per ulteriori informazioni, consulta le chiavi AWS possedute.

Se disabiliti Amazon Inspector, elimina definitivamente tutte le risorse che archivia o gestisce per te, come l'inventario raccolto e i risultati di sicurezza.

Crittografia inattiva per il codice contenuto nei tuoi risultati

Per la scansione del codice Amazon Inspector Lambda, Amazon Inspector collabora con Amazon Inspector per scansionare il codice CodeGuru alla ricerca di vulnerabilità. Quando viene rilevata una vulnerabilità, CodeGuru estrae un frammento di codice contenente la vulnerabilità e lo archivia fino a quando Amazon Inspector non richiede l'accesso. Per impostazione predefinita, CodeGuru utilizza una chiave AWS proprietaria per crittografare il codice estratto, tuttavia, puoi configurare Amazon Inspector in modo che utilizzi la tua chiave AWS KMS gestita dal cliente per la crittografia.

Il seguente flusso di lavoro spiega come Amazon Inspector utilizza la chiave configurata per crittografare il codice:

1. Fornisci una AWS KMS chiave ad Amazon Inspector utilizzando l'API Amazon UpdateEncryptionKeyInspector.
2. Amazon Inspector inoltra le informazioni sulla tua AWS KMS chiave a. CodeGuru CodeGuru memorizza le informazioni per usi futuri.
3. CodeGuru richiede un modulo di concessione AWS KMS per la chiave configurata in Amazon Inspector.
4. CodeGuru crea una chiave di dati crittografata a partire dalla tua AWS KMS chiave e la archivia. Questa chiave dati viene utilizzata per crittografare i dati del codice memorizzati da CodeGuru.

5. Ogni volta che Amazon Inspector richiede dati da scansioni di codice CodeGuru utilizza la concessione per decrittografare la chiave dati crittografata, quindi utilizza quella chiave per decrittografare i dati in modo che possano essere recuperati.

Quando disabiliti la scansione del codice Lambda CodeGuru ritira la concessione ed elimina la chiave dati associata.

Autorizzazioni per la crittografia del codice con una chiave gestita dal cliente

Per utilizzare la crittografia è necessario disporre di una politica che consenta l'accesso alle AWS KMS azioni, nonché di una dichiarazione che conceda Amazon Inspector CodeGuru e le autorizzazioni per utilizzare tali azioni tramite chiavi di condizione.

Se stai impostando, aggiornando o reimpostando la chiave di crittografia per il tuo account, dovrai utilizzare una politica di amministrazione di Amazon Inspector, ad esempio. AWS politica gestita: AmazonInspector2FullAccess Dovrai inoltre concedere le seguenti autorizzazioni agli utenti di sola lettura che devono recuperare frammenti di codice dai risultati o dai dati relativi alla chiave scelta per la crittografia.

Per KMS, la politica deve consentire di eseguire le seguenti azioni:

- `kms:CreateGrant`
- `kms:Decrypt`
- `kms:DescribeKey`
- `kms:GenerateDataKeyWithoutPlainText`
- `kms:Encrypt`
- `kms:RetireGrant`

Dopo aver verificato di disporre delle AWS KMS autorizzazioni corrette nella tua politica, devi allegare una dichiarazione che consenta ad Amazon Inspector CodeGuru e di utilizzare la tua chiave per la crittografia. Allega la seguente dichiarazione sulla politica:

> **Note**
>
> Sostituisci la regione con la AWS regione in cui è abilitata la scansione del codice Amazon Inspector Lambda.

```
{
            "Sid": "allow CodeGuru Security to request a grant for a AWS KMS key",
          "Effect": "Allow",
          "Action": "kms:CreateGrant",
          "Resource": "*",
          "Condition": {
           "ForAllValues:StringEquals": {
            "kms:GrantOperations": [
             "GenerateDataKey",
             "GenerateDataKeyWithoutPlaintext",
             "Encrypt",
             "Decrypt",
             "RetireGrant",
             "DescribeKey"
            ]
           },
           "StringEquals": {
            "kms:ViaService": [
             "codeguru-security.Region.amazonaws.com"
            ]
           }
          }
         },
         {
          "Sid": "allow Amazon Inspector and CodeGuru Security to use your AWS KMS key",
          "Effect": "Allow",
          "Action": [
           "kms:Encrypt",
           "kms:Decrypt",
           "kms:RetireGrant",
           "kms:DescribeKey",
           "kms:GenerateDataKeyWithoutPlaintext"
          ],
          "Resource": "*",
          "Condition": {
           "StringEquals": {
            "kms:ViaService": [
             "inspector2.Region.amazonaws.com",
             "codeguru-security.Region.amazonaws.com"
            ]
           }
          }
```

```
        }
```

> **Note**
>
> Quando aggiungi l'istruzione, assicurati che la sintassi sia valida. Le politiche utilizzano il formato JSON. Ciò significa che è necessario aggiungere una virgola prima o dopo l'istruzione, a seconda di dove si aggiunge l'istruzione alla politica. Se aggiungete l'istruzione come ultima istruzione, aggiungete una virgola dopo la parentesi di chiusura dell'istruzione precedente. Se la aggiungete come prima istruzione o tra due istruzioni esistenti, aggiungete una virgola dopo la parentesi che chiude l'istruzione.

Configurazione della crittografia con una chiave gestita dal cliente

Per configurare la crittografia per il tuo account utilizzando una chiave gestita dal cliente, devi essere un amministratore di Amazon Inspector con le autorizzazioni descritte in. Autorizzazioni per la crittografia del codice con una chiave gestita dal cliente Inoltre, avrai bisogno di una AWS KMS chiave nella stessa AWS regione dei risultati o di una chiave multiregionale. Puoi utilizzare una chiave simmetrica esistente nel tuo account o creare una chiave simmetrica gestita dal cliente utilizzando la console di AWS gestione o le API. AWS KMS Per ulteriori informazioni, consulta Creazione di chiavi di crittografia simmetriche nella guida per l'utente. AWS KMS AWS KMS

Utilizzo dell'API Amazon Inspector per configurare la crittografia

Per impostare una chiave per la crittografia, il UpdateEncryptionKeyfunzionamento dell'API Amazon Inspector dopo aver effettuato l'accesso come amministratore di Amazon Inspector. Nella richiesta API, utilizza il `kmsKeyId` campo per specificare l'ARN della AWS KMS chiave che desideri utilizzare. Per `scanType` entrare `CODE` e per `resourceType` entrare`AWS_LAMBDA_FUNCTION`.

Puoi utilizzare l'UpdateEncryptionKeyAPI per verificare la visualizzazione della AWS KMS chiave utilizzata da Amazon Inspector per la crittografia.

> **Note**
>
> Se tenti di utilizzare `GetEncryptionKey` quando non hai impostato una chiave gestita dal cliente, l'operazione restituisce un `ResourceNotFoundException` errore, il che significa che per la crittografia viene utilizzata una chiave di AWS proprietà.

Se elimini la chiave o modifichi la sua politica per negare l'accesso ad Amazon Inspector CodeGuru , non sarai in grado di accedere ai risultati delle vulnerabilità del codice e la scansione del codice Lambda non riuscirà per il tuo account.

Puoi utilizzare `ResetEncryptionKey` per riprendere a utilizzare una chiave AWS proprietaria per crittografare il codice estratto come parte dei risultati di Amazon Inspector.

Crittografia in transito

AWS crittografa tutti i dati in transito tra sistemi AWS interni e altri servizi. AWS

Per la raccolta dell'inventario, Systems Manager raccoglie i dati di telemetria dalle istanze EC2 di proprietà del cliente e li invia AWS tramite un canale protetto da Transport Layer Security (TLS) per la valutazione. Vedi Data Protection in Systems Manager per capire come SSM crittografa i dati in transito.

Allo stesso modo, i risultati delle scansioni delle funzioni Amazon ECR e AWS Lambda inviati a Security Hub vengono crittografati utilizzando un canale protetto da TLS.

Identity and Access Management per Amazon Inspector

AWS Identity and Access Management (IAM) è uno strumento Servizio AWS che aiuta un amministratore a controllare in modo sicuro l'accesso alle risorse. AWS Gli amministratori IAM controllano chi può essere autenticato (effettuare l'accesso) e autorizzato (disporre delle autorizzazioni) a utilizzare le risorse Amazon Inspector. IAM è uno strumento Servizio AWS che puoi utilizzare senza costi aggiuntivi.

Argomenti

- Destinatari
- Autenticazione con identità
- Gestione dell'accesso con policy
- Come funziona Amazon Inspector con IAM
- Esempi di policy basate sull'identità per Amazon Inspector
- AWS politiche gestite per Amazon Inspector
- Utilizzo di ruoli collegati ai servizi per Amazon Inspector

- Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Inspector

Destinatari

Il modo in cui utilizzi AWS Identity and Access Management (IAM) varia a seconda del lavoro svolto in Amazon Inspector.

Utente del servizio: se utilizzi il servizio Amazon Inspector per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. Man mano che utilizzi più funzionalità di Amazon Inspector per svolgere il tuo lavoro, potresti aver bisogno di autorizzazioni aggiuntive. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di Amazon Inspector, consulta. Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Inspector

Amministratore del servizio: se sei responsabile delle risorse di Amazon Inspector presso la tua azienda, probabilmente hai pieno accesso ad Amazon Inspector. È tuo compito determinare a quali funzionalità e risorse di Amazon Inspector devono accedere gli utenti del servizio. Devi inviare le richieste all'amministratore IAM per cambiare le autorizzazioni degli utenti del servizio. Esamina le informazioni contenute in questa pagina per comprendere i concetti di base relativi a IAM. Per ulteriori informazioni su come la tua azienda può utilizzare IAM con Amazon Inspector, consulta. Come funziona Amazon Inspector con IAM

Amministratore IAM: se sei un amministratore IAM, potresti voler saperne di più su come scrivere policy per gestire l'accesso ad Amazon Inspector. Per visualizzare esempi di policy basate sull'identità di Amazon Inspector che puoi utilizzare in IAM, consulta. Esempi di policy basate sull'identità per Amazon Inspector

Autenticazione con identità

L'autenticazione è il modo in cui accedi AWS utilizzando le tue credenziali di identità. Devi essere autenticato (aver effettuato l' Utente root dell'account AWS accesso AWS) come utente IAM o assumendo un ruolo IAM.

Puoi accedere AWS come identità federata utilizzando le credenziali fornite tramite una fonte di identità. AWS IAM Identity Center Gli utenti (IAM Identity Center), l'autenticazione Single Sign-On della tua azienda e le tue credenziali di Google o Facebook sono esempi di identità federate. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Quando accedi AWS utilizzando la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere al AWS Management Console o al portale di AWS accesso. Per ulteriori informazioni sull'accesso a AWS, vedi Come accedere al tuo Account AWS nella Guida per l'Accedi ad AWS utente.

Se accedi a AWS livello di codice, AWS fornisce un kit di sviluppo software (SDK) e un'interfaccia a riga di comando (CLI) per firmare crittograficamente le tue richieste utilizzando le tue credenziali. Se non utilizzi AWS strumenti, devi firmare tu stesso le richieste. Per ulteriori informazioni sull'utilizzo del metodo consigliato per firmare autonomamente le richieste, consulta Signing AWS API request nella IAM User Guide.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. Ad esempio, ti AWS consiglia di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza del tuo account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Center e Utilizzo dell'autenticazione a più fattori (MFA) in AWS nella Guida per l'utente di IAM.

Account AWS utente root

Quando si crea un account Account AWS, si inizia con un'identità di accesso che ha accesso completo a tutte Servizi AWS le risorse dell'account. Questa identità è denominata utente Account AWS root ed è accessibile effettuando l'accesso con l'indirizzo e-mail e la password utilizzati per creare l'account. Si consiglia vivamente di non utilizzare l'utente root per le attività quotidiane. Conservare le credenziali dell'utente root e utilizzarle per eseguire le operazioni che solo l'utente root può eseguire. Per un elenco completo delle attività che richiedono l'accesso come utente root, consulta la sezione Attività che richiedono le credenziali dell'utente root nella Guida per l'utente di IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, un provider di identità Web AWS Directory Service, la directory Identity Center o qualsiasi utente che accede Servizi AWS utilizzando credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di

utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni sul Centro identità IAM, consulta Cos'è Centro identità IAM? nella Guida per l'utente di AWS IAM Identity Center .

Utenti e gruppi IAM

Un utente IAM è un'identità interna Account AWS che dispone di autorizzazioni specifiche per una singola persona o applicazione. Ove possibile, consigliamo di fare affidamento a credenziali temporanee invece di creare utenti IAM con credenziali a lungo termine come le password e le chiavi di accesso. Tuttavia, per casi d'uso specifici che richiedono credenziali a lungo termine con utenti IAM, si consiglia di ruotare le chiavi di accesso. Per ulteriori informazioni, consulta la pagina Rotazione periodica delle chiavi di accesso per casi d'uso che richiedono credenziali a lungo termine nella Guida per l'utente di IAM.

Un gruppo IAM è un'identità che specifica un insieme di utenti IAM. Non è possibile eseguire l'accesso come gruppo. È possibile utilizzare gruppi per specificare le autorizzazioni per più utenti alla volta. I gruppi semplificano la gestione delle autorizzazioni per set di utenti di grandi dimensioni. Ad esempio, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente di IAM.

Ruoli IAM

Un ruolo IAM è un'identità interna all'utente Account AWS che dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. Puoi assumere temporaneamente un ruolo IAM in AWS Management Console cambiando ruolo. Puoi assumere un ruolo chiamando un'operazione AWS CLI o AWS API o utilizzando un URL personalizzato. Per ulteriori informazioni sui metodi per l'utilizzo dei ruoli, consulta Utilizzo di ruoli IAM nella Guida per l'utente di IAM.

I ruoli IAM con credenziali temporanee sono utili nelle seguenti situazioni:

- Accesso utente federato: per assegnare le autorizzazioni a una identità federata, è possibile creare un ruolo e definire le autorizzazioni per il ruolo. Quando un'identità federata viene

autenticata, l'identità viene associata al ruolo e ottiene le autorizzazioni da esso definite. Per ulteriori informazioni sulla federazione dei ruoli, consulta Creazione di un ruolo per un provider di identità di terza parte nella Guida per l'utente di IAM. Se utilizzi IAM Identity Center, configura un set di autorizzazioni. IAM Identity Center mette in correlazione il set di autorizzazioni con un ruolo in IAM per controllare a cosa possono accedere le identità dopo l'autenticazione. Per ulteriori informazioni sui set di autorizzazioni, consulta Set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

- Autorizzazioni utente IAM temporanee: un utente IAM o un ruolo può assumere un ruolo IAM per ottenere temporaneamente autorizzazioni diverse per un'attività specifica.
- Accesso multi-account: è possibile utilizzare un ruolo IAM per permettere a un utente (un principale affidabile) con un account diverso di accedere alle risorse nell'account. I ruoli sono lo strumento principale per concedere l'accesso multi-account. Tuttavia, con alcuni Servizi AWS, è possibile allegare una policy direttamente a una risorsa (anziché utilizzare un ruolo come proxy). Per informazioni sulle differenze tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.
- Accesso a più servizi: alcuni Servizi AWS utilizzano le funzionalità di altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.
  - Sessioni di accesso diretto (FAS): quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, combinate con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
  - Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.
  - Ruolo collegato al servizio: un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I

ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

- Applicazioni in esecuzione su Amazon EC2: puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che AWS CLI effettuano richieste API. AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente di IAM.

Gestione dell'accesso con policy

Puoi controllare l'accesso AWS creando policy e collegandole a AWS identità o risorse. Una policy è un oggetto AWS che, se associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWS valuta queste politiche quando un principale (utente, utente root o sessione di ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle politiche viene archiviata AWS come documenti JSON. Per ulteriori informazioni sulla struttura e sui contenuti dei documenti delle policy JSON, consulta Panoramica delle policy JSON nella Guida per l'utente di IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. Successivamente l'amministratore può aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Le policy IAM definiscono le autorizzazioni relative a un'azione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'azione `iam:GetRole`. Un utente con tale policy può ottenere informazioni sul ruolo dall' AWS Management Console AWS CLI, dall'o dall' AWS API.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruoli IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Le policy basate su identità possono essere ulteriormente classificate come policy inline o policy gestite. Le policy inline sono integrate direttamente in un singolo utente, gruppo o ruolo. Le politiche gestite sono politiche autonome che puoi allegare a più utenti, gruppi e ruoli nel tuo Account AWS. Le politiche gestite includono politiche AWS gestite e politiche gestite dai clienti. Per informazioni su come scegliere tra una policy gestita o una policy inline, consulta Scelta fra policy gestite e policy inline nella Guida per l'utente di IAM.

Policy basate su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non puoi utilizzare le policy AWS gestite di IAM in una policy basata sulle risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano gli ACL. AWS WAF Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta tipi di policy aggiuntivi e meno comuni. Questi tipi di policy possono impostare il numero massimo di autorizzazioni concesse dai tipi di policy più comuni.

- Limiti delle autorizzazioni: un limite delle autorizzazioni è una funzione avanzata nella quale si imposta il numero massimo di autorizzazioni che una policy basata su identità può concedere a un'entità IAM (utente o ruolo IAM). È possibile impostare un limite delle autorizzazioni per un'entità. Le autorizzazioni risultanti sono l'intersezione delle policy basate su identità dell'entità e i relativi limiti delle autorizzazioni. Le policy basate su risorse che specificano l'utente o il ruolo nel campo `Principal` sono condizionate dal limite delle autorizzazioni. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni sui limiti delle autorizzazioni, consulta Limiti delle autorizzazioni per le entità IAM nella Guida per l'utente di IAM.
- Politiche di controllo dei servizi (SCP): le SCP sono politiche JSON che specificano le autorizzazioni massime per un'organizzazione o un'unità organizzativa (OU) in. AWS Organizations AWS Organizations è un servizio per il raggruppamento e la gestione centralizzata di più Account AWS di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità negli account dei membri, inclusa ciascuna. Utente root dell'account AWS Per ulteriori informazioni su organizzazioni e policy SCP, consulta la pagina sulle Policy di controllo dei servizi nella Guida per l'utente di AWS Organizations .
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente di IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per scoprire come si AWS determina se consentire una richiesta quando sono coinvolti più tipi di policy, consulta Logica di valutazione delle policy nella IAM User Guide.

Come funziona Amazon Inspector con IAM

Prima di utilizzare IAM per gestire l'accesso ad Amazon Inspector, scopri quali funzionalità IAM sono disponibili per l'uso con Amazon Inspector.

Funzionalità IAM che puoi utilizzare con Amazon Inspector

Funzionalità IAM	Supporto per Amazon Inspector
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione della policy (specifica del servizio)	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	No
Ruoli collegati al servizio	Sì

Per avere una panoramica generale del funzionamento di Amazon Inspector e Servizi AWS altri con la maggior parte delle funzionalità IAM, Servizi AWS consulta la sezione dedicata alla compatibilità con IAM nella IAM User Guide.

Politiche basate sull'identità per Amazon Inspector

Supporta le policy basate su identità	Sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Con le policy basate su identità di IAM, è possibile specificare quali operazioni e risorse sono consentite o respinte, nonché le condizioni in base alle quali le operazioni sono consentite o respinte. Non è possibile specificare l'entità principale in una policy basata sull'identità perché si applica all'utente o al ruolo a cui è associato. Per informazioni su tutti gli elementi utilizzabili in una policy JSON, consulta Guida di riferimento agli elementi delle policy JSON IAM nella Guida per l'utente di IAM.

Esempi di policy basate sull'identità per Amazon Inspector

Per visualizzare esempi di politiche basate sull'identità di Amazon Inspector, consulta. Esempi di policy basate sull'identità per Amazon Inspector

Politiche basate sulle risorse all'interno di Amazon Inspector

Supporta le policy basate su risorse	No

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarle per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o. Servizi AWS

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando il principale e la risorsa sono diversi Account AWS, un amministratore IAM dell'account affidabile deve inoltre concedere all'entità principale (utente o ruolo) l'autorizzazione ad accedere alla risorsa. L'autorizzazione viene concessa collegando all'entità una policy basata sull'identità. Tuttavia, se una policy basata su risorse concede l'accesso a un principale nello stesso account, non sono richieste

ulteriori policy basate su identità. Per ulteriori informazioni, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente di IAM.

Azioni politiche per Amazon Inspector

Supporta le operazioni di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action` di una policy JSON descrive le operazioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni politiche in genere hanno lo stesso nome dell'operazione AWS API associata. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per visualizzare un elenco delle azioni di Amazon Inspector, consulta Azioni definite da Amazon Inspector nel Service Authorization Reference.

Le azioni politiche in Amazon Inspector utilizzano il seguente prefisso prima dell'azione:

```
inspector2
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      "inspector2:action1",
      "inspector2:action2"
         ]
```

Per visualizzare esempi di politiche basate sull'identità di Amazon Inspector, consulta. Esempi di policy basate sull'identità per Amazon Inspector

Risorse relative alle policy per Amazon Inspector

Supporta le risorse di policy	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource` della policy specifica l'oggetto o gli oggetti ai quali si applica l'azione. Le istruzioni devono includere un elemento `Resource` o un elemento `NotResource`. Come best practice, specifica una risorsa utilizzando il suo nome della risorsa Amazon (ARN). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per visualizzare un elenco dei tipi di risorse di Amazon Inspector e dei relativi ARN, consulta Risorse definite da Amazon Inspector nel Service Authorization Reference. Per sapere con quali azioni puoi specificare l'ARN di ogni risorsa, consulta Azioni definite da Amazon Inspector.

Per visualizzare esempi di politiche basate sull'identità di Amazon Inspector, consulta. Esempi di policy basate sull'identità per Amazon Inspector

Chiavi relative alle condizioni delle politiche per Amazon Inspector

Supporta le chiavi di condizione delle policy specifiche del servizio	Sì

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition` (o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition` è facoltativo. Puoi compilare espressioni

condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition` in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWS utilizzando un'operazione `AND` logica. Se si specificano più valori per una singola chiave di condizione, AWS valuta la condizione utilizzando un'operazione logica. `OR` Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche del servizio. Per visualizzare tutte le chiavi di condizione AWS globali, consulta le chiavi di contesto delle condizioni AWS globali nella Guida per l'utente IAM.

Per visualizzare un elenco dei codici di condizione di Amazon Inspector, consulta Condition keys for Amazon Inspector nel Service Authorization Reference. Per sapere con quali azioni e risorse puoi utilizzare una chiave di condizione, consulta Azioni definite da Amazon Inspector.

Per visualizzare esempi di politiche basate sull'identità di Amazon Inspector, consulta. Esempi di policy basate sull'identità per Amazon Inspector

ACL in Amazon Inspector

Supporta le ACL	No

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni ad accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Amazon Inspector

Supporta ABAC (tag nelle policy)	Parziale

Il controllo dell'accesso basato su attributi (ABAC) è una strategia di autorizzazione che definisce le autorizzazioni in base agli attributi. In AWS, questi attributi sono chiamati tag. Puoi allegare tag a entità IAM (utenti o ruoli) e a molte AWS risorse. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente di IAM. Per visualizzare un tutorial con i passaggi per l'impostazione di ABAC, consulta Utilizzo del controllo degli accessi basato su attributi (ABAC) nella Guida per l'utente di IAM.

Utilizzo di credenziali temporanee con Amazon Inspector

Supporta le credenziali temporanee	Sì

Alcune Servizi AWS non funzionano quando accedi utilizzando credenziali temporanee. Per ulteriori informazioni, incluse quelle che Servizi AWS funzionano con credenziali temporanee, consulta la sezione relativa alla Servizi AWS compatibilità con IAM nella IAM User Guide.

Stai utilizzando credenziali temporanee se accedi AWS Management Console utilizzando qualsiasi metodo tranne nome utente e password. Ad esempio, quando accedi AWS utilizzando il link Single Sign-On (SSO) della tua azienda, tale processo crea automaticamente credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente di IAM.

È possibile creare manualmente credenziali temporanee utilizzando l'API or. AWS CLI AWS È quindi possibile utilizzare tali credenziali temporanee per accedere. AWS AWS consiglia di generare

dinamicamente credenziali temporanee anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni principali multiservizio per Amazon Inspector

Supporta l'inoltro delle sessioni di accesso (FAS)	Sì

Quando utilizzi un utente o un ruolo IAM per eseguire azioni AWS, sei considerato un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. FAS utilizza le autorizzazioni del principale che chiama an Servizio AWS, in combinazione con la richiesta Servizio AWS per effettuare richieste ai servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che richiede interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.

Ruoli di servizio per Amazon Inspector

Supporta i ruoli di servizio	No

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWS nella Guida per l'utente di IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe interrompere la funzionalità di Amazon Inspector. Modifica i ruoli di servizio solo quando Amazon Inspector fornisce indicazioni in tal senso.

Ruoli collegati ai servizi per Amazon Inspector

Supporta i ruoli collegati ai servizi	Sì

Un ruolo collegato al servizio è un tipo di ruolo di servizio collegato a un. Servizio AWS Il servizio può assumere il ruolo per eseguire un'operazione per tuo conto. I ruoli collegati al servizio vengono visualizzati nel tuo account Account AWS e sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per informazioni dettagliate sulla creazione o la gestione di ruoli collegati ai servizi, consulta Servizi AWS That work with IAM. Trova un servizio nella tabella che include un `Yes` nella colonna Service-linked role (Ruolo collegato ai servizi). Scegli il collegamento Sì per visualizzare la documentazione relativa al ruolo collegato ai servizi per tale servizio.

Esempi di policy basate sull'identità per Amazon Inspector

Per impostazione predefinita, gli utenti e i ruoli non sono autorizzati a creare o modificare risorse Amazon Inspector. Inoltre, non possono eseguire attività utilizzando AWS Management Console, AWS Command Line Interface (AWS CLI) o AWS API. Per concedere agli utenti l'autorizzazione a eseguire azioni sulle risorse di cui hanno bisogno, un amministratore IAM può creare policy IAM. L'amministratore può quindi aggiungere le policy IAM ai ruoli e gli utenti possono assumere i ruoli.

Per informazioni su come creare una policy basata su identità IAM utilizzando questi documenti di policy JSON di esempio, consulta Creazione di policy IAM nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Amazon Inspector, incluso il formato degli ARN per ciascun tipo di risorsa, consulta Azioni, risorse e chiavi di condizione per Amazon Inspector nel Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console Amazon Inspector
- Consentire agli utenti di visualizzare le loro autorizzazioni
- Consenti l'accesso in sola lettura a tutte le risorse Amazon Inspector
- Consenti l'accesso completo a tutte le risorse di Amazon Inspector

Best practice per le policy

Le politiche basate sull'identità determinano se qualcuno può creare, accedere o eliminare risorse Amazon Inspector nel tuo account. Queste azioni possono comportare costi aggiuntivi per l' Account AWS. Quando crei o modifichi policy basate su identità, segui queste linee guida e raccomandazioni:

- Inizia con le policy AWS gestite e passa alle autorizzazioni con privilegi minimi: per iniziare a concedere autorizzazioni a utenti e carichi di lavoro, utilizza le politiche gestite che concedono le autorizzazioni per molti casi d'uso comuni.AWS Sono disponibili nel tuo. Account AWS Ti consigliamo di ridurre ulteriormente le autorizzazioni definendo politiche gestite dai AWS clienti specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWS o Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.
- Applica le autorizzazioni con privilegi minimi: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente di IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso ad azioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi anche utilizzare le condizioni per concedere l'accesso alle azioni del servizio se vengono utilizzate tramite uno specifico Servizio AWS, ad esempio AWS CloudFormation. Per ulteriori informazioni, consulta la sezione Elementi delle policy JSON di IAM: condizione nella Guida per l'utente di IAM.
- Utilizzo di IAM Access Analyzer per convalidare le policy IAM e garantire autorizzazioni sicure e funzionali: IAM Access Analyzer convalida le policy nuove ed esistenti in modo che aderiscano alla sintassi della policy IAM (JSON) e alle best practice di IAM. IAM Access Analyzer offre oltre 100 controlli delle policy e consigli utili per creare policy sicure e funzionali. Per ulteriori informazioni, consulta Convalida delle policy per IAM Access Analyzer nella Guida per l'utente di IAM.
- Richiedi l'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o un utente root nel Account AWS tuo, attiva l'MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente di IAM.

Per maggiori informazioni sulle best practice in IAM, consulta Best practice di sicurezza in IAM nella Guida per l'utente di IAM.

Utilizzo della console Amazon Inspector

Per accedere alla console Amazon Inspector, devi disporre di un set minimo di autorizzazioni. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli sulle risorse Amazon Inspector presenti nel tuo. Account AWS Se crei una policy basata sull'identità più restrittiva rispetto alle autorizzazioni minime richieste, la console non funzionerà nel modo previsto per le entità (utenti o ruoli) associate a tale policy.

Non è necessario consentire autorizzazioni minime per la console agli utenti che effettuano chiamate solo verso AWS CLI o l'API. AWS Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per garantire che utenti e ruoli possano continuare a utilizzare la console Amazon Inspector, collega anche Amazon *ConsoleAccess* Inspector *ReadOnly* AWS o la policy gestita alle entità. Per ulteriori informazioni, consulta Aggiunta di autorizzazioni a un utente nella Guida per l'utente IAM.

Consentire agli utenti di visualizzare le loro autorizzazioni

Questo esempio mostra in che modo è possibile creare una policy che consente agli utenti IAM di visualizzare le policy inline e gestite che sono cpllegate alla relativa identità utente. Questa policy include le autorizzazioni per completare questa azione sulla console o utilizzando programmaticamente l'API o. AWS CLI AWS

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
```

```
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

Consenti l'accesso in sola lettura a tutte le risorse Amazon Inspector

Questo esempio mostra una policy che consente l'accesso in sola lettura a tutte le risorse di Amazon Inspector.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "inspector2:Describe*",
                "inspector2:Get*",
                "inspector2:BatchGet*",
                "inspector2:List*"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
```

```
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
    ]
}
```

Consenti l'accesso completo a tutte le risorse di Amazon Inspector

Questo esempio mostra una policy che consente l'accesso completo a tutte le risorse di Amazon Inspector.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "inspector2:*",
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": "iam:CreateServiceLinkedRole",
            "Resource": "*",
            "Condition": {
                "StringLike": {
                    "iam:AWSServiceName": "inspector2.amazonaws.com"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "organizations:EnableAWSServiceAccess",
                "organizations:RegisterDelegatedAdministrator",
                "organizations:ListDelegatedAdministrators",
                "organizations:ListAWSServiceAccessForOrganization",
                "organizations:DescribeOrganizationalUnit",
                "organizations:DescribeAccount",
                "organizations:DescribeOrganization"
            ],
            "Resource": "*"
        }
```

```
    ]
}
```

AWS politiche gestite per Amazon Inspector

Una politica AWS gestita è una politica autonoma creata e amministrata da. AWS AWS le politiche gestite sono progettate per fornire autorizzazioni per molti casi d'uso comuni, in modo da poter iniziare ad assegnare autorizzazioni a utenti, gruppi e ruoli.

Tieni presente che le policy AWS gestite potrebbero non concedere le autorizzazioni con il privilegio minimo per i tuoi casi d'uso specifici, poiché sono disponibili per tutti i clienti. AWS Consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente specifiche per i tuoi casi d'uso.

Non è possibile modificare le autorizzazioni definite nelle politiche gestite. AWS Se AWS aggiorna le autorizzazioni definite in una politica AWS gestita, l'aggiornamento ha effetto su tutte le identità principali (utenti, gruppi e ruoli) a cui è associata la politica. AWS è più probabile che aggiorni una policy AWS gestita quando ne Servizio AWS viene lanciata una nuova o quando diventano disponibili nuove operazioni API per i servizi esistenti.

Per ulteriori informazioni, consultare Policy gestite da AWSnella Guida per l'utente di IAM.

AWS politica gestita: AmazonInspector2FullAccess

È possibile allegare la policy `AmazonInspector2FullAccess`alle identità IAM.

Questa politica concede autorizzazioni amministrative che consentono l'accesso completo ad Amazon Inspector.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `inspector2`— Consente l'accesso completo alle funzionalità di Amazon Inspector.
- `iam`— Consente ad Amazon Inspector di creare il ruolo collegato al servizio,. `AmazonInspector2AgentlessServiceRole` Ciò è necessario per consentire ad Amazon Inspector di eseguire operazioni come recuperare informazioni sulle istanze Amazon EC2 e sugli archivi Amazon ECR e sulle immagini dei container, analizzare la rete VPC e descrivere gli account associati alla tua organizzazione. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon Inspector.
- `organizations`— Consente agli amministratori di utilizzare Amazon Inspector per un'organizzazione in. AWS Organizations Dopo aver attivato l'accesso affidabile per Amazon Inspector AWS Organizations in, i membri dell'account amministratore delegato possono gestire le impostazioni e visualizzare i risultati in tutta l'organizzazione.
- `codeguru-security`— Consente agli amministratori di utilizzare Amazon Inspector per recuperare frammenti di codice informativo e modificare le impostazioni di crittografia per il codice archiviato da Security. CodeGuru Per ulteriori informazioni, consulta Crittografia inattiva per il codice contenuto nei tuoi risultati.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": "inspector2:*",
   "Resource": "*"
  },
  {
   "Effect": "Allow",
   "Action": [
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration",
    "codeguru-security:UpdateAccountConfiguration"
   ],
   "Resource": "*"
  },
```

```
  {
   "Effect": "Allow",
   "Action": "iam:CreateServiceLinkedRole",
   "Resource": "*",
   "Condition": {
    "StringEquals": {
     "iam:AWSServiceName": "inspector2.amazonaws.com"
    }
   }
  },
  {
   "Effect": "Allow",
   "Action": [
    "organizations:EnableAWSServiceAccess",
    "organizations:RegisterDelegatedAdministrator",
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS politica gestita: AmazonInspector2ReadOnlyAccess

È possibile allegare la policy `AmazonInspector2ReadOnlyAccess`alle identità IAM.

Questa politica concede autorizzazioni che consentono l'accesso in sola lettura ad Amazon Inspector.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `inspector2`— Consente l'accesso in sola lettura alle funzionalità di Amazon Inspector.
- `organizations`— Consente di visualizzare i dettagli sulla copertura di Amazon Inspector per un'organizzazione. AWS Organizations

- `codeguru-security`— Consente di recuperare frammenti di codice da Security. CodeGuru Consente inoltre di visualizzare le impostazioni di crittografia per il codice memorizzato in CodeGuru Security.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Effect": "Allow",
   "Action": [
    "organizations:ListDelegatedAdministrators",
    "organizations:ListAWSServiceAccessForOrganization",
    "organizations:DescribeOrganizationalUnit",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "inspector2:BatchGet*",
    "inspector2:List*",
    "inspector2:Describe*",
    "inspector2:Get*",
    "inspector2:Search*",
    "codeguru-security:BatchGetFindings",
    "codeguru-security:GetAccountConfiguration"
   ],
   "Resource": "*"
  }
 ]
}
```

AWS politica gestita: AmazonInspector2ManagedCisPolicy

Puoi collegare la policy `AmazonInspector2ManagedCisPolicy` anche alle tue entità IAM. Questa policy deve essere associata a un ruolo che concede le autorizzazioni alle istanze Amazon EC2 per eseguire scansioni CIS dell'istanza. Puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 e che effettuano richieste API. AWS CLI AWS Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un AWS ruolo a un'istanza EC2 e renderlo disponibile per tutte le sue applicazioni, crei un profilo di istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente di IAM.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `inspector2`— Consente l'accesso alle azioni utilizzate per eseguire scansioni CIS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
            "inspector2:StartCisSession",
            "inspector2:StopCisSession",
            "inspector2:SendCisSessionTelemetry",
            "inspector2:SendCisSessionHealth"
            ],
            "Resource": "*",
        }
     ]
 }
```

AWS politica gestita: AmazonInspector2ServiceRolePolicy

Non è possibile allegare la policy `AmazonInspector2ServiceRolePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente ad Amazon Inspector di eseguire azioni per tuo conto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon Inspector.

AWS politica gestita: AmazonInspector2AgentlessServiceRolePolicy

Non è possibile allegare la policy `AmazonInspector2AgentlessServiceRolePolicy` alle entità IAM. Questa policy è associata a un ruolo collegato al servizio che consente ad Amazon Inspector di eseguire azioni per tuo conto. Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon Inspector.

Amazon Inspector si aggiorna alle AWS politiche gestite

Visualizza i dettagli sugli aggiornamenti delle politiche AWS gestite per Amazon Inspector da quando questo servizio ha iniziato a tracciare queste modifiche. Per ricevere avvisi automatici sulle modifiche a questa pagina, iscriviti al feed RSS nella pagina della cronologia dei documenti di Amazon Inspector.

Modifica	Descrizione	Data
AmazonInspector2 ManagedCisPolicy — Nuova politica	Amazon Inspector ha aggiunto una nuova policy gestita che puoi utilizzare come parte di un profilo di istanza per consentire le scansioni CIS su un'istanza.	23 gennaio 2024
AmazonInspector2 ServiceRolePolicy — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono ad Amazon Inspector di avviare scansioni CIS sulle istanze di destinazione.	23 gennaio 2024
AmazonInspector2 AgentlessServiceRolePolicy — Nuova politica	Amazon Inspector ha aggiunto una nuova policy relativa ai ruoli collegati ai servizi per consentire la scansione senza agenti dell'istanza EC2.	27 novembre 2023
AmazonInspector2 ReadOnlyAccess — Aggiornamenti a una policy esistente	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono agli utenti di sola lettura di recuperare i dettagli di vulnerability intelligence per rilevare le vulnerabilità dei pacchetti.	22 settembre 2023

Modifica	Descrizione	Data
AmazonInspector2 — Aggiornamenti a una policy esistente ServiceRolePolicy	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono ad Amazon Inspector di scansionare le configurazioni di rete delle istanze Amazon EC2 che fanno parte dei gruppi target Elastic Load Balancing.	31 agosto 2023
AmazonInspector2 — Aggiornamenti a una policy esistente ReadOnlyAccess	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono agli utenti di sola lettura di esportare Software Bill of Materials (SBOM) per le proprie risorse.	29 giugno 2023
AmazonInspector2 ReadOnlyAccess — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono agli utenti di sola lettura di recuperare i dettagli delle impostazioni di crittografia per i risultati della scansione del codice Lambda per il proprio account.	13 giugno 2023
AmazonInspector2 FullAccess — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono agli utenti di configurare una chiave KMS gestita dal cliente per crittografare il codice nei risultati della scansione del codice Lambda.	13 giugno 2023

Modifica	Descrizione	Data
AmazonInspector2 ReadOnlyAccess — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono agli utenti di sola lettura di recuperare i dettagli dello stato e dei risultati della scansione del codice Lambda per il proprio account.	02 maggio 2023
AmazonInspector2 ServiceRolePolicy — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono ad Amazon Inspector di creare canali AWS CloudTrail collegati ai servizi nel tuo account quando attivi la scansione Lambda. Ciò consente ad Amazon Inspector di monitorare CloudTrail gli eventi nel tuo account.	30 aprile 2023
AmazonInspector2 FullAccess — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono agli utenti di recuperare i dettagli delle vulnerabilità del codice rilevate dalla scansione del codice Lambda.	21 aprile 2023

Modifica	Descrizione	Data
AmazonInspector2 ServiceRolePolicy — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono ad Amazon Inspector di inviare informazioni ad Amazon EC2 Systems Manager sui percorsi personalizzati definiti da un cliente per l'ispezione approfondita di Amazon EC2.	17 aprile 2023
AmazonInspector2 ServiceRolePolicy — Aggiornamenti a una policy esistente	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono ad Amazon Inspector di creare canali AWS CloudTrail collegati ai servizi nel tuo account quando attivi la scansione Lambda. Ciò consente ad Amazon Inspector di monitorare CloudTrail gli eventi nel tuo account.	30 aprile 2023

Modifica	Descrizione	Data
AmazonInspector2 ServiceRolePolicy — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono ad Amazon Inspector di richiedere scansioni del codice di sviluppo nelle AWS Lambda funzioni e ricevere dati di scansione da Amazon Security. CodeGuru Inoltre, Amazon Inspector ha aggiunto le autorizzazioni per la revisione delle politiche IAM. Amazon Inspector utilizza queste informazioni per scansionare le funzioni Lambda alla ricerca di vulnerabilità del codice.	28 febbraio 2023
AmazonInspector2 ServiceRolePolicy — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto una nuova istruzione che consente ad Amazon Inspector di recuperare informazioni CloudWatch sull'ultima volta che AWS Lambda una funzione è stata richiamata. Amazon Inspector utilizza queste informazioni per concentrare le scansioni sulle funzioni Lambda del tuo ambiente che sono state attive negli ultimi 90 giorni.	20 febbraio 2023

Modifica	Descrizione	Data
AmazonInspector2 ServiceRolePolicy — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto una nuova dichiarazione che consente ad Amazon Inspector di recuperare informazioni AWS Lambda sulle funzioni, inclusa ogni versione di livello associata a ciascuna funzione. Amazon Inspector utilizza queste informazioni per scansionare le funzioni Lambda alla ricerca di vulnerabilità di sicurezza.	28 novembre 2022
AmazonInspector2 ServiceRolePolicy — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto una nuova azione per consentire ad Amazon Inspector di descrivere le esecuzioni delle associazioni SSM. Inoltre, Amazon Inspector ha aggiunto un ulteriore ambito delle risorse per consentire ad Amazon Inspector di creare, aggiornare, eliminare e avviare associazioni SSM con documenti SSM di proprietà. `AmazonInspector2`	31 agosto 2022
AmazonInspector2 Aggiornamenti ServiceRolePolicy a una policy esistente	Amazon Inspector ha aggiornato l'ambito delle risorse della policy per consentire ad Amazon Inspector di raccogliere l'inventario del software in altre partizioni. AWS	12 agosto 2022

Modifica	Descrizione	Data
AmazonInspector2 ServiceRolePolicy — Aggiornamenti a una politica esistente	Amazon Inspector ha ristrutturato l'ambito delle risorse delle azioni che consentono ad Amazon Inspector di creare, eliminare e aggiornare le associazioni SSM.	10 agosto 2022
AmazonInspector2 — Nuova politica ReadOnlyAccess	Amazon Inspector ha aggiunto una nuova policy per consentire l'accesso in sola lettura alle funzionalità di Amazon Inspector.	21 gennaio 2022
AmazonInspector2 — Nuova politica FullAccess	Amazon Inspector ha aggiunto una nuova policy per consentire l'accesso completo alle funzionalità di Amazon Inspector.	29 novembre 2021
AmazonInspector2 ServiceRolePolicy — Nuova politica	Amazon Inspector ha aggiunto una nuova politica per consentire ad Amazon Inspector di eseguire azioni in altri servizi per tuo conto.	29 novembre 2021
Amazon Inspector ha iniziato a tracciare le modifiche	Amazon Inspector ha iniziato a tracciare le modifiche per le sue politiche AWS gestite.	29 novembre 2021

Utilizzo di ruoli collegati ai servizi per Amazon Inspector

Amazon Inspector utilizza un ruolo collegato al servizio AWS Identity and Access Management (IAM) denominato. `AWSServiceRoleForAmazonInspector2` Questo ruolo collegato al servizio è un ruolo IAM collegato direttamente ad Amazon Inspector. È predefinito da Amazon Inspector e include

tutte le autorizzazioni richieste da Amazon Inspector per chiamare altri utenti per tuo conto. Servizi AWS

Un ruolo collegato al servizio semplifica la configurazione di Amazon Inspector perché non è necessario aggiungere manualmente le autorizzazioni necessarie. Amazon Inspector definisce le autorizzazioni del suo ruolo collegato al servizio e, se non diversamente definito, solo Amazon Inspector può assumere il ruolo. Le autorizzazioni definite includono la policy di attendibilità e la policy delle autorizzazioni che non può essere collegata a nessun'altra entità IAM.

È necessario configurare le autorizzazioni per consentire a un'entità IAM (come un gruppo o un ruolo) di creare, modificare o eliminare un ruolo collegato al servizio. Per ulteriori informazioni, consulta Autorizzazioni del ruolo collegato ai servizi nella Guida per l'utente di IAM. È possibile eliminare un ruolo collegato al servizio solo dopo aver eliminato le relative risorse. In questo modo proteggi le tue risorse Amazon Inspector perché non puoi rimuovere inavvertitamente l'autorizzazione ad accedere alle risorse.

Per informazioni sugli altri servizi che supportano i ruoli collegati al servizio, consulta Servizi AWS che funzionano con IAM e cerca i servizi che riportano Sì nella colonna Ruoli collegati al servizio. Scegli un Sì con un link per consultare la documentazione relativa al ruolo collegato al servizio per quel servizio.

Autorizzazioni di ruolo collegate ai servizi per Amazon Inspector

Amazon Inspector utilizza il ruolo collegato al servizio denominato. `AWSServiceRoleForAmazonInspector2` Questo ruolo collegato al servizio si fida che il servizio assuma il `inspector2.amazonaws.com` ruolo.

La politica di autorizzazione per il ruolo, che è denominato`AmazonInspector2ServiceRolePolicy`, consente ad Amazon Inspector di eseguire attività come:

- Usa le azioni di Amazon Elastic Compute Cloud (Amazon EC2) per recuperare informazioni sulle tue istanze e sui percorsi di rete.
- Utilizza AWS Systems Manager le azioni per recuperare l'inventario dalle tue istanze Amazon EC2 e per recuperare informazioni sui pacchetti di terze parti da percorsi personalizzati.
- Usa l' AWS Systems Manager `SendCommand`azione per richiamare le scansioni CIS per le istanze di destinazione.
- Utilizza le azioni di Amazon Elastic Container Registry per recuperare informazioni sulle immagini dei contenitori.

- Usa AWS Lambda le azioni per recuperare informazioni sulle tue funzioni Lambda.
- Usa AWS Organizations le azioni per descrivere gli account associati.
- Usa CloudWatch le azioni per recuperare informazioni sull'ultima volta che le tue funzioni Lambda sono state richiamate.
- Utilizza azioni IAM selezionate per recuperare informazioni sulle tue policy IAM che potrebbero creare vulnerabilità di sicurezza nel tuo codice Lambda.
- Usa le azioni CodeGuru di sicurezza per eseguire scansioni del codice nelle tue funzioni Lambda. Amazon Inspector utilizza le seguenti azioni CodeGuru di sicurezza:
  - codeguru-security: CreateScan — Concede l'autorizzazione a creare una scansione di sicurezza. CodeGuru
  - codeguru-security: GetScan — Concede l'autorizzazione a recuperare i metadati della scansione di sicurezza. CodeGuru
  - codeguru-security: — Concede il permesso di recuperare i risultati generati da Security. ListFindings CodeGuru
  - codeguru-security: DeleteScansByCategory — Concede a Security l'autorizzazione a eliminare le CodeGuru scansioni avviate da Amazon Inspector.
  - codeguru-security: BatchGetFindings — Concede l'autorizzazione a recuperare un batch di risultati specifici generati da Security. CodeGuru
- Utilizza determinate azioni Elastic Load Balancing per eseguire scansioni di rete delle istanze EC2 che fanno parte dei gruppi target di Elastic Load Balancing.

Il ruolo è configurato con la seguente politica di autorizzazioni.

```
    {
"Version": "2012-10-17",
"Statement": [
 {
  "Sid": "TirosPolicy",
  "Effect": "Allow",
  "Action": [
   "directconnect:DescribeConnections",
   "directconnect:DescribeDirectConnectGatewayAssociations",
   "directconnect:DescribeDirectConnectGatewayAttachments",
   "directconnect:DescribeDirectConnectGateways",
   "directconnect:DescribeVirtualGateways",
   "directconnect:DescribeVirtualInterfaces",
```

```
    "ec2:DescribeAvailabilityZones",
    "ec2:DescribeCustomerGateways",
    "ec2:DescribeInstances",
    "ec2:DescribeInternetGateways",
    "ec2:DescribeManagedPrefixLists",
    "ec2:DescribeNatGateways",
    "ec2:DescribeNetworkAcls",
    "ec2:DescribeNetworkInterfaces",
    "ec2:DescribePrefixLists",
    "ec2:DescribeRegions",
    "ec2:DescribeRouteTables",
    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSubnets",
    "ec2:DescribeTransitGatewayAttachments",
    "ec2:DescribeTransitGatewayConnects",
    "ec2:DescribeTransitGatewayPeeringAttachments",
    "ec2:DescribeTransitGatewayRouteTables",
    "ec2:DescribeTransitGatewayVpcAttachments",
    "ec2:DescribeTransitGateways",
    "ec2:DescribeVpcEndpointServiceConfigurations",
    "ec2:DescribeVpcEndpoints",
    "ec2:DescribeVpcPeeringConnections",
    "ec2:DescribeVpcs",
    "ec2:DescribeVpnConnections",
    "ec2:DescribeVpnGateways",
    "ec2:GetManagedPrefixListEntries",
    "ec2:GetTransitGatewayRouteTablePropagations",
    "ec2:SearchTransitGatewayRoutes",
    "elasticloadbalancing:DescribeListeners",
    "elasticloadbalancing:DescribeLoadBalancerAttributes",
    "elasticloadbalancing:DescribeLoadBalancers",
    "elasticloadbalancing:DescribeRules",
    "elasticloadbalancing:DescribeTags",
    "elasticloadbalancing:DescribeTargetGroups",
    "elasticloadbalancing:DescribeTargetGroupAttributes",
    "elasticloadbalancing:DescribeTargetHealth",
    "network-firewall:DescribeFirewall",
    "network-firewall:DescribeFirewallPolicy",
    "network-firewall:DescribeResourcePolicy",
    "network-firewall:DescribeRuleGroup",
    "network-firewall:ListFirewallPolicies",
    "network-firewall:ListFirewalls",
    "network-firewall:ListRuleGroups",
    "tiros:CreateQuery",
```

```
    "tiros:GetQueryAnswer"
   ],
   "Resource": [
    "*"
   ]
  },
  {
   "Sid": "PackageVulnerabilityScanning",
   "Effect": "Allow",
   "Action": [
    "ecr:BatchGetImage",
    "ecr:BatchGetRepositoryScanningConfiguration",
    "ecr:DescribeImages",
    "ecr:DescribeRegistry",
    "ecr:DescribeRepositories",
    "ecr:GetAuthorizationToken",
    "ecr:GetDownloadUrlForLayer",
    "ecr:GetRegistryScanningConfiguration",
    "ecr:ListImages",
    "ecr:PutRegistryScanningConfiguration",
    "organizations:DescribeAccount",
    "organizations:DescribeOrganization",
    "organizations:ListAccounts",
    "ssm:DescribeAssociation",
    "ssm:DescribeAssociationExecutions",
    "ssm:DescribeInstanceInformation",
    "ssm:ListAssociations",
    "ssm:ListResourceDataSync"
   ],
   "Resource": "*"
  },
  {
   "Sid": "LambdaPackageVulnerabilityScanning",
   "Effect": "Allow",
   "Action": [
    "lambda:ListFunctions",
    "lambda:GetFunction",
    "lambda:GetLayerVersion",
    "cloudwatch:GetMetricData"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GatherInventory",
```

```
    "Effect": "Allow",
    "Action": [
     "ssm:CreateAssociation",
     "ssm:StartAssociationsOnce",
     "ssm:DeleteAssociation",
     "ssm:UpdateAssociation"
    ],
    "Resource": [
     "arn:aws:ec2:*:*:instance/*",
     "arn:aws:ssm:*:*:document/AmazonInspector2-*",
     "arn:aws:ssm:*:*:document/AWS-GatherSoftwareInventory",
     "arn:aws:ssm:*:*:managed-instance/*",
     "arn:aws:ssm:*:*:association/*"
    ]
   },
   {
    "Sid": "DataSyncCleanup",
    "Effect": "Allow",
    "Action": [
     "ssm:CreateResourceDataSync",
     "ssm:DeleteResourceDataSync"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:resource-data-sync/InspectorResourceDataSync-do-not-delete"
    ]
   },
   {
    "Sid": "ManagedRules",
    "Effect": "Allow",
    "Action": [
     "events:PutRule",
     "events:DeleteRule",
     "events:DescribeRule",
     "events:ListTargetsByRule",
     "events:PutTargets",
     "events:RemoveTargets"
    ],
    "Resource": [
     "arn:aws:events:*:*:rule/DO-NOT-DELETE-AmazonInspector*ManagedRule"
    ]
   },
   {
    "Sid": "LambdaCodeVulnerabilityScanning",
    "Effect": "Allow",
```

```
    "Action": [
     "codeguru-security:CreateScan",
     "codeguru-security:GetAccountConfiguration",
     "codeguru-security:GetFindings",
     "codeguru-security:GetScan",
     "codeguru-security:ListFindings",
     "codeguru-security:BatchGetFindings",
     "codeguru-security:DeleteScansByCategory"
    ],
    "Resource": [
     "*"
    ]
   },
   {
    "Sid": "CodeGuruCodeVulnerabilityScanning",
    "Effect": "Allow",
    "Action": [
     "iam:GetRole",
     "iam:GetRolePolicy",
     "iam:GetPolicy",
     "iam:GetPolicyVersion",
     "iam:ListAttachedRolePolicies",
     "iam:ListPolicies",
     "iam:ListPolicyVersions",
     "iam:ListRolePolicies",
     "lambda:ListVersionsByFunction"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "ForAnyValue:StringEquals": {
      "aws:CalledVia": [
       "codeguru-security.amazonaws.com"
      ]
     }
    }
   },
   {
    "Sid": "Ec2DeepInspection",
    "Effect": "Allow",
    "Action": [
     "ssm:PutParameter",
     "ssm:GetParameters",
```

```
    "ssm:DeleteParameter"
   ],
   "Resource": [
    "arn:aws:ssm:*:*:parameter/inspector-aws/service/inspector-linux-application-paths"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "AllowManagementOfServiceLinkedChannel",
   "Effect": "Allow",
   "Action": [
    "cloudtrail:CreateServiceLinkedChannel",
    "cloudtrail:DeleteServiceLinkedChannel"
   ],
   "Resource": [
    "arn:aws:cloudtrail:*:*:channel/aws-service-channel/inspector2/*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "AllowListServiceLinkedChannels",
   "Effect": "Allow",
   "Action": [
    "cloudtrail:ListServiceLinkedChannels"
   ],
   "Resource": [
    "*"
   ],
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    }
   }
  },
  {
   "Sid": "AllowToRunInvokeCisSpecificDocuments",
```

```
    "Effect": "Allow",
    "Action": [
     "ssm:SendCommand",
     "ssm:GetCommandInvocation"
    ],
    "Resource": [
     "arn:aws:ssm:*:*:document/AmazonInspector2-InvokeInspectorSsmPluginCIS"
    ]
   },
   {
    "Sid": "AllowToRunCisCommandsToSpecificResources",
    "Effect": "Allow",
    "Action": [
     "ssm:SendCommand"
    ],
    "Resource": [
     "arn:aws:ec2:*:*:instance/*"
    ],
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   },
   {
    "Sid": "AllowToPutCloudwatchMetricData",
    "Effect": "Allow",
    "Action": [
     "cloudwatch:PutMetricData"
    ],
    "Resource": [
     "*"
    ],
    "Condition": {
     "StringEquals": {
      "cloudwatch:namespace": "AWS/Inspector2"
     }
    }
   }
  ]
}
```

Creazione di un ruolo collegato ai servizi per Amazon Inspector

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando attivi Amazon Inspector nell'API AWS Management Console, nella o nell' AWS API AWS CLI, Amazon Inspector crea il ruolo collegato al servizio per te.

Modifica di un ruolo collegato al servizio per Amazon Inspector

Amazon Inspector non consente di modificare il ruolo collegato al `AWSServiceRoleForAmazonInspector2` servizio. Dopo aver creato un ruolo collegato al servizio, non è possibile modificare il nome del ruolo perché diverse entità potrebbero fare riferimento al ruolo. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per Amazon Inspector

Se non hai più bisogno di utilizzare Amazon Inspector, ti consigliamo di eliminare il ruolo collegato al `AWSServiceRoleForAmazonInspector2` servizio. Prima di poter eliminare il ruolo, devi disattivare Amazon Inspector in Regione AWS ogni luogo in cui è attivato. Quando disattivi Amazon Inspector, il ruolo non viene eliminato per te. Pertanto, se attivi nuovamente Amazon Inspector, può utilizzare il ruolo esistente. In questo modo puoi evitare di avere un'entità inutilizzata che non viene monitorata o gestita attivamente. Tuttavia, è necessario effettuare la pulizia delle risorse associate al ruolo collegato al servizio prima di poterlo eliminare manualmente.

Se devi ricreare un ruolo collegato ai servizi che hai precedentemente eliminato, puoi utilizzare lo stesso processo per ricreare il ruolo nel tuo account. Quando attivi Amazon Inspector, Amazon Inspector ricrea per te il ruolo collegato al servizio.

> **Note**
>
> Se il servizio Amazon Inspector utilizza il ruolo quando tenti di eliminare le risorse, l'eliminazione potrebbe non riuscire. In tal caso, attendi qualche minuto e poi riprova a eseguire l'operazione.

Puoi utilizzare la console IAM AWS CLI, o l' AWS API per eliminare il ruolo `AWSServiceRoleForAmazonInspector2` collegato al servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Autorizzazioni di ruolo collegate ai servizi per le scansioni senza agenti di Amazon Inspector

La scansione senza agenti di Amazon Inspector utilizza il ruolo collegato al servizio denominato. `AWSServiceRoleForAmazonInspector2Agentless` Questa reflex consente ad Amazon Inspector di creare uno snapshot del volume Amazon EBS nel tuo account e quindi accedere ai dati da tale snapshot. Questo ruolo collegato al servizio si fida che il servizio assuma il ruolo. `agentless.inspector2.amazonaws.com`

> **Important**
>
> Le istruzioni in questo ruolo collegato al servizio impediscono ad Amazon Inspector di eseguire scansioni senza agenti su qualsiasi istanza EC2 che hai escluso dalle scansioni utilizzando il tag. `InspectorEc2Exclusion` Inoltre, le istruzioni impediscono ad Amazon Inspector di accedere ai dati crittografati da un volume quando la chiave KMS utilizzata per crittografarli ha il tag. `InspectorEc2Exclusion` Per ulteriori informazioni, consulta Esclusione delle istanze dalle scansioni di Amazon Inspector.

La politica di autorizzazione per il ruolo, che è denominato`AmazonInspector2AgentlessServiceRolePolicy`, consente ad Amazon Inspector di eseguire attività come:

- Usa le azioni di Amazon Elastic Compute Cloud (Amazon EC2) per recuperare informazioni sulle istanze, i volumi e gli snapshot EC2.
  - Usa le azioni di tagging di Amazon EC2 per etichettare gli snapshot per le scansioni con la chiave tag. `InspectorScan`
  - Utilizza le azioni snapshot di Amazon EC2 per creare istantanee, etichettarle con la chiave `InspectorScan` tag e quindi eliminare le istantanee dei volumi Amazon EBS a cui è stato assegnato il tag key. `InspectorScan`
- Utilizza le azioni di Amazon EBS per recuperare informazioni dagli snapshot contrassegnati con la `InspectorScan` chiave tag.
- Utilizza azioni di decrittografia selezionate per AWS KMS decrittografare istantanee crittografate con chiavi gestite dal cliente. AWS KMS Amazon Inspector non decrittografa le istantanee quando la chiave KMS utilizzata per crittografarle è contrassegnata con il tag. `InspectorEc2Exclusion`

Il ruolo è configurato con la seguente politica di autorizzazioni.

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "InstanceIdentification",
   "Effect": "Allow",
   "Action": [
    "ec2:DescribeInstances",
    "ec2:DescribeVolumes",
    "ec2:DescribeSnapshots"
   ],
   "Resource": "*"
  },
  {
   "Sid": "GetSnapshotData",
   "Effect": "Allow",
   "Action": [
    "ebs:ListSnapshotBlocks",
    "ebs:GetSnapshotBlock"
   ],
   "Resource": "arn:aws:ec2:*:*:snapshot/*",
   "Condition": {
    "StringLike": {
     "aws:ResourceTag/InspectorScan": "*"
    }
   }
  },
  {
   "Sid": "CreateSnapshotsAnyInstanceOrVolume",
   "Effect": "Allow",
   "Action": "ec2:CreateSnapshots",
   "Resource": [
    "arn:aws:ec2:*:*:instance/*",
    "arn:aws:ec2:*:*:volume/*"
   ]
  },
  {
   "Sid": "DenyCreateSnapshotsOnExcludedInstances",
   "Effect": "Deny",
   "Action": "ec2:CreateSnapshots",
   "Resource": "arn:aws:ec2:*:*:instance/*",
```

```
    "Condition": {
     "StringEquals": {
      "ec2:ResourceTag/InspectorEc2Exclusion": "true"
     }
    }
   },
   {
    "Sid": "CreateSnapshotsOnAnySnapshotOnlyWithTag",
    "Effect": "Allow",
    "Action": "ec2:CreateSnapshots",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
     "Null": {
      "aws:TagKeys": "false"
     },
     "ForAllValues:StringEquals": {
      "aws:TagKeys": "InspectorScan"
     }
    }
   },
   {
    "Sid": "CreateOnlyInspectorScanTagOnlyUsingCreateSnapshots",
    "Effect": "Allow",
    "Action": "ec2:CreateTags",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
     "StringLike": {
      "ec2:CreateAction": "CreateSnapshots"
     },
     "Null": {
      "aws:TagKeys": "false"
     },
     "ForAllValues:StringEquals": {
      "aws:TagKeys": "InspectorScan"
     }
    }
   },
   {
    "Sid": "DeleteOnlySnapshotsTaggedForScanning",
    "Effect": "Allow",
    "Action": "ec2:DeleteSnapshot",
    "Resource": "arn:aws:ec2:*:*:snapshot/*",
    "Condition": {
     "StringLike": {
```

```
      "ec2:ResourceTag/InspectorScan": "*"
     }
    }
   },
   {
    "Sid": "DenyKmsDecryptForExcludedKeys",
    "Effect": "Deny",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceTag/InspectorEc2Exclusion": "true"
     }
    }
   },
   {
    "Sid": "DecryptSnapshotBlocksVolContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id": "vol-*"
     }
    }
   },
   {
    "Sid": "DecryptSnapshotBlocksSnapContext",
    "Effect": "Allow",
    "Action": "kms:Decrypt",
    "Resource": "arn:aws:kms:*:*:key/*",
    "Condition": {
     "StringEquals": {
      "aws:ResourceAccount": "${aws:PrincipalAccount}"
     },
     "StringLike": {
      "kms:ViaService": "ec2.*.amazonaws.com",
      "kms:EncryptionContext:aws:ebs:id": "snap-*"
     }
    }
```

```
  },
  {
   "Sid": "DescribeKeysForEbsOperations",
   "Effect": "Allow",
   "Action": "kms:DescribeKey",
   "Resource": "arn:aws:kms:*:*:key/*",
   "Condition": {
    "StringEquals": {
     "aws:ResourceAccount": "${aws:PrincipalAccount}"
    },
    "StringLike": {
     "kms:ViaService": "ec2.*.amazonaws.com"
    }
   }
  },
  {
   "Sid": "ListKeyResourceTags",
   "Effect": "Allow",
   "Action": "kms:ListResourceTags",
   "Resource": "arn:aws:kms:*:*:key/*"
  }
 ]
}
```

Creazione di un ruolo collegato al servizio per la scansione senza agenti

Non hai bisogno di creare manualmente un ruolo collegato ai servizi. Quando attivi Amazon Inspector nell'API AWS Management Console, nella o nell' AWS API AWS CLI, Amazon Inspector crea il ruolo collegato al servizio per te.

Modifica di un ruolo collegato al servizio per una scansione senza agenti

Amazon Inspector non consente di modificare il ruolo collegato al `AWSServiceRoleForAmazonInspector2Agentless` servizio. Dopo aver creato un ruolo collegato al servizio, non è possibile modificare il nome del ruolo perché diverse entità potrebbero fare riferimento al ruolo. È possibile tuttavia modificarne la descrizione utilizzando IAM. Per ulteriori informazioni, consulta Modifica di un ruolo collegato ai servizi nella Guida per l'utente di IAM.

Eliminazione di un ruolo collegato al servizio per la scansione senza agenti

Se non è più necessario utilizzare una funzionalità o un servizio che richiede un ruolo collegato al servizio, ti consigliamo di eliminare il ruolo. In questo modo non hai un'entità non utilizzata che non viene monitorata o gestita attivamente.

> **Important**
>
> Per eliminare il `AWSServiceRoleForAmazonInspector2Agentless` ruolo, è necessario impostare la modalità di scansione su basata su agenti in tutte le regioni in cui è disponibile la scansione senza agenti. Per ulteriori informazioni, vedere [TBD setting scan mode link].

Per eliminare manualmente il ruolo collegato ai servizi mediante IAM

Utilizza la console IAM AWS CLI, o l' AWS API per eliminare il ruolo collegato al AWSServiceRoleForAmazonInspector2Agentless servizio. Per ulteriori informazioni, consulta Eliminazione del ruolo collegato al servizio nella Guida per l'utente di IAM.

Risoluzione dei problemi relativi all'identità e all'accesso ad Amazon Inspector

Utilizza le seguenti informazioni per aiutarti a diagnosticare e risolvere i problemi più comuni che potresti riscontrare quando lavori con Amazon Inspector e IAM.

Argomenti

- Non sono autorizzato a eseguire un'azione in Amazon Inspector
- Non sono autorizzato a eseguire iam: PassRole
- Desidero consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon Inspector

Non sono autorizzato a eseguire un'azione in Amazon Inspector

Se ricevi un errore che indica che non sei autorizzato a eseguire un'operazione, le tue policy devono essere aggiornate per poter eseguire l'operazione.

L'errore di esempio seguente si verifica quando l'utente IAM `mateojackson` prova a utilizzare la console per visualizzare i dettagli relativi a una risorsa *`my-example-widget`* fittizia ma non dispone di autorizzazioni `inspector2:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 inspector2:GetWidget on resource: my-example-widget
```

In questo caso, la policy per l'utente `mateojackson` deve essere aggiornata per consentire l'accesso alla risorsa *`my-example-widget`* utilizzando l'azione `inspector2:`*`GetWidget`*.

Se hai bisogno di assistenza, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam: PassRole

Se ricevi un messaggio di errore indicante che non sei autorizzato a eseguire l'`iam:PassRole`azione, le tue politiche devono essere aggiornate per consentirti di trasferire un ruolo ad Amazon Inspector.

Alcuni Servizi AWS consentono di trasferire un ruolo esistente a quel servizio invece di creare un nuovo ruolo di servizio o un ruolo collegato al servizio. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

Il seguente errore di esempio si verifica quando un utente IAM denominato `marymajor` tenta di utilizzare la console per eseguire un'azione in Amazon Inspector. Tuttavia, l'azione richiede che il servizio disponga delle autorizzazioni concesse da un ruolo di servizio. Mary non dispone delle autorizzazioni per passare il ruolo al servizio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

In questo caso, le policy di Mary devono essere aggiornate per poter eseguire l'operazione `iam:PassRole`.

Se hai bisogno di aiuto, contatta il tuo AWS amministratore. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Desidero consentire a persone esterne a me di accedere Account AWS alle mie risorse Amazon Inspector

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per sapere se Amazon Inspector supporta queste funzionalità, consulta. Come funziona Amazon Inspector con IAM
- Per sapere come fornire l'accesso alle tue risorse su tutto Account AWS ciò che possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWS di tua proprietà nella IAM User Guide.
- Per scoprire come fornire l'accesso alle tue risorse a terze parti Account AWS, consulta Fornire l'accesso a soggetti Account AWS di proprietà di terze parti nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso tramite la federazione delle identità, consulta Fornire l'accesso a utenti autenticati esternamente (Federazione delle identità) nella Guida per l'utente di IAM.
- Per informazioni sulle differenze tra l'utilizzo di ruoli e policy basate su risorse per l'accesso multi-account, consulta Differenza tra i ruoli IAM e le policy basate su risorse nella Guida per l'utente IAM.

Monitoraggio di Amazon Inspector

Il monitoraggio è una parte importante per mantenere l'affidabilità, la disponibilità e le prestazioni di Amazon Inspector e delle altre AWS soluzioni. AWS fornisce strumenti di monitoraggio per monitorare Amazon Inspector, segnalare quando qualcosa non va e intraprendere azioni automatiche quando necessario:

- Amazon EventBridge è un servizio di bus eventi senza server che semplifica la connessione delle applicazioni con dati provenienti da una varietà di fonti. EventBridge fornisce un flusso di dati in tempo reale dalle tue applicazioni, dalle applicazioni oftware-as-a S-Service (SaaS) e dai servizi AWS e indirizza tali dati verso destinazioni come Lambda. Ciò consente di monitorare gli eventi che si verificano nei servizi e creare architetture basate sugli eventi. Per ulteriori informazioni, consulta la Amazon EventBridge User Guide.

- AWS CloudTrail acquisisce chiamate API ed eventi correlati da parte di o per conto del tuo Account AWS. CloudTrail quindi consegna i file di log a un bucket Amazon S3 specificato. Puoi identificare quali utenti e account hanno effettuato le chiamate AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate. Per ulteriori informazioni, consulta la Guida per l'utente AWS CloudTrail.

Registrazione delle chiamate API Amazon Inspector tramite AWS CloudTrail

Amazon Inspector è integrato con AWS CloudTrail un servizio che fornisce una registrazione delle azioni intraprese da un utente o ruolo IAM o da un Servizio AWS utente in Amazon Inspector. CloudTrail acquisisce tutte le chiamate API per Amazon Inspector come eventi. Le chiamate acquisite includono chiamate dalla console Amazon Inspector e chiamate alle operazioni dell'API Amazon Inspector. Se crei un trail, puoi abilitare la distribuzione continua di CloudTrail eventi a un bucket Amazon S3, inclusi gli eventi per Amazon Inspector. Se non configuri un percorso, puoi comunque visualizzare gli eventi più recenti nella CloudTrail console nella cronologia degli eventi. Utilizzando le informazioni raccolte da CloudTrail, puoi determinare:

- La richiesta che è stata fatta ad Amazon Inspector.
- Indirizzo IP dal quale è stata effettuata la richiesta.
- Chi ha effettuato la richiesta.
- Quando è stata effettuata la richiesta.

Per ulteriori informazioni CloudTrail, consulta la Guida AWS CloudTrail per l'utente.

Informazioni su Amazon Inspector in CloudTrail

CloudTrail è abilitato sul tuo account al Account AWS momento della creazione dell'account. Quando si verifica un'attività in Amazon Inspector, tale attività viene registrata in un CloudTrail evento insieme ad altri Servizio AWS eventi nella cronologia degli eventi. Puoi visualizzare, cercare e scaricare eventi recenti in. Account AWS Per ulteriori informazioni, consulta Visualizzazione degli eventi con la cronologia degli CloudTrail eventi.

Per una registrazione continua degli eventi del tuo Account AWS, compresi gli eventi per Amazon Inspector, crea un percorso. Un trail consente di CloudTrail inviare file di log a un bucket Amazon S3.

Per impostazione predefinita, quando si crea un percorso nella console, questo sarà valido in tutte le Regioni AWS. Il percorso registra gli eventi di tutte le Regioni nella partizione AWS e distribuisce i file di log nel bucket Amazon S3 specificato. Inoltre, puoi configurarne altri Servizi AWS per analizzare ulteriormente e agire in base ai dati sugli eventi raccolti nei CloudTrail log. Per ulteriori informazioni, consulta i seguenti argomenti:

- Panoramica della creazione di un percorso
- CloudTrail servizi e integrazioni supportati
- Configurazione delle notifiche Amazon SNS per CloudTrail
- Ricezione di file di CloudTrail registro da più account
- Ricezione di file di CloudTrail registro da più regioni

Tutte le azioni di Amazon Inspector vengono registrate da. CloudTrail Tutte le azioni che Amazon Inspector può eseguire sono documentate nell'Amazon Inspector API Reference. Ad esempio, le chiamate a `CreateFindingsReportListCoverage`, e `UpdateOrganizationConfiguration` le azioni generano voci nei file di registro. CloudTrail

Ogni evento o voce di log contiene informazioni sull'utente che ha generato la richiesta. Le informazioni di identità consentono di determinare quanto segue:

- Se la richiesta è stata effettuata con le credenziali utente root o utente IAM.
- Se la richiesta è stata effettuata con credenziali di sicurezza temporanee per un ruolo o un utente federato.
- Se la richiesta è stata effettuata da un altro Servizio AWS.

Per ulteriori informazioni, vedete l'elemento CloudTrail userIdentity.

Informazioni sulle voci dei file di log di Amazon Inspector

Un trail è una configurazione che consente la distribuzione di eventi come file di log in un bucket Amazon S3 specificato dall'utente. CloudTrail i file di registro contengono una o più voci di registro. Un evento rappresenta una singola richiesta da un'origine. Gli eventi includono le informazioni sull'operazione richiesta, la data e l'ora dell'operazione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

Amazon Inspector Scansiona le informazioni in CloudTrail

Amazon Inspector Scan è integrato con. CloudTrail Tutte le operazioni dell'API Amazon Inspector Scan vengono registrate come eventi di gestione. Per un elenco delle operazioni dell'API Amazon Inspector Scan a cui Amazon Inspector accede, CloudTrail consulta Amazon Inspector Scan nel riferimento alle API di Amazon Inspector.

L'esempio seguente mostra una voce di CloudTrail registro che dimostra l'azione: `ScanSbom`


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AROA123456789EXAMPLE:akua_mansa",
        "arn": "arn:aws:sts::111122223333:assumed-role/Admin/akua_mansa",
        "accountId": "111122223333",
        "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AROA123456789EXAMPLE",
                "arn": "arn:aws:iam::111122223333:role/Admin",
                "accountId": "111122223333",
                "userName": "Admin"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-10-17T15:22:59Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-17T16:02:34Z",
    "eventSource": "gamma-inspector-scan.amazonaws.com",
    "eventName": "ScanSbom",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "203.0.113.0",
    "userAgent": "aws-sdk-java/2.20.162 Mac_OS_X/13.5.2 OpenJDK_64-
Bit_Server_VM/17.0.8+7-LTS Java/17.0.8 vendor/Amazon.com_Inc. io/sync http/
UrlConnection cfg/retry-mode/legacy",
    "requestParameters": {
        "sbom": {
```

```
            "specVersion": "1.5",
            "metadata": {
                "component": {
                    "name": "debian",
                    "type": "operating-system",
                    "version": "9"
                }
            },
            "components": [
                {
                    "name": "packageOne",
                    "purl": "pkg:deb/debian/packageOne@1.0.0?arch=x86_64&distro=9",
                    "type": "application"
                }
            ],
            "bomFormat": "CycloneDX"
        }
    },
    "responseElements": null,
    "requestID": "f041a27f-f33e-4f70-b09b-5fbc5927282a",
    "eventID": "abc8d1e4-d214-4f07-bc56-8a31be6e36fe",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "111122223333",
    "eventCategory": "Management"
}
```


Convalida della conformità per Amazon Inspector

Per sapere se un Servizio AWS programma rientra nell'ambito di uno specifico programma di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS Program e scegli il programma di conformità che ti interessa. Per informazioni generali, consulta Programmi di AWS conformità Programmi di di .

È possibile scaricare report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Scaricamento dei report in AWS Artifact .

La vostra responsabilità di conformità durante l'utilizzo Servizi AWS è determinata dalla sensibilità dei dati, dagli obiettivi di conformità dell'azienda e dalle leggi e dai regolamenti applicabili. AWS fornisce le seguenti risorse per contribuire alla conformità:

- Guide introduttive su sicurezza e conformità: queste guide all'implementazione illustrano considerazioni sull'architettura e forniscono passaggi per implementare ambienti di base incentrati sulla AWS sicurezza e la conformità.
- Progettazione per la sicurezza e la conformità HIPAA su Amazon Web Services: questo white paper descrive come le aziende possono utilizzare AWS per creare applicazioni idonee all'HIPAA.

> **Note**
>
> Non Servizi AWS tutte sono idonee all'HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- AWS Risorse per la per la conformità: questa raccolta di cartelle di lavoro e guide potrebbe essere valida per il tuo settore e la tua località.
- AWS Guide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).
- Valutazione delle risorse con regole nella Guida per gli AWS Config sviluppatori: il AWS Config servizio valuta la conformità delle configurazioni delle risorse alle pratiche interne, alle linee guida e alle normative del settore.
- AWS Security Hub— Ciò Servizio AWS fornisce una visione completa dello stato di sicurezza interno. AWS La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWS e verificare la conformità agli standard e alle best practice del settore della sicurezza. Per un elenco dei servizi e dei controlli supportati, consulta la pagina Documentazione di riferimento sui controlli della Centrale di sicurezza.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente AWS l'utilizzo per semplificare la gestione dei rischi e la conformità alle normative e agli standard di settore.

Resilienza in Amazon Inspector

L'infrastruttura AWS globale è costruita attorno Regioni AWS a zone di disponibilità. Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate, collegate con reti a bassa latenza, ad alto throughput e altamente ridondanti. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza

interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Sicurezza dell'infrastruttura in Amazon Inspector

In quanto servizio gestito, Amazon Inspector è protetto dalla sicurezza di rete AWS globale. Per informazioni sui servizi di AWS sicurezza e su come AWS protegge l'infrastruttura, consulta AWS Cloud Security. Per progettare il tuo AWS ambiente utilizzando le migliori pratiche per la sicurezza dell'infrastruttura, vedi Infrastructure Protection in Security Pillar AWS Well-Architected Framework.

Utilizza chiamate API AWS pubblicate per accedere ad Amazon Inspector attraverso la rete. I client devono supportare quanto segue:

- Transport Layer Security (TLS). È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Suite di cifratura con Perfect Forward Secrecy (PFS), ad esempio Ephemeral Diffie-Hellman (DHE) o Elliptic Curve Ephemeral Diffie-Hellman (ECDHE). La maggior parte dei sistemi moderni, come Java 7 e versioni successive, supporta tali modalità.

Inoltre, le richieste devono essere firmate utilizzando un ID chiave di accesso e una chiave di accesso segreta associata a un principale IAM. O puoi utilizzare AWS Security Token Service (AWS STS) per generare credenziali di sicurezza temporanee per sottoscrivere le richieste.

Risposta agli incidenti in Amazon Inspector

La sicurezza è la massima priorità in. AWS Come parte del modello di responsabilità condivisa del AWS cloud, AWS gestisce un data center, una rete e un'architettura software che soddisfa i requisiti delle organizzazioni più sensibili alla sicurezza. AWS è responsabile di qualsiasi risposta agli incidenti relativi al servizio stesso AWS Config . Inoltre, in qualità di AWS cliente, condividi la responsabilità di mantenere la sicurezza nel cloud. Ciò significa che controllate la sicurezza che scegliete di implementare utilizzando gli AWS strumenti e le funzionalità a cui avete accesso e siete responsabili della risposta agli incidenti dal punto di vista del modello di responsabilità condivisa.

Stabilendo una base di sicurezza che soddisfi gli obiettivi delle applicazioni eseguite nel cloud, sei in grado di rilevare deviazioni a cui puoi rispondere. Poiché la risposta agli incidenti di sicurezza può essere un argomento complesso, ti invitiamo a consultare le seguenti risorse in modo da comprendere meglio l'impatto che la risposta agli incidenti (IR) e le tue scelte hanno sugli obiettivi aziendali: AWS Security Incident Response Guide, white paper sulle migliori pratiche di AWS sicurezza e white paper Security Perspective of the AWS Cloud Adoption Framework (CAF).

Integrazioni con Amazon Inspector

Amazon Inspector si integra con altri servizi. AWS Questi servizi possono importare dati da Amazon Inspector per consentirti di visualizzare i risultati in modi nuovi. Consulta le seguenti opzioni di integrazione per ulteriori informazioni su come il servizio è configurato per funzionare con Amazon Inspector.

Integrazione di Amazon Inspector con Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) è un registro di container Docker completamente gestito che semplifica l'archiviazione, la condivisione e la distribuzione delle immagini dei container. I registri privati di Amazon ECR ospitano le immagini dei container in un'architettura altamente disponibile e scalabile. Puoi usare Amazon Inspector per scansionare le immagini dei container che risiedono nei tuoi repository Amazon ECR alla ricerca di pacchetti di sistemi operativi e pacchetti di linguaggi di programmazione vulnerabili.

Per ulteriori informazioni sull'utilizzo di Amazon ECR con Amazon Inspector, consulta. Integrazione di Amazon Inspector con Amazon Elastic Container Registry (Amazon ECR)

Integrazione di Amazon Inspector con AWS Security Hub

AWS Security Hubraccoglie dati di sicurezza da tutti i tuoi AWS account, servizi e altri prodotti supportati per valutare lo stato di sicurezza del tuo ambiente in base agli standard e alle migliori pratiche del settore. Oltre a valutare il livello di sicurezza, Security Hub crea una posizione centrale per i risultati di tutti i AWS servizi integrati e i prodotti AWS Partner Network. L'attivazione di Security Hub con Amazon Inspector consente automaticamente a Security Hub di importare i dati dei risultati di Amazon Inspector.

Per ulteriori informazioni sull'utilizzo di Security Hub con Amazon Inspector, consulta. Integrazione di Amazon Inspector con AWS Security Hub

Integrazione di Amazon Inspector con Amazon Elastic Container Registry (Amazon ECR)

Amazon ECR è un registro di container completamente gestito che supporta immagini e artefatti Docker e OCI su. AWS Se utilizzi Amazon ECR, puoi attivare la scansione avanzata del registro per

consentire ad Amazon Inspector di rilevare automaticamente le immagini dei container e scansionarle alla ricerca di pacchetti di sistemi operativi e pacchetti di linguaggi di programmazione vulnerabili.

Questa integrazione consente di visualizzare i risultati di Amazon Inspector per le immagini dei container all'interno della console Amazon ECR. Inoltre, dalla console Amazon ECR puoi gestire la frequenza di scansione e affinare l'ambito delle scansioni creando filtri di inclusione.

Attivazione dell'integrazione

Puoi attivare l'integrazione attivando la scansione di Amazon Inspector tramite la console o l'API di Amazon Inspector oppure configurando il tuo repository per utilizzare la scansione avanzata con Amazon Inspector tramite la console o l'API Amazon ECR.

Per ulteriori informazioni sull'attivazione dell'integrazione tramite Amazon Inspector, consulta. Scansione automatizzata delle risorse con Amazon Inspector

Per informazioni sull'attivazione e la configurazione della scansione avanzata in Amazon ECR, consulta Enhanced Scanning nella guida per l'utente di Amazon ECR.

Utilizzo dell'integrazione con un ambiente multi-account

Se sei un membro di un ambiente con più account, puoi attivare la scansione avanzata tramite Amazon ECR. Tuttavia, una volta attivato, può essere disattivato solo dall'amministratore delegato di Amazon Inspector. Se è disattivata, torna alla scansione di base. Per ulteriori informazioni, consulta Disattivazione di Amazon Inspector.

Integrazione di Amazon Inspector con AWS Security Hub

Security Hub offre una visione completa dello stato di sicurezza AWS e ti aiuta a controllare il tuo ambiente rispetto agli standard e alle best practice del settore della sicurezza. Security Hub raccoglie dati sulla sicurezza da tutti AWS gli account, i servizi e altri prodotti supportati. È possibile utilizzare le informazioni fornite per analizzare le tendenze in materia di sicurezza e identificare i problemi di sicurezza con la massima priorità.

L'integrazione di Amazon Inspector con Security Hub consente di inviare i risultati da Amazon Inspector a Security Hub. Security Hub può quindi includere tali risultati nella sua analisi della posizione di sicurezza.

Nel AWS Security Hub, i problemi di sicurezza vengono registrati come risultati. Alcuni risultati derivano da problemi rilevati da altri AWS servizi o da prodotti di terze parti. Security Hub dispone

inoltre di una serie di regole che utilizza per rilevare problemi di sicurezza e generare risultati. Security Hub fornisce strumenti per gestire i risultati da tutte queste fonti. È possibile visualizzare e filtrare gli elenchi dei risultati e visualizzare i dettagli dei risultati. Per ulteriori informazioni sui risultati in Security Hub, vedere Visualizzazione dei risultati nella Guida AWS Security Hub per l'utente. È inoltre possibile monitorare lo stato di un'indagine in un esito. Consulta Operazioni sui risultati nella Guida per l'utente di AWS Security Hub .

Tutti i risultati in Security Hub utilizzano un formato JSON standard chiamato AWS Security Finding Format (ASFF). L'ASFF include dettagli sull'origine del problema, sulle risorse interessate e sullo stato corrente del risultato. Consulta AWS Security Finding Format (ASFF) nella Guida per l'utente di AWS Security Hub .

Security Hub archivierà i risultati di Amazon Inspector una volta che tali risultati saranno stati risolti e chiusi in Amazon Inspector.

Visualizzazione dei risultati di Amazon Inspector in AWS Security Hub

I risultati di Amazon Inspector Classic e del nuovo Amazon Inspector sono disponibili nello stesso pannello di Security Hub. Tuttavia, puoi filtrare i risultati del nuovo Amazon Inspector aggiungendo un filtro `"aws/inspector/ProductVersion": "2"` alla barra dei filtri. L'aggiunta di questo filtro esclude i risultati di Amazon Inspector Classic dalla dashboard di Security Hub.

Esempio di ricerca da Amazon Inspector


```
{
  "SchemaVersion": "2018-10-08",
  "Id": "arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/inspector",
  "ProductName": "Inspector",
  "CompanyName": "Amazon",
  "Region": "us-east-1",
  "GeneratorId": "AWSInspector",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Checks/Vulnerabilities/CVE"
  ],
  "FirstObservedAt": "2023-01-31T20:25:38Z",
  "LastObservedAt": "2023-05-04T18:18:43Z",
  "CreatedAt": "2023-01-31T20:25:38Z",
  "UpdatedAt": "2023-05-04T18:18:43Z",
  "Severity": {
    "Label": "HIGH",
```

```
    "Normalized": 70
   },
   "Title": "CVE-2022-34918 - kernel",
   "Description": "An issue was discovered in the Linux kernel through 5.18.9. A type
  confusion bug in nft_set_elem_init (leading to a buffer overflow) could be used by a
  local attacker to escalate privileges, a different vulnerability than CVE-2022-32250.
  (The attacker can obtain root access, but must start with an unprivileged user
  namespace to obtain CAP_NET_ADMIN access.) This can be fixed in nft_setelem_parse_data
  in net/netfilter/nf_tables_api.c.",
   "Remediation": {
     "Recommendation": {
       "Text": "Remediation is available. Please refer to the Fixed version in the
  vulnerability details section above. For detailed remediation guidance for each of the
  affected packages, refer to the vulnerabilities section of the detailed finding JSON."
     }
   },
   "ProductFields": {
     "aws/inspector/FindingStatus": "ACTIVE",
     "aws/inspector/inspectorScore": "7.8",
     "aws/inspector/resources/1/resourceDetails/awsEc2InstanceDetails/platform":
  "AMAZON_LINUX_2",
     "aws/inspector/ProductVersion": "2",
     "aws/inspector/instanceId": "i-0f1ed287081bdf0fb",
     "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/inspector/
  arn:aws:inspector2:us-east-1:123456789012:finding/FINDING_ID",
     "aws/securityhub/ProductName": "Inspector",
     "aws/securityhub/CompanyName": "Amazon"
   },
   "Resources": [
     {
       "Type": "AwsEc2Instance",
       "Id": "arn:aws:ec2:us-east-1:123456789012:i-0f1ed287081bdf0fb",
       "Partition": "aws",
       "Region": "us-east-1",
       "Tags": {
         "Patch Group": "SSM",
         "Name": "High-SEv-Test"
       },
       "Details": {
         "AwsEc2Instance": {
           "Type": "t2.micro",
           "ImageId": "ami-0cff7528ff583bf9a",
           "IpV4Addresses": [
             "52.87.229.97",
```

```
            "172.31.57.162"
          ],
          "KeyName": "ACloudGuru",
          "IamInstanceProfileArn": "arn:aws:iam::123456789012:instance-profile/
AmazonSSMRoleForInstancesQuickSetup",
          "VpcId": "vpc-a0c2d7c7",
          "SubnetId": "subnet-9c934cb1",
          "LaunchedAt": "2022-07-26T21:49:46Z"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "Vulnerabilities": [
    {
      "Id": "CVE-2022-34918",
      "VulnerablePackages": [
        {
          "Name": "kernel",
          "Version": "5.10.118",
          "Epoch": "0",
          "Release": "111.515.amzn2",
          "Architecture": "X86_64",
          "PackageManager": "OS",
          "FixedInVersion": "0:5.10.130-118.517.amzn2",
          "Remediation": "yum update kernel"
        }
      ],
      "Cvss": [
        {
          "Version": "2.0",
          "BaseScore": 7.2,
          "BaseVector": "AV:L/AC:L/Au:N/C:C/I:C/A:C",
          "Source": "NVD"
        },
        {
          "Version": "3.1",
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD"
```

```
        },
        {
          "Version": "3.1",
          "BaseScore": 7.8,
          "BaseVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H",
          "Source": "NVD",
          "Adjustments": []
        }
      ],
      "Vendor": {
        "Name": "NVD",
        "Url": "https://nvd.nist.gov/vuln/detail/CVE-2022-34918",
        "VendorSeverity": "HIGH",
        "VendorCreatedAt": "2022-07-04T21:15:00Z",
        "VendorUpdatedAt": "2022-10-26T17:05:00Z"
      },
      "ReferenceUrls": [
        "https://git.kernel.org/pub/scm/linux/kernel/git/netdev/net.git/commit/?
id=7e6bc1f6cabcd30aba0b11219d8e01b952eacbb6",
        "https://lore.kernel.org/netfilter-devel/cd9428b6-7ffb-dd22-d949-
d86f4869f452@randorisec.fr/T/",
        "https://www.debian.org/security/2022/dsa-5191"
      ],
      "FixAvailable": "YES"
    }
  ],
  "FindingProviderFields": {
    "Severity": {
      "Label": "HIGH"
    },
    "Types": [
      "Software and Configuration Checks/Vulnerabilities/CVE"
    ]
  },
  "ProcessedAt": "2023-05-05T20:28:38.822Z"
}
```


Attivazione e configurazione dell'integrazione

Per utilizzare l'integrazione con Amazon Inspector AWS Security Hub, devi attivare Security Hub. Per informazioni su come attivare Security Hub, vedere Configurazione del Security Hub nella Guida per l'AWS Security Hub utente.

Quando attivi sia Amazon Inspector che Security Hub, l'integrazione viene attivata automaticamente e Amazon Inspector inizia a inviare i risultati a Security Hub. Amazon Inspector invia tutti i risultati generati a Security Hub utilizzando il AWS Security Finding Format (ASFF).

Interruzione della pubblicazione dei risultati a AWS Security Hub

Come interrompere l'invio dei risultati

Per interrompere l'invio dei risultati a Security Hub, puoi utilizzare la console o l'API di Security Hub.

Vedi Disattivazione e attivazione del flusso di risultati da un'integrazione (console) o Disattivazione del flusso di risultati da un'integrazione (API Security Hub AWS CLI) nella Guida per l'utente.AWS Security Hub

Sistemi operativi e linguaggi di programmazione supportati da Amazon Inspector

Amazon Inspector può scansionare le applicazioni software installate sulle istanze Amazon Elastic Compute Cloud (Amazon EC2), le immagini dei container archiviate nei repository Amazon Elastic Container Registry (Amazon ECR) e le funzioni. AWS Lambda Per le immagini dei container ECR, Amazon Inspector è in grado di rilevare le vulnerabilità del sistema operativo e dei pacchetti del linguaggio di programmazione. Per le funzioni Lambda, Amazon Inspector può scansionare le vulnerabilità del codice. Quando Amazon Inspector analizza le risorse, utilizza il proprio motore di scansione appositamente progettato e raccoglie più di 50 feed di dati per generare risultati relativi a vulnerabilità ed esposizioni comuni (CVE). Le fonti includono avvisi di sicurezza dei fornitori, NVD, MITRE, feed open source, ricerche interne e feed di dati con licenza.

Affinché Amazon Inspector esegua la scansione di una risorsa, la risorsa deve eseguire un sistema operativo supportato o utilizzare un linguaggio di programmazione supportato. Gli argomenti di questa sezione elencano i sistemi operativi, i runtime e i linguaggi di programmazione attualmente supportati da Amazon Inspector per diverse risorse e tipi di scansione. Sono inoltre elencati i sistemi operativi che Amazon Inspector supportava in precedenza, ma che da allora sono stati interrotti dai fornitori. Amazon Inspector può fornire solo un supporto limitato per un sistema operativo dopo che un fornitore ha interrotto il supporto per il sistema operativo.

Argomenti

Sistemi operativi supportati: Amazon EC2 scanning

La tabella seguente elenca i sistemi operativi attualmente supportati da Amazon Inspector per le scansioni delle istanze Amazon EC2. Elenca inoltre la fonte degli avvisi di sicurezza del fornitore per ciascuna di esse e indica se il sistema operativo può essere scansionato utilizzando il metodo di scansione basato su agenti o senza agente. Per ulteriori informazioni sui metodi di scansione, vedere e. Scansione basata su agenti Scansione senza agenti

> **Note**
>
> I rilevamenti del sistema operativo Linux sono supportati solo per l'archivio predefinito del gestore di pacchetti e non includono applicazioni di terze parti, repository di supporto esteso (ad esempio, BYOS RHEL, PAYG RHEL e RHEL per SAP) e repository opzionali, come Red Hat Application Streams.

Sistema operativo	Versione	Avvisi di sicurezza dei fornitori	Supporto per la scansione senza agente	Supporto per la scansione basato su agenti
AlmaLinux	8	AHIMÈ	Sì	Sì
AlmaLinux	9	AHIMÈ	Sì	Sì
Amazon Linux (AL2)	AL2	AHIMÈ	Sì	Sì
Amazon Linux 2023 (AL2023)	AL2023	AHIMÈ	Sì	Sì
Bottlerocket	1.7.0 e versioni successive	OGHSA, CVE	No	Sì
CentOS Linux (CentOS)	7	CESA	Sì	Sì
Server Debian (Buster)	10	DSA	Sì	Sì

Sistema operativo	Versione	Avvisi di sicurezza dei fornitori	Supporto per la scansione senza agente	Supporto per la scansione basato su agenti
Server Debian (Bullseye)	11	DSA	Sì	Sì
Server Debian (Bookworm)	12	DSA	Sì	Sì
Fedora	38	CVE	Sì	Sì
Fedora	39	CVE	Sì	Sì
OpenSUSE	15.5	CVE	Sì	Sì
Oracle Linux (Oracle)	7	ELSA	Sì	Sì
Oracle Linux (Oracle)	8	ELSA	Sì	Sì
Oracle Linux (Oracle)	9	ELSA	Sì	Sì
Red Hat Enterprise Linux (RHEL)	7	RISSA	Sì	Sì
Red Hat Enterprise Linux (RHEL)	8	RHSA	Sì	Sì
Red Hat Enterprise Linux (RHEL)	9	RHSA	Sì	Sì
Rocky Linux	8	RLSA	Sì	Sì
Rocky Linux	9	RLSA	Sì	Sì

Sistema operativo	Versione	Avvisi di sicurezza dei fornitori	Supporto per la scansione senza agente	Supporto per la scansione basato su agenti
SUSE Linux Enterprise Server (SLES)	12.4	SUSE COVE	Sì	Sì
SUSE Linux Enterprise Server (SLES)	12,5	SUSE COVE	Sì	Sì
SUSE Linux Enterprise Server (SLES)	15.3	UNA GROTTA DI SUUSE	Sì	Sì
SUSE Linux Enterprise Server (SLES)	15.4	UNA GROTTA DI SUUSE	Sì	Sì
SUSE Linux Enterprise Server (SLES)	15,5	UNA GROTTA DI SUUSE	Sì	Sì
Ubuntu (affidabile)	14.04 (ESM)	USN, Ubuntu Pro	Sì	Sì
Ubuntu (Xenial)	16.04 (SEM)	USN, Ubuntu Pro	Sì	Sì
Ubuntu (Bionico)	18.04 (SECONDI)	USN, Ubuntu Pro	Sì	Sì
Ubuntu (focale)	20.04 (LITRI)	SOLE	Sì	Sì
Ubuntu (Jammy)	22.04 (LITRI)	SOLE	Sì	Sì

Sistema operativo	Versione	Avvisi di sicurezza dei fornitori	Supporto per la scansione senza agente	Supporto per la scansione basato su agenti
Ubuntu (Minotauro Mantico)	23.10	SOLE	Sì	Sì
Windows Server	2016	MSKB	No	Sì
Windows Server	2019	MSKB	No	Sì
Windows Server	2022	MSKB	No	Sì
macOS (Mojave)	10.14	APPLE-SV	No	Sì
macOS (Catalina)	10.15	APPLE-IT	No	Sì
macOS (Big Sur)	11	APPLE-SV	No	Sì
macOS (Monterey)	12	APPLE-SV	No	Sì
macOS (Ventura)	13	APPLE-SA	No	Sì

Linguaggi di programmazione supportati: Amazon EC2 deep inspection

Amazon Inspector attualmente supporta i seguenti linguaggi di programmazione durante la scansione delle istanze Amazon EC2 Linux alla ricerca di vulnerabilità nei pacchetti software di terze parti:

- Java
- JavaScript
- Python

Amazon Inspector utilizza Systems Manager Distributor per distribuire il plug-in utilizzato per l'ispezione approfondita nell'istanza Amazon EC2. Systems Manager Distributor supporta i sistemi operativi elencati come Piattaforme e architetture di pacchetti supportate nella guida Systems Manager. Il sistema operativo dell'istanza Amazon EC2 deve essere supportato da Systems Manager Distributor e Amazon Inspector for Amazon Inspector per Amazon Inspector per eseguire scansioni di ispezione approfondite.

> **Note**
>
> L'ispezione approfondita non è supportata per i sistemi operativi Bottlerocket.

Sistemi operativi supportati: scansione CIS

La tabella seguente elenca i sistemi operativi attualmente supportati da Amazon Inspector per le scansioni CIS. La tabella include anche la versione di benchmark CIS utilizzata per eseguire scansioni di quel sistema operativo.

Sistema operativo	Versione	Versione benchmark CIS
Amazon Linux 2	AL2	2.0.0
Amazon Linux 2023	AL2023	1.0.0
Windows Server	2019	2.0.0
Windows Server	2022	2.0.0

Sistemi operativi supportati: scansione Amazon ECR con Amazon Inspector

Amazon Inspector attualmente supporta la scansione dei seguenti sistemi operativi durante la scansione delle immagini dei container nei repository Amazon ECR:. La tabella elenca anche la fonte degli avvisi di sicurezza del fornitore per ciascun sistema operativo.

Sistema operativo	Versione	Avvisi di sicurezza dei fornitori
Alpine Linux (Alpine)	3.16	Alpine SecDB
Alpine Linux (Alpine)	3.17	Alpine SecDB
Alpine Linux (Alpine)	3.18	Alpine SecDB
Alpine Linux (Alpine)	3.19	Alpine SecDB
AlmaLinux	8	ALSA
AlmaLinux	9	ALSA
Amazon Linux (AL2)	AL2	ALAS
Amazon Linux 2023 (AL2023)	AL2023	ALAS
CentOS Linux (CentOS)	7	CESA
Debian Server (Buster)	10	DSA
Debian Server (Bullseye)	11	DSA
Debian Server (Bookworm)	12	DSA
Fedora	38	CVE
Fedora	39	CVE
OpenSUSE	15.5	CVE
Oracle Linux (Oracle)	7	ELSA
Oracle Linux (Oracle)	8	ELSA
Oracle Linux (Oracle)	9	ELSA
Photon OS	3	PHSA
Photon OS	4	PHSA

Sistema operativo	Versione	Avvisi di sicurezza dei fornitori
Photon OS	5	PHSA
Red Hat Enterprise Linux (RHEL)	7	RHSA
Red Hat Enterprise Linux (RHEL)	8	RHSA
Red Hat Enterprise Linux (RHEL)	9	RHSA
Rocky Linux	8	RLSA
Rocky Linux	9	RLSA
SUSE Linux Enterprise Server (SLES)	12.4	SUSE CVE
SUSE Linux Enterprise Server (SLES)	12.5	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.3	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.4	SUSE CVE
SUSE Linux Enterprise Server (SLES)	15.5	SUSE CVE
Ubuntu (Trusty)	14.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Xenial)	16.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Bionic)	18.04 (ESM)	USN, Ubuntu Pro
Ubuntu (Focal)	20.04 (LTS)	USN
Ubuntu (Jammy)	22.04 (LTS)	USN

Sistema operativo	Versione	Avvisi di sicurezza dei fornitori
Ubuntu (Mantic Minotaur)	23.10	USN

Linguaggi di programmazione supportati: Amazon ECR scanning

Amazon Inspector attualmente supporta i seguenti linguaggi di programmazione per la scansione delle immagini dei container nei repository Amazon ECR:

- C#
- Go
- Java
- JavaScript
- PHP
- Python
- Ruby
- Rust

Runtime supportati: scansione standard di Amazon Inspector Lambda

La scansione standard di Amazon Inspector Lambda attualmente supporta i seguenti linguaggi di programmazione durante la scansione delle funzioni Lambda alla ricerca di vulnerabilità nei pacchetti software di terze parti:

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x
  - nodejs14.x

- nodejs16.x
- nodejs18.x
- nodejs20.x

- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Go
  - go1.x
- Ruby
  - ruby2.7
  - ruby3.2
- .NET
  - .NET 6

Runtime supportati: scansione del codice Amazon Inspector Lambda

La scansione del codice Amazon Inspector Lambda attualmente supporta i seguenti linguaggi di programmazione durante la scansione delle funzioni Lambda alla ricerca di vulnerabilità nel codice:

- Java
  - java8
  - java8.al2
  - java11
  - java17
- Node.js
  - nodejs12.x
  - nodejs14.x

  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
- Ruby
  - ruby2.7
  - ruby3.2

Sistemi operativi fuori produzione

Il supporto standard del fornitore per i sistemi operativi elencati nelle tabelle seguenti è stato interrotto dal fornitore. Nelle tabelle, la colonna Interrotto indica quando il fornitore ha interrotto il supporto standard per un sistema operativo.

Amazon Inspector in precedenza forniva il supporto completo per questi sistemi operativi e continuerà a scansionare le istanze Amazon EC2 e le immagini dei container Amazon ECR che le eseguono. Tuttavia, in conformità alla politica dei fornitori, i sistemi operativi non vengono più aggiornati con patch e, in molti casi, non vengono più rilasciati nuovi avvisi di sicurezza relativi a tali sistemi. Inoltre, alcuni fornitori rimuovono gli avvisi e i rilevamenti di sicurezza esistenti dai propri feed quando un sistema operativo interessato raggiunge la fine del supporto standard. Di conseguenza, Amazon Inspector potrebbe smettere di generare risultati per i CVE noti. Qualsiasi risultato generato da Amazon Inspector per un sistema operativo fuori produzione deve essere utilizzato solo a scopo informativo.

Come best practice di sicurezza e per una copertura continua di Amazon Inspector, ti consigliamo di passare a una versione corrente e supportata di un sistema operativo.

Sistemi operativi fuori produzione: scansione Amazon EC2

Sistema operativo	Versione	Discontinuo
Amazon Linux (AL1)	2012	31 dicembre 2021
CentOS Linux (CentOS)	8	31 dicembre 2021
Server Debian (Stretch)	9	30 giugno 2022
Fedora	35	13 dicembre 2022
Fedora	36	16 maggio 2023
Fedora	37	5 dicembre 2023
OpenSUSE	15.3	1 dicembre 2022
OpenSUSE	15.4	7 dicembre 2023
openSUSE Leap (SUSE Leap)	15.2	1° dicembre 2021
Oracle Linux (Oracle)	6	1 marzo 2021
SUSE Linux Enterprise Server (SLES)	12	1 luglio 2019
SUSE Linux Enterprise Server (SLES)	12.1	31 maggio 2020
SUSE Linux Enterprise Server (SLES)	12.2	31 marzo 2021
SUSE Linux Enterprise Server (SLES)	12.3	30 giugno 2022
SUSE Linux Enterprise Server (SLES)	15	31 dicembre 2019
SUSE Linux Enterprise Server (SLES)	15.1	31 gennaio 2021

Sistema operativo	Versione	Discontinuo
SUSE Linux Enterprise Server (SLES)	15.2	31 dicembre 2021
Ubuntu (Groovy)	20.10	22 luglio 2021
Ubuntu (Hirsute)	21.04	20 gennaio 2022
Ubuntu (Impish)	21.10	31 luglio 2022
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024
Windows Server	2012	10 ottobre 2023
Windows Server	2012 R2	10 ottobre 2023

Sistemi operativi fuori produzione: Amazon ECR scanning

Sistema operativo	Versione	Discontinuo
Alpine Linux (Alpine)	3.12	1 maggio 2022
Alpine Linux (Alpine)	3.13	1 novembre 2022
Alpine Linux (Alpine)	3.14	May 1, 2023
Alpine Linux (Alpine)	3.15	November 1, 2023
Amazon Linux (AL1)	2012	31 dicembre 2021
CentOS Linux (CentOS)	8	31 dicembre 2021
Server Debian (Stretch)	9	30 giugno 2022
Fedora	35	13 dicembre 2022
Fedora	36	16 maggio 2023

Sistema operativo	Versione	Discontinuo
OpenSUSE	15.3	1 dicembre 2022
OpenSUSE	15.4	December 7, 2023
openSUSE Leap (SUSE Leap)	15.2	1° dicembre 2021
Oracle Linux (Oracle)	6	1 marzo 2021
SUSE Linux Enterprise Server (SLES)	12	1 luglio 2019
SUSE Linux Enterprise Server (SLES)	12.1	31 maggio 2020
SUSE Linux Enterprise Server (SLES)	12.2	31 marzo 2021
SUSE Linux Enterprise Server (SLES)	12.3	30 giugno 2022
SUSE Linux Enterprise Server (SLES)	15	31 dicembre 2019
SUSE Linux Enterprise Server (SLES)	15.1	31 gennaio 2021
SUSE Linux Enterprise Server (SLES)	15.2	31 dicembre 2021
Ubuntu (Groovy)	20.10	22 luglio 2021
Ubuntu (Hirsute)	21.04	20 gennaio 2022
Ubuntu (Impish)	21.10	31 luglio 2022
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024

Disattivazione di Amazon Inspector

Puoi disattivare Amazon Inspector da Regione AWS qualsiasi dispositivo utilizzando la console o l'API di Amazon Inspector. Segui le istruzioni alla fine di questo argomento per disattivare Amazon Inspector. Se disattivi tutte le scansioni Amazon Inspector per un account, Account AWS Amazon Inspector viene disattivato automaticamente per questo account. Per informazioni sulla disattivazione dei tipi di scansione per diverse risorse, consulta. Scansione automatizzata delle risorse con Amazon Inspector

Dopo la disattivazione di Amazon Inspector per un account, tutti i tipi di scansione vengono disattivati per quell'account in quella regione. Inoltre, tutte le impostazioni di scansione, le regole di soppressione, i filtri e i risultati di Amazon Inspector per l'account in quella regione vengono eliminati.

Non ti viene addebitato alcun costo per l'utilizzo di Amazon Inspector mentre è disattivato per il tuo account in quella regione. Dopo aver disattivato Amazon Inspector, puoi scegliere di riattivarlo in un secondo momento.

> **Note**
>
> Prima di disattivare Amazon Inspector, ti consigliamo di esportare i risultati. Per ulteriori informazioni, consulta Esportazione dei report dei risultati da Amazon Inspector.

Quando disattivi la scansione di Amazon Inspector Amazon EC2, vengono eliminate le seguenti associazioni SSM utilizzate da Amazon Inspector:

- `InspectorDistributor-do-not-delete`
- `InspectorInventoryCollection-do-not-delete`
- `InvokeInspectorSsmPlugin-do-not-delete`. Inoltre, il plug-in Amazon Inspector SSM installato tramite questa associazione viene rimosso da tutti i tuoi host. Windows Per ulteriori informazioni, consulta Scansione Windows delle istanze.

Prerequisiti

A seconda del tipo di account, potrebbe essere necessario eseguire ulteriori passaggi prima di disattivare Amazon Inspector come segue:

- Se disponi di un account Amazon Inspector autonomo, puoi disattivarlo in qualsiasi momento.
- Se sei un account membro in un ambiente con più account Amazon Inspector, non puoi disattivare il tuo servizio. Devi contattare l'amministratore delegato della tua organizzazione per disattivare il servizio.
- Se sei un amministratore delegato, devi dissociare tutti i tuoi account membro prima di poter disattivare Amazon Inspector. Per ulteriori informazioni, consulta Dissociazione degli account dei membri in Amazon Inspector.

> **Note**
>
> La dissociazione di un account non disattiva Amazon Inspector per quell'account, ma un account membro dissociato diventa un account autonomo.

> **Note**
>
> Quando disattivi Amazon Inspector come amministratore delegato, la funzionalità di attivazione automatica viene disattivata per la tua organizzazione.

Disattiva Amazon Inspector

Console

Per disattivare Amazon Inspector

1. Apri la console Amazon Inspector all'indirizzo https://console.aws.amazon.com/inspector/v2/home.
2. Utilizzando il Regione AWS selettore nell'angolo superiore destro della pagina, scegli la regione in cui desideri disattivare Amazon Inspector.
3. Nel pannello di navigazione, scegli Impostazioni generali.
4. Scegliete Disattiva Inspector.
5. Quando viene richiesta la conferma, immettete disactivate nella casella di testo, quindi scegliete Deactivate Inspector.
6. (Consigliato) Ripeti questi passaggi in ogni regione per cui desideri disattivare Amazon Inspector.

API

Esegui l'operazione Disable API. Nella richiesta, fornisci gli ID dell'account che stai disattivando e `EC2, ECR, LAMBDA` se desideri `resourceTypes` disattivare tutte le scansioni, l'account verrà disattivato.

Quote per Amazon Inspector

Il tuo AWS account ha le seguenti quote per Amazon Inspector per regione.

Risorsa	Default	Commenti
Regole di eliminazione	500	Il numero massimo di regole di soppressi one salvate per AWS account per regione. Non è possibile richiedere un aumento della quota.
Risultati della rete Amazon EC2	10.000	Il numero massimo di risultati di rete Amazon EC2 per account. AWS Non è possibile richiedere un aumento della quota.
Account membri	10000	Il numero massimo di account membro associati a un account amministratore delegato di Amazon Inspector. Questo limite si basa su AWS Organizations, consulta Quotas for. AWS Organizations
Configurazioni di scansione CIS	500	Il numero massimo di configurazioni di scansione CIS.

Risorsa	Default	Commenti
		Non è possibile richiedere un aumento della quota.

Per un elenco delle quote associate ad Amazon Inspector Classic, consulta le quote del servizio Amazon Inspector nel. Riferimenti generali di AWS

Per un elenco delle quote associate a Organizations, vedere Organizations service quotas in. Riferimenti generali di AWS

Regioni ed endpoint

La scansione senza agenti di Amazon Inspector per Amazon EC2 è disponibile in anteprima. L'utilizzo della funzionalità di scansione senza agenti di Amazon EC2 è soggetto alla Sezione 2 dei Termini di AWS servizio («Beta e anteprime»).

Per visualizzare Regioni AWS dove è disponibile Amazon Inspector, consulta gli endpoint Amazon Inspector nel. Riferimenti generali di Amazon Web Services

Endpoint per l'API Amazon Inspector Scan

La tabella seguente mostra gli endpoint regionali che possono essere utilizzati per chiamare l'API Amazon Inspector Scan. Quando utilizzi l'API, devi fornire l'endpoint e la regione corrispondente alla regione in cui sei attualmente autenticato. AWS

La convenzione di denominazione per gli endpoint Amazon Inspector Scan è. `inspector-scan.`*`region`*`.amazonaws.com` Ad esempio, se sei autenticato in`us-west-2`, utilizzerai l'endpoint per chiamare l'API`inspector-scan.us-west-2.amazonaws.com`. `inspector-scan`

Nome della regione	Regione	Endpoint	Protocollo
Stati Uniti orientali (Ohio)	us-east-2	inspector-scan.us-east-2.amazonaws.com inspector-scan-fips.us-east-2.amazonaws.com	HTTPS
US East (N. Virginia)	us-east-1	inspector-scan.us-east-1.amazonaws.com inspector-scan-fips.us-east-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
US West (N. California)	us-west-1	inspector-scan.us-west-1.amazonaws.com inspector-scan-fips.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	inspector-scan.us-west-2.amazonaws.com inspector-scan-fips.us-west-2.amazonaws.com	HTTPS
Africa (Cape Town)	af-south-1	inspector-scan.af-south-1.amazonaws.com	HTTPS
Asia Pacifico (Hong Kong)	ap-east-1	inspector-scan.ap-east-1.amazonaws.com	HTTPS
Asia Pacifico (Giacarta)	ap-southeast-3	inspector-scan.ap-southeast-3.amazonaws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	inspector-scan.ap-south-1.amazonaws.com	HTTPS
Asia Pacifico (Osaka-Locale)	ap-northeast-3	inspector-scan.ap-northeast-3.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Seul)	ap-northeast-2	inspector-scan.ap-northeast-2.amazonaws.com	HTTPS
Asia Pacific (Singapore)	ap-southeast-1	inspector-scan.ap-southeast-1.amazonaws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	inspector-scan.ap-southeast-2.amazonaws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	inspector-scan.ap-northeast-1.amazonaws.com	HTTPS
Canada (Central)	ca-central-1	inspector-scan.ca-central-1.amazonaws.com	HTTPS
Europe (Frankfurt)	eu-central-1	inspector-scan.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	inspector-scan.eu-west-1.amazonaws.com	HTTPS
Europe (London)	eu-west-2	inspector-scan.eu-west-2.amazonaws.com	HTTPS
Europa (Milano)	eu-south-1	inspector-scan.eu-south-1.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Europe (Paris)	eu-west-3	inspector-scan.eu-west-3.amazonaws.com	HTTPS
Europa (Stoccolma)	eu-north-1	inspector-scan.eu-north-1.amazonaws.com	HTTPS
Europa (Zurigo)	eu-central-2	inspector-scan.eu-central-2.amazonaws.com	HTTPS
Medio Oriente (Bahrein)	me-south-1	inspector-scan.me-south-1.amazonaws.com	HTTPS
Sud America (São Paulo)	sa-east-1	inspector-scan.sa-east-1.amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	ispector-scan. us-gov-east-1. amazonaws.com inspector-scan-fips. us-gov-east-1. amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	ispector-scan. us-gov-west-1. amazonaws.com inspector-scan-fips. us-gov-west-1. amazonaws.com	HTTPS

Disponibilità di funzionalità specifiche per ogni regione

Questa sezione descrive la disponibilità delle funzionalità di Amazon Inspector di. Regione AWS

Scansione EC2 senza agente per le regioni Amazon EC2

La tabella seguente mostra Regioni AWS dove è attualmente disponibile la scansione senza agente per Amazon EC2.

Nome della regione	Codice regione
US East (N. Virginia)	us-east-1
US West (Oregon)	us-west-2
Europa (Irlanda)	eu-west-1

Regioni di scansione del codice Lambda

La tabella seguente mostra Regioni AWS dove è attualmente disponibile la scansione del codice Lambda.

Nome della regione	Codice regione
US East (N. Virginia)	us-east-1
US West (Oregon)	us-west-2
Stati Uniti orientali (Ohio)	us-east-2
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacific (Tokyo)	ap-northeast-1
Europe (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2

Nome della regione	Codice regione
Europa (Stoccolma)	eu-north-1
Asia Pacific (Singapore)	ap-southeast-1

AWS GovCloud (US) Regioni

Per le informazioni più recenti, consulta Amazon Inspector nella Guida per l'AWS GovCloud (US) utente.

Cronologia dei documenti per la Amazon Inspector User Guide

La tabella seguente descrive le modifiche importanti alla documentazione dall'ultima versione di Amazon Inspector. Per ricevere notifiche sugli aggiornamenti di questa documentazione, puoi abbonarti a un feed RSS.

Modifica	Descrizione	Data
Funzionalità aggiornate	Amazon Inspector aggiorna il periodo di conservazione dei risultati chiusi da 30 giorni a 7 giorni. Per ulteriori informazioni, consulta Comprendere i risultati in Amazon Inspector.	12 febbraio 2024
Funzionalità aggiornate	Amazon Inspector ha aggiunto una nuova dichiarazione alla AmazonInspector2ServiceRolePolicy policy. La nuova istruzione consente ad Amazon Inspector di avviare scansioni CIS per la tua istanza.	23 gennaio 2024
Nuova politica	Amazon Inspector ha aggiunto una nuova policy, la AmazonInspector2ManagedCisPolicypolicy, che puoi utilizzare come parte di un profilo di istanza per consentire le scansioni CIS su un'istanza.	23 gennaio 2024
Nuova funzionalità	Amazon Inspector ora aggiornerà la durata della	23 gennaio 2024

	nuova scansione ECR delle immagini dei container quando le estrai. Per modificare la durata della nuova scansione in base alle date di push o pull, consulta Configurazione della durata della nuova scansione ECR.	
Nuova funzionalità	Amazon Inspector ora può eseguire scansioni di Center for Internet Security (CIS) su istanze EC2. Per ulteriori informazioni, consulta Scansioni CIS di Amazon Inspector.	23 gennaio 2024
Nuova funzionalità	Amazon Inspector ora può scansionare le immagini dei container nelle tue pipeline CI/CD. Per ulteriori informazioni, consulta Integrazione CI/CD con Amazon Inspector.	30 novembre 2023
Nuova politica	Amazon Inspector ha aggiunto una nuova policy che consente ad Amazon Inspector di scansionare le istantanee di Amazon EBS dall'istanza EC2 per una scansione senza agenti. Per ulteriori informazioni sulla politica, consulta Agentless scanning.	27 novembre 2023

Nuova funzionalità	Amazon Inspector ora supporta la scansione delle istanze Linux Amazon EC2 supportate senza agenti SSM tramite la scansione senza agenti. Per ulteriori informazioni, consulta la sezione Scansione senza agente.	27 novembre 2023
Nuove risorse supportate	Amazon Inspector ora supporta la scansione di istanze Amazon EC2 per macOS. Vedi Sistemi operativi supportati: scansione di Amazon EC2 per le versioni macOS supportate.	5 ottobre 2023
Nuove regioni	Amazon Inspector è ora disponibile in Asia Pacifico (Giacarta), Africa (Città del Capo), Asia Pacifico (Osaka) ed Europa (Zurigo).	29 settembre 2023
Nuova caratteristica	Ora puoi escludere le istanze EC2 dalle scansioni di Amazon Inspector utilizzando i tag di esclusione.	14 settembre 2023
Nuova caratteristica	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono ad Amazon Inspector di scansionare le configurazioni di rete delle istanze Amazon EC2 che fanno parte dei gruppi target Elastic Load Balancing.	31 agosto 2023

Nuova caratteristica	Amazon Inspector ora fornisce dettagli di intelligence sulle vulnerabilità per rilevare le vulnerabilità dei pacchetti.	31 luglio 2023
Funzionalità aggiornate	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono agli utenti di sola lettura di esportare Software Bill of Materials (SBOM) per le proprie risorse.	29 giugno 2023
Nuova caratteristica	Ora puoi esportare SBOM per le risorse scansionate da Amazon Inspector.	13 giugno 2023
Nuova caratteristica	La scansione del codice Lambda è ora disponibile a livello generale. Sono state aggiunte nuove funzionalità che consentono di crittografare il codice identificato nei risultati della scansione del codice Lambda. Inoltre, la scansione del codice Lambda ora fornisce suggerimenti per correggere le riscritture del codice.	13 giugno 2023

Funzionalità aggiornate	Amazon Inspector ha aggiunto una nuova dichiarazione alla AmazonInspector2ReadOnlyAccess policy. Le nuove istruzioni consentono agli utenti di sola lettura di recuperare i dettagli dello stato e dei risultati della scansione del codice Lambda per il proprio account.	2 maggio 2023
Nuova caratteristica	Amazon Inspector ha aggiunto la ricerca nel database delle vulnerabilità che consente di verificare se Amazon Inspector copre un CVE specifico.	1 maggio 2023
Funzionalità aggiornate	Amazon Inspector ha aggiunto nuove autorizzazioni alla AmazonInspector2ServiceRolePolicypolicy che consentono ad Amazon Inspector di creare canali AWS CloudTrail collegati ai servizi nel tuo account quando attivi la scansione Lambda. Ciò consente ad Amazon Inspector di monitorare CloudTrail gli eventi nel tuo account.	30 aprile 2023

Funzionalità aggiornate	Amazon Inspector ha aggiunto una nuova dichiarazione alla AmazonInspector2FullAccess policy. La nuova dichiarazione consente agli utenti di recuperare i dettagli delle vulnerabilità del codice rilevate dalla scansione del codice Lambda.	17 aprile 2023
Funzionalità aggiornate	Amazon Inspector ha aggiunto una nuova dichiarazione alla AmazonInspector2ServiceRolePolicy policy. La nuova dichiarazione consente ad Amazon Inspector di inviare informazioni ad Amazon EC2 Systems Manager sui percorsi personalizzati che hai definito per l'ispezione approfondita di Amazon EC2.	17 aprile 2023
Nuova caratteristica	Amazon Inspector aggiunge supporto aggiuntivo per le istanze Linux EC2 sotto forma di Amazon Inspector deep inspection, che analizza le istanze alla ricerca di vulnerabilità dei pacchetti nei pacchetti di linguaggi di programmazione delle applicazioni.	17 aprile 2023

Funzionalità aggiornate	Amazon Inspector ha aggiunto una nuova dichiarazione alla AmazonInspector2ServiceRolePolicy policy. Le nuove istruzioni consentono ad Amazon Inspector di richiedere scansioni del codice di sviluppo nelle AWS Lambda funzioni e ricevere dati di scansione da Amazon Security. CodeGuru Inoltre, Amazon Inspector ha aggiunto le autorizzazioni per la revisione delle politiche IAM. Amazon Inspector utilizza queste informazioni per scansionare le funzioni Lambda alla ricerca di vulnerabilità del codice.	28 febbraio 2023
Nuova caratteristica	Amazon Inspector aggiunge un supporto aggiuntivo per le funzioni Lambda sotto forma di scansione del codice Lambda, che analizza il codice dello sviluppatore delle funzioni Lambda alla ricerca di vulnerabilità di sicurezza.	28 febbraio 2023

Funzionalità aggiornate	Amazon Inspector ha aggiunto una nuova dichiarazione alla AmazonInspector2ServiceRolePolicy policy. La nuova istruzione consente ad Amazon Inspector di recuperare informazioni CloudWatch sull'ultima volta che una AWS Lambda funzione è stata richiamata. Utilizza queste informazioni per concentrare le scansioni sulle funzioni Lambda del tuo ambiente che sono state attive negli ultimi 90 giorni.	20 febbraio 2023
Funzionalità aggiornate	Amazon Inspector ha aggiunto una nuova dichiarazione alla AmazonInspector2ServiceRolePolicy policy. La nuova dichiarazione consente ad Amazon Inspector di recuperare informazioni sulle tue funzioni. AWS Lambda Amazon Inspector utilizza queste informazioni per scansionare le funzioni Lambda alla ricerca di vulnerabilità di sicurezza.	28 novembre 2022
Nuova caratteristica	Amazon Inspector aggiunge il supporto per le funzioni di scansione AWS Lambda.	28 novembre 2022

Contenuti aggiornati	Sono state aggiunte procedure , esempi di policy e suggerime nti per esportare i report dei risultati da Amazon Inspector a un bucket Amazon Simple Storage Service (Amazon S3).	14 ottobre 2022
Nuovo contenuto	Sono state aggiunte informazi oni sulla valutazione della copertura di Amazon Inspector del AWS tuo ambiente utilizzando la console Amazon Inspector. Le informazioni includono descrizioni dei valori Status per le singole risorse del tuo ambiente.	7 ottobre 2022
Nuova caratteristica	Amazon Inspector ora fornisce ulteriori dettagli su come correggere le vulnerabilità dei pacchetti. Sono stati aggiunti nuovi campi per trovare i dettagli. I nuovi campi forniscono informazioni sulla disponibilità di una correzion e tramite un aggiornamento del pacchetto. Se è disponibi le una correzione, la sezione Correzione consigliata di un risultato mostra i comandi che è possibile eseguire per apportare la correzione.	2 settembre 2022

Funzionalità aggiornate	Amazon Inspector ha aggiunto una nuova azione alla AmazonInspector2ServiceRolePolicy policy. La nuova azione consente ad Amazon Inspector di descrivere le esecuzioni delle associazioni SSM. Amazon Inspector ha inoltre aggiunto un ulteriore ambito delle risorse per consentire ad Amazon Inspector di creare, aggiornare, eliminare e avviare associazioni SSM con documenti SSM di proprietà. `AmazonInspector2`	31 agosto 2022
Nuova caratteristica	Amazon Inspector ora supporta le scansioni delle istanze. Windows Amazon Inspector ora può scansionare le istanze gestite SSM che eseguono sistemi operativi supportati. Windows Le scansioni degli Windows host vengono eseguite dal plug-in Amazon Inspector SSM, che viene installato e richiamato tramite nuove associazioni SSM create automaticamente da Amazon Inspector.	31 agosto 2022

Funzionalità aggiornate	Amazon Inspector ha aggiornato l'ambito delle risorse della AmazonInspector2ServiceRolePolicypolicy per consentire ad Amazon Inspector di raccogliere l'inventario del software in altre partizioni. AWS	12 agosto 2022
Funzionalità aggiornate	Nella AmazonInspector2ServiceRolePolicypolicy, Amazon Inspector ha ristrutturato l'ambito delle risorse delle azioni che consentono ad Amazon Inspector di creare, eliminare e aggiornare le associazioni SSM.	10 agosto 2022

Nuova caratteristica	Amazon Inspector ora supporta la modifica dell'impostazione della durata della nuova scansione automatica ECR. L'impostazione della durata della nuova scansione automatica di Amazon ECR determina per quanto tempo Amazon Inspector monitora continuamente le immagini inserite nei repository. Quando un'immagine è più vecchia della durata della scansione, Amazon Inspector non scansionerà più l'immagine e chiuderà tutti i risultati esistenti. A tutti i nuovi account verrà automaticamente impostata la durata della nuova scansione automatica ECR su Durata. Gli account creati in precedenza avevano una durata di scansione automatica ECR di 30 giorni, ma ora puoi scegliere tra durate di 30 giorni, 180 giorni o a vita per le scansioni.	25 giugno 2022
Nuove funzionalità	Amazon Inspector ha aggiunto una nuova policy AWS gestita, la AmazonInspector2ReadOnlyAccesspolicy, per consentire l'accesso in sola lettura alle funzionalità di Amazon Inspector.	21 gennaio 2022

Disponibilità generale	Questa è la versione pubblica iniziale della Amazon Inspector User Guide.	29 novembre 2021

AWS Glossario

Per la AWS terminologia più recente, consultate il AWS glossario nella sezione Reference.Glossario AWS

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.