Guida per l'utente

Amazon Inspector

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

Amazon Inspector: Guida per l'utente

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

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

Table of Contents

Che cos'è Amazon Inspector? ... 1
Funzionalità ... 1
Accesso ad Amazon Inspector ... 3
Nozioni di base ... 5
Prima di attivare Amazon Inspector ... 5
Tutorial introduttivo: attivazione di Amazon Inspector ... 6
Scansioni automatiche ... 8
Panoramica dei tipi di scansione di Amazon Inspector ... 8
Attivazione di un tipo di scansione ... 10
Attivazione delle scansioni ... 11
Scansione delle EC2 istanze Amazon ... 12
Scansione basata su agenti ... 13
Scansione senza agenti ... 17
Gestione della modalità di scansione ... 19
Esclusione delle istanze dalle scansioni di Amazon Inspector ... 20
Sistemi operativi supportati ... 20
Ispezione approfondita per istanze Linux ... 21
Istanza di scansione Windows EC2 ... 26
Scansione delle immagini dei contenitori Amazon ECR ... 28
Comportamenti di scansione per la scansione Amazon ECR ... 29
Mappatura delle immagini dei container ai container in esecuzione ... 30
Sistemi operativi e tipi di supporti supportati ... 31
Configurazione della durata della nuova scansione di Amazon ECR ... 32
Funzione di scansione Lambda ... 35
Comportamenti di scansione per la scansione della funzione Lambda ... 35
Runtime e funzioni supportati ... 36
Scansione standard Amazon Inspector Lambda ... 37
Scansione del codice Amazon Inspector Lambda ... 38
Disattivazione di un tipo di scansione ... 40
Disattivazione delle scansioni ... 41
Scansioni CIS ... 43
Requisiti delle EC2 istanze Amazon per le scansioni CIS di Amazon Inspector ... 44
Requisiti degli endpoint Amazon Virtual Private Cloud per l'esecuzione di scansioni CIS su istanze Amazon private EC2 ... 45

Esecuzione di scansioni CIS ... 45
Considerazioni sulla gestione delle scansioni CIS di Amazon Inspector con AWS Organizations ... 46
Bucket Amazon S3 di proprietà di Amazon Inspector utilizzati per le scansioni CIS di Amazon Inspector ... 48
Creazione di una configurazione di scansione CIS ... 50
Visualizzazione dei risultati della scansione CIS ... 51
Modifica di una configurazione di scansione CIS ... 52
Scaricamento dei risultati di una scansione CIS ... 52
Codice di sicurezza di Amazon Inspector ... 54
Prerequisiti ... 54
Attivazione della sicurezza del codice ... 54
Creazione di una chiave di accesso gestita dal cliente AWS KMS ... 54
Creare un'integrazione ... 57
Creazione di un'integrazione per GitHub ... 58
Creazione di un'integrazione per GitLab Self Managed ... 60
Visualizzazione delle integrazioni ... 62
Visualizzazione degli archivi di codice ... 63
Eliminazione di un'integrazione ... 64
Creazione di una configurazione di scansione ... 64
Visualizzazione delle configurazioni di scansione ... 67
Modifica di una configurazione di scansione ... 68
Eliminazione di una configurazione di scansione ... 69
Esecuzione di una scansione su richiesta ... 69
Lingue supportate ... 69
Disattivazione di Code Security ... 71
Comprensione degli esiti ... 72
Tipi di esiti ... 73
Vulnerabilità del pacchetto ... 73
Vulnerabilità del codice ... 74
Raggiungibilità della rete ... 74
Visualizzazione dei risultati ... 75
Visualizzazione dei dettagli del risultato ... 77
Visualizzazione del punteggio di Amazon Inspector ... 80
Punteggio Amazon Inspector ... 81
Intelligenza sulla vulnerabilità ... 83

Comprensione dei livelli di gravità dei risultati ... 84
Gravità della vulnerabilità dei pacchetti software ... 84
Gravità della vulnerabilità del codice ... 85
Severità della raggiungibilità della rete ... 84
Gestione degli esiti ... 88
Filtro dei risultati ... 88
Creazione di filtri nella console Amazon Inspector ... 88
Eliminazione dei risultati ... 89
Creazione di una regola di soppressione ... 90
Visualizzazione dei risultati soppressi ... 90
Modifica di una regola di soppressione ... 91
Eliminazione di una regola di soppressione ... 91
Esportazione dei report sui risultati ... 92
Passaggio 1: verifica le tue autorizzazioni ... 93
Passaggio 2: configura un bucket S3 ... 95
Fase 3: Configurare un AWS KMS key ... 98
Fase 4: Configurare ed esportare un rapporto sui risultati ... 101
Risolvi gli errori ... 104
Automatizzazione delle risposte ai risultati con EventBridge ... 105
Schema degli eventi ... 105
Creazione di una EventBridge regola per notificarti i risultati di Amazon Inspector ... 108
EventBridge per ambienti con più account Amazon Inspector ... 112
Dashboard ... 113
Visualizzazione del pannello di controllo ... 113
Comprendere i componenti del dashboard ... 114
Ricerca nel database delle vulnerabilità ... 118
Ricerca nel database delle vulnerabilità ... 118
Comprendere i dettagli del CVE ... 119
Dettagli CVE ... 119
Intelligence sulle vulnerabilità ... 119
Riferimenti ... 119
Esportazione SBOMs ... 120
Formati Amazon Inspector ... 120
Filtri per SBOMs ... 125
Configura ed esporta SBOMs ... 126
EventBridge schema ... 129

Schema EventBridge di base Amazon per Amazon Inspector ... 129
Esempio di schema di eventi di ricerca di Amazon Inspector ... 130
Esempio di schema di eventi completo per la scansione iniziale di Amazon Inspector ... 142
Esempio di schema degli eventi di copertura di Amazon Inspector ... 145
Esempio di schema di attivazione automatica di Amazon Inspector ... 146
Plugin SSM ... 147
Il plug-in Amazon Inspector SSM per Linux ... 147
Disinstallazione del plug-in Amazon Inspector SSM ... 147
Il plug-in Amazon Inspector SSM per Windows ... 148
Disinstallazione del plug-in Amazon Inspector SSM ... 148
Generatore SBOM Amazon Inspector ... 150
Tipi di pacchetti supportati ... 150
Controlli di configurazione dell'immagine del contenitore supportati ... 150
Installazione di Sbomgen ... 151
Uso di Sbomgen ... 152
Genera un SBOM per un'immagine del contenitore e restituisci il risultato ... 152
Genera un SBOM da directory e archivi ... 154
Genera un SBOM da Go o Rust compilati file binari ... 154
Genera un SBOM dai volumi montati ... 154
Invia un SBOM ad Amazon Inspector per l'identificazione delle vulnerabilità ... 155
Utilizza scanner aggiuntivi per migliorare le capacità di rilevamento ... 157
Ottimizza le scansioni dei contenitori regolando la dimensione massima del file da scansionare ... 158
Disattiva l'indicatore di avanzamento ... 159
Autenticazione in registri privati con Sbomgen ... 159
Autenticazione tramite credenziali memorizzate nella cache (scelta consigliata) ... 160
Effettua l'autenticazione utilizzando il metodo interattivo ... 160
Effettua l'autenticazione utilizzando il metodo non interattivo ... 160
Esempi di risultati da Sbomgen ... 161
Versioni precedenti ... 163
Raccolta di sistemi operativi ... 168
Artefatti del sistema operativo supportati ... 169
Raccolta di pacchetti del sistema operativo basata su APK ... 170
Raccolta di pacchetti del sistema operativo basata su DPKG ... 171
Raccolta di pacchetti del sistema operativo basata su RPM ... 172
Raccolta di pacchetti di immagini Chainguard ... 173

Raccolta di pacchetti di immagini Distroless 174
Raccolta di pacchetti MiniMOS 175
Raccolta di dipendenze 176
Vai alla scansione delle dipendenze 177
Scansione delle dipendenze in Java 180
JavaScript scansione delle dipendenze 184
Scansione delle dipendenze.NET 190
Scansione delle dipendenze PHP 196
Scansione delle dipendenze in Python 199
Scansione delle dipendenze con Ruby 203
Scansione delle dipendenze da Rust 207
Artefatti non supportati 210
Raccolta di ecosistemi 211
Ecosistemi supportati 212
Apachecollezione ecosistemica 212
Javaraccolta di ecosistemi 214
Googleraccolta di ecosistemi 216
WordPressraccolta ecosistemica 218
Node.JSraccolta runtime 220
Collezione di ecosistemi OpenSSL 221
Raccolta di licenze 222
Raccogli informazioni sulla licenza 222
Pacchetti supportati 223
Package URLs 230
Struttura PURL 230
Riferimenti alle versioni 232
Raccomandazioni 232
Java 233
JavaScript 233
Python 233
Utilizzo CycloneDX namespace 234
`amazon:inspector:sbom_scanner`tassonomia dei namespace 234
`amazon:inspector:sbom_generator`tassonomia dello spazio dei nomi 236
Integrazione CI/CD 239
Integrazione con i plugin 239
Soluzioni supportate CI/CD 240

Integrazione personalizzata ... 240
Configura un account per l'integrazione CI/CD ... 241
Iscriviti a un Account AWS ... 242
Crea un utente con accesso amministrativo ... 242
Configura un ruolo IAM per l'integrazione CI/CD ... 243
Controlli dei file Dockerfile di Amazon Inspector ... 245
Utilizzo dei controlli Dockerfile Sbomgen ... 245
Controlli Dockerfile supportati ... 247
Creazione di un'integrazione CI/CD personalizzata ... 253
Fase 1: Configurazione Account AWS ... 254
Fase 2: Installazione Sbomgen del binario ... 254
Fase 3. Uso di Sbomgen ... 254
Fase 4. Chiamata dell'API Amazon Inspector Scan ... 254
(Facoltativo) Fase 5. Genera e scansiona SBOM con un solo comando ... 255
Formati di output delle API ... 255
Plugin Jenkins ... 263
Fase 1: Configura un Account AWS ... 264
Fase 2: Installa il plugin Amazon Inspector Jenkins ... 264
(Facoltativo) Fase 3. Aggiungi le credenziali docker a Jenkins ... 264
(Facoltativo) Fase 4. Aggiungere AWS credenziali ... 265
Fase 5. Aggiungi il supporto CSS in uno Jenkins script ... 265
Fase 6. Aggiungi Amazon Inspector Scan alla tua build ... 265
Fase 7. Visualizza il report sulla vulnerabilità di Amazon Inspector ... 269
Risoluzione dei problemi ... 270
TeamCity Plugin ... 272
Operazioni GitHub ... 274
GitLab componenti ... 274
Utilizzo delle operazioni CodeCatalyst ... 275
Utilizzo delle azioni di scansione di Amazon Inspector ... 275
Valutazione della copertura ... 276
Valutazione della copertura a livello di account ... 277
Valutazione della copertura delle istanze Amazon EC2 ... 277
Valori di stato EC2 delle istanze Amazon ... 278
Valutazione della copertura dei repository Amazon ECR ... 280
Valori dello stato di scansione del repository Amazon ECR ... 281
Valutazione della copertura delle immagini dei container Amazon ECR ... 282

Valori dello stato di scansione delle immagini dei contenitori Amazon ECR 283
Valutazione della copertura delle funzioni AWS Lambda 284
Le funzioni Lambda scansionano i valori dello stato 285
Gestione di più account 286
Informazioni sull'account amministratore delegato e sull'account membro 286
Azioni dell'amministratore delegato 286
Azioni relative agli account dei membri 288
Designazione di un account amministratore 289
Considerazioni 289
Autorizzazioni necessarie per designare un amministratore delegato 289
Designazione di un amministratore delegato 290
Attivazione delle scansioni Amazon Inspector per gli account dei membri 292
Dissociazione degli account dei membri 295
Rimozione dell'amministratore delegato 296
Applicazione di tag alle risorse 298
Nozioni fondamentali sull'etichettatura 298
Aggiungere tag 299
Aggiungere tag alle risorse di Amazon Inspector 299
Rimozione dei tag 300
Rimuovere i tag dalle risorse di Amazon Inspector 301
Utilizzo 302
Utilizzo della console di utilizzo 302
Scopri come Amazon Inspector calcola i costi di utilizzo 304
Informazioni sulla versione di prova gratuita di Amazon Inspector 304
Sicurezza 306
Protezione dei dati 307
Crittografia dei dati a riposo 308
Crittografia in transito 312
Identity and Access Management 312
Destinatari 313
Autenticazione con identità 314
Gestione dell'accesso con policy 317
Come funziona Amazon Inspector con IAM 320
Esempi di policy basate su identità 327
AWS politiche gestite 331
Uso di ruoli collegati ai servizi 347

Risoluzione dei problemi ... 363
Monitoraggio di Amazon Inspector ... 365
CloudTrail registri ... 365
Convalida della conformità ... 369
Resilienza ... 370
Sicurezza dell'infrastruttura ... 370
Risposta agli incidenti ... 371
AWS PrivateLink ... 371
Considerazioni ... 372
Creazione di un endpoint di interfaccia ... 372
Integrazioni ... 373
Integrazione di Amazon Inspector con Amazon ECR ... 373
Integrazione di Amazon Inspector con Security Hub ... 373
Integrazione con Amazon ECR ... 373
Attivazione dell'integrazione ... 374
Utilizzo dell'integrazione con un ambiente multi-account ... 374
Integrazione di Security Hub ... 374
Visualizzazione dei risultati di Amazon Inspector in AWS Security Hub ... 375
Attivazione e configurazione dell'integrazione di Amazon Inspector con Security Hub ... 379
Disattivazione del flusso di risultati da un'integrazione ... 379
Visualizzazione dei controlli di sicurezza per Amazon Inspector in Security Hub ... 379
Sistemi operativi e linguaggi di programmazione supportati ... 380
Sistemi operativi supportati ... 381
Sistemi operativi supportati: Amazon EC2 scanning ... 381
Sistemi operativi supportati: scansione Amazon ECR con Amazon Inspector ... 385
Sistemi operativi supportati: scansione CIS ... 387
Sistemi operativi fuori produzione ... 388
Linguaggi di programmazione compatibili ... 395
Linguaggi di programmazione supportati: Amazon EC2 agentless scanning ... 395
Linguaggi di programmazione supportati: Amazon EC2 deep inspection ... 396
Linguaggi di programmazione supportati: Amazon ECR scanning ... 396
Runtime supportati ... 397
Runtime supportati: scansione standard di Amazon Inspector Lambda ... 397
Runtime supportati: scansione del codice Amazon Inspector Lambda ... 398
Disattivazione di Amazon Inspector ... 400
Disattiva Amazon Inspector ... 401

Quote 402
Regioni ed endpoint 404
Endpoint di servizio per Amazon Inspector 404
Endpoint per l'API Amazon Inspector Scan 404
Disponibilità di funzionalità specifiche per ogni regione 419
Cronologia dei documenti 424
AWS Glossario 448
..... cdxlix

Che cos'è Amazon Inspector?

Amazon Inspector è un servizio di gestione delle vulnerabilità che rileva automaticamente i carichi di lavoro e li analizza continuamente per individuare vulnerabilità del software ed esposizione involontaria alla rete. Amazon Inspector rileva e analizza le EC2 istanze Amazon, le immagini dei container in Amazon ECR e le funzioni Lambda. Quando Amazon Inspector rileva una vulnerabilità del software o un'esposizione involontaria della rete, crea un risultato, ovvero un rapporto dettagliato sul problema. Puoi gestire i risultati nella console o nell'API di Amazon Inspector.

Argomenti

- Caratteristiche di Amazon Inspector
- Accesso ad Amazon Inspector

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' EC2 istanza, installazione di una patch e quando viene pubblicato un nuovo CVE (Common Vulnerabilities and Exposures) 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' EC2 istanza Amazon 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 Strumenti per 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 Strumenti per PowerShell l'utente.

AWS SDKs

AWS fornisce SDKs che consistono in librerie e codice di esempio per vari linguaggi e piattaforme di programmazione, tra cui Java, Go, Python, C++ e.NET. SDKs Forniscono un accesso comodo 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 di AWS SDKs, 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 SDKs, 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

Questa sezione fornisce informazioni da considerare prima di attivare Amazon Inspector e un tutorial introduttivo che descrive come attivare Amazon Inspector e visualizzare i risultati nella console Amazon Inspector e con l'API Amazon Inspector.

Argomenti

- Prima di attivare Amazon Inspector
- Tutorial introduttivo: attivazione di Amazon Inspector

Prima di attivare Amazon Inspector

Prima di attivare Amazon Inspector, considera quanto segue:

Amazon Inspector è un servizio regionale

I tuoi dati vengono archiviati nel Regione AWS punto in cui attivi Amazon Inspector. Ripeti i passaggi indicati nella prima parte del tutorial introduttivo per tutti i Regioni AWS casi in cui intendi utilizzare Amazon Inspector.

Amazon Inspector crea i ruoli collegati ai servizi 2 e 2Agentless AWSService RoleForAmazonInspector AWSService RoleForAmazonInspector

Un ruolo collegato a un servizio è un ruolo in AWS Identity and Access Management (IAM) collegato a un servizio. AWS AWSServiceRoleForAmazonInspector2 e AWSServiceRoleForAmazonInspector2Agentless consentono ad Amazon Inspector di accedere ai Servizi AWS requisiti necessari per eseguire le valutazioni di sicurezza.

Le identità IAM con autorizzazioni di amministratore possono abilitare Amazon Inspector

Proteggi le tue credenziali creando utenti con IAM o. AWS IAM Identity Center Questo ti aiuta ad assicurarti che gli utenti dispongano solo delle autorizzazioni necessarie per gestire Amazon Inspector. Per ulteriori informazioni, consulta la policy AWS gestita:. AmazonInspectorFullAccess

La scansione ibrida viene abilitata automaticamente

La scansione ibrida include la scansione basata su agenti e la scansione senza agenti. Per impostazione predefinita, Amazon Inspector utilizza questi metodi di scansione su tutte le istanze

Amazon EC2 idonee. Per ulteriori informazioni, consulta Scansione EC2 delle istanze Amazon con Amazon Inspector.

La scansione Amazon ECR e la scansione della funzione Lambda non richiedono l'agente SSM

La scansione basata su agenti utilizza l'agente SSM per raccogliere l'inventario del software. La scansione senza agenti utilizza le istantanee di Amazon EBS per raccogliere l'inventario del software.

> **Note**
>
> Per impostazione predefinita, l'agente SSM è già installato nelle EC2 istanze Amazon basate su Amazon Machine Images. Tuttavia, in alcuni casi potrebbe essere necessario attivare l'agente SSM manualmente. Per ulteriori informazioni, consulta Lavorare con l'agente SSM nella Guida per l'AWS Systems Manager utente.

I costi mensili si basano sui carichi di lavoro scansionati

Per ulteriori informazioni, consulta Prezzi di Amazon Inspector.

Tutorial introduttivo: attivazione di Amazon Inspector

Questo argomento descrive come attivare Amazon Inspector per un ambiente di account autonomo (account membro) e un ambiente multi-account (account amministratore delegato). Quando attivi Amazon Inspector, inizia automaticamente a rilevare i carichi di lavoro e a scansionarli per individuare vulnerabilità del software ed esposizione involontaria della rete.

Standalone account environment

La procedura seguente descrive come attivare Amazon Inspector nella console per un account membro. Per attivare Amazon Inspector in modo programmatico, inspector2-. enablement-with-cli

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Seleziona Inizia.
3. Scegli Activate Amazon Inspector.

Quando attivi Amazon Inspector per un account indipendente, tutti i tipi di scansione vengono attivati per impostazione predefinita. Per informazioni sugli account membro, consulta Comprendere l'account amministratore delegato e gli account membro in Amazon Inspector.

Multi-account environment

La procedura seguente descrive come attivare Amazon Inspector nella console per un account amministratore delegato. Per attivare in modo programmatico Amazon Inspector per più account, usa lo script di shell Amazon Inspector inspector2 -. enablement-with-cli

> **Note**
>
> È necessario utilizzare l'account di AWS Organizations gestione per completare questa procedura. Solo l'account AWS Organizations di gestione può designare un amministratore delegato. Potrebbero essere necessarie autorizzazioni per designare un amministratore delegato. Per ulteriori informazioni, consulta Autorizzazioni necessarie per designare un amministratore delegato.

Quando attivi Amazon Inspector per la prima volta, Amazon Inspector crea il `AWSServiceRoleForAmazonInspector` ruolo collegato al servizio per l'account. Per informazioni su come Amazon Inspector utilizza i ruoli collegati ai servizi, consulta. Utilizzo di ruoli collegati ai servizi per Amazon Inspector

Per designare un amministratore delegato per Amazon Inspector

1. Accedi all'account di AWS Organizations gestione, quindi apri la console Amazon Inspector su https://console.aws.amazon.com/inspector/ v2/home.
2. Scegli Avvia.
3. In Amministratore delegato, inserisci l'ID a 12 cifre dell'ID Account AWS che desideri designare come amministratore delegato.
4. Scegli Delegato, quindi scegli nuovamente Delegato.
5. (Facoltativo) Se desideri attivare Amazon Inspector per l'account di AWS Organizations gestione, scegli Attiva Amazon Inspector in Autorizzazioni di servizio.

Quando si designa un amministratore delegato, per impostazione predefinita vengono attivati tutti i tipi di scansione per l'account. Per informazioni sull'account amministratore delegato, consulta Comprendere l'account amministratore delegato e gli account dei membri in Amazon Inspector.

Tipi di scansione automatizzati in Amazon Inspector

Amazon Inspector utilizza un motore di scansione appositamente progettato che monitora le risorse alla ricerca di vulnerabilità del software e di esposizione involontaria della rete. Quando Amazon Inspector rileva una vulnerabilità del software o un'esposizione involontaria della rete, crea una scoperta. Quando attivi Amazon Inspector per la prima volta, il tuo account viene registrato automaticamente a tutti i tipi di scansione, tra cui Amazon Amazon scan EC2 , Amazon ECR Scanning e Lambda standard Scanning.

> **Note**
>
> La scansione del codice Lambda è un livello opzionale di scansione delle funzioni Lambda che puoi attivare in qualsiasi momento.

Argomenti

- Panoramica dei tipi di scansione di Amazon Inspector
- Attivazione di un tipo di scansione
- Scansione EC2 delle istanze Amazon con Amazon Inspector
- Scansione delle immagini dei container Amazon Elastic Container Registry con Amazon Inspector
- AWS Lambda Funzioni di scansione con Amazon Inspector
- Disattivazione di un tipo di scansione in Amazon Inspector

Panoramica dei tipi di scansione di Amazon Inspector

Amazon Inspector offre diversi tipi di scansione, che si concentrano su tipi di risorse specifici nel tuo AWS ambiente.

EC2 Scansione Amazon

Quando attivi Amazon EC2 scan, Amazon Inspector analizza le tue EC2 istanze alla ricerca di vulnerabilità ed esposizioni comuni (CVEs), problemi di esposizione della rete, problemi di raggiungibilità della rete, vulnerabilità del sistema operativo e del pacchetto del linguaggio di programmazione. Amazon Inspector esegue le scansioni utilizzando l'agente SSM installato

sull'istanza o tramite istantanee delle istanze di Amazon EBS. Per ulteriori informazioni, consulta Scansione EC2 delle istanze Amazon con Amazon Inspector. Per impostazione predefinita, quando attivi Amazon EC2 Scanning, abiliti automaticamente la modalità di scansione ibrida. Per ulteriori informazioni, consulta la sezione Scansione senza agenti.

Scansione Amazon ECR

Quando attivi la scansione Amazon ECR, Amazon Inspector converte tutti i repository del tuo registro privato da repository di container per la scansione di base a repository di container a scansione avanzata. Puoi configurare questa impostazione con regole di inclusione per eseguire la scansione solo in modalità push o per scansionare repository selezionati. Amazon Inspector analizza tutte le immagini inviate negli ultimi 30 giorni o recuperate negli ultimi 90 giorni. Amazon Inspector continua a monitorare le immagini per 90 giorni per impostazione predefinita. Puoi modificare questa impostazione in qualsiasi momento. Per ulteriori informazioni, consulta Scansione delle immagini dei container Amazon Elastic Container Registry con Amazon Inspector.

Scansione standard Lambda

Quando attivi la scansione standard Lambda, Amazon Inspector rileva tutte le funzioni Lambda nel tuo account e le analizza immediatamente per individuare eventuali vulnerabilità. Amazon Inspector analizza nuove funzioni e livelli Lambda quando vengono distribuiti. Amazon Inspector li analizza nuovamente quando vengono aggiornati o quando ne vengono pubblicati di nuovi CVEs . Per ulteriori informazioni, scansione, consulta. AWS Lambda Funzioni di scansione con Amazon Inspector

Scansione standard Lambda + scansione del codice Lambda

Quando attivi la scansione del codice Lambda, Amazon Inspector rileva le funzioni e i livelli Lambda nel tuo account e li analizza per individuare eventuali vulnerabilità del codice. Questo tipo di scansione valuta le dipendenze dei pacchetti applicativi utilizzati in una funzione Lambda per. CVEs Quando si attiva questo tipo di scansione, si attiva anche la scansione standard Lambda. Per ulteriori informazioni, consulta AWS Lambda Funzioni di scansione con Amazon Inspector.

Codice di sicurezza per Amazon Inspector

Questo tipo di scansione sfrutta il motore di scansione Amazon Q Developer per scansionare il codice di applicazioni di prime parti, le dipendenze delle applicazioni di terze parti e Infrastructure as Code per individuare eventuali vulnerabilità. Per ulteriori informazioni, consulta Code Security for Amazon Inspector.

Attivazione di un tipo di scansione

Puoi attivare un tipo di scansione in qualsiasi momento. Quando attivi un tipo di scansione, Amazon Inspector inizia a scansionare le risorse idonee per quel tipo di scansione.

EC2 Scansione Amazon

Questo tipo di scansione estrae i metadati da EC2 un'istanza Amazon prima di confrontarli con le regole raccolte dagli avvisi di sicurezza. Quando attivi questo tipo di scansione, Amazon Inspector analizza tutte le EC2 istanze Amazon idonee nel tuo account alla ricerca di vulnerabilità dei pacchetti e problemi di raggiungibilità della rete. Dopo aver attivato questo tipo di scansione, puoi visualizzare quante istanze vengono scansionate nella scheda Istanze.

Scansione Amazon ECR

Questo tipo di scansione analizza le immagini e gli archivi dei container in Amazon ECR. Quando attivi questo tipo di scansione, modifichi l'impostazione di configurazione della scansione per il registro privato dalla scansione di base alla scansione avanzata. Dopo aver attivato la scansione Amazon ECR, puoi visualizzare quante immagini e repository vengono scansionati nelle schede Immagini container e Repositori container.

Scansione standard Lambda + scansione del codiceLambda

La scansione Lambda standard è il tipo di scansione Lambda predefinito. Quando attivi la scansione standard Lambda, tutte le funzioni Lambda vengono analizzate alla ricerca di vulnerabilità del software, purché siano state richiamate o aggiornate negli ultimi 90 giorni. Dopo aver attivato la scansione standard Lambda, puoi visualizzare quante funzioni Lambda vengono scansionate nella scheda Funzioni Lambda.

La scansione del codice Lambda analizza il codice dell'applicazione personalizzato in una funzione Lambda. Quando attivi la scansione del codice Lambda, tutte le funzioni Lambda verranno analizzate alla ricerca di vulnerabilità del codice, purché siano state richiamate o aggiornate negli ultimi 90 giorni. Dopo aver attivato la scansione standard Lambda, puoi visualizzare quante funzioni Lambda vengono scansionate per individuare eventuali vulnerabilità del codice nella scheda Funzioni Lambda.

> **Note**
>
> È possibile attivare la scansione standard Lambda e la scansione del codice Lambda indipendentemente o insieme.

Codice di sicurezza di Amazon Inspector

Questo tipo di scansione analizza il codice applicativo di prime parti, le dipendenze delle applicazioni di terze parti e Infrastructure as Code alla ricerca di vulnerabilità. Quando attivi Code Security, Amazon Inspector inizia a scansionare i tuoi repository di codice alla ricerca di vulnerabilità del codice in base alle configurazioni di scansione. Dopo aver attivato Amazon Inspector Code Security, puoi visualizzare quanti repository di codice vengono scansionati nella scheda Code repository.

Attivazione delle scansioni

La procedura seguente descrive come attivare un tipo di scansione in Amazon Inspector.

> **Note**
>
> Se sei l'amministratore delegato di un' AWS organizzazione, puoi abilitare i tipi di scansione di Amazon Inspector per più account in più regioni utilizzando uno script di shell. Per ulteriori informazioni, consulta inspector2 - on. enablement-with-cli GitHub Altrimenti, 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 su v2/home. https://console.aws.amazon.com/inspector/
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 l'account per IDs cui stai attivando le scansioni e il token di idempotenza e uno o più di, `EC2` `ECRLAMBDA`, o `LAMBDA_CODE` `resourceTypes` per attivare scansioni di quel tipo.

Scansione EC2 delle istanze Amazon con Amazon Inspector

Amazon Inspector Amazon EC2 scan estrae i metadati dall' EC2 istanza prima di confrontarli con le regole raccolte dagli avvisi di sicurezza. Amazon Inspector analizza le istanze alla ricerca di vulnerabilità dei pacchetti e problemi di raggiungibilità della rete per produrre risultati. Amazon Inspector esegue scansioni di raggiungibilità della rete una volta ogni 12 ore e scansioni di vulnerabilità dei pacchetti con una cadenza variabile che dipende dal metodo di scansione associato all'istanza. EC2

Le scansioni delle vulnerabilità dei pacchetti possono essere eseguite utilizzando un metodo di scansione basato su agenti o senza agente. Entrambi questi metodi di scansione determinano come e quando Amazon Inspector raccoglie l'inventario del software da un' EC2 istanza per le scansioni delle vulnerabilità dei pacchetti. La scansione basata su agenti raccoglie l'inventario software utilizzando l'agente SSM, mentre la scansione senza agenti raccoglie l'inventario software utilizzando le istantanee di Amazon EBS.

Amazon Inspector utilizza i metodi di scansione attivati per il tuo account. Quando attivi Amazon Inspector per la prima volta, il tuo account viene automaticamente registrato alla scansione ibrida, che utilizza entrambi i metodi di scansione. Tuttavia, puoi modificare questa impostazione in qualsiasi momento. Per informazioni su come attivare un tipo di scansione, vedere Attivazione di un tipo di scansione. Questa sezione fornisce informazioni sulla EC2 scansione di Amazon.

> **Note**
>
> Amazon EC2 scanning non esegue la scansione delle directory del file system relative all'ambiente virtuale, anche se il provisioning viene eseguito tramite un'ispezione approfondita. Ad esempio, il percorso non `/var/lib/docker/` viene analizzato perché viene comunemente utilizzato per i tempi di esecuzione dei container.

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 basate su Linux EC2

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.

> **Note**
>
> Per la scansione basata su agenti, l' EC2 istanza Amazon deve essere gestita da SSM all'interno dello stesso. Account AWS

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: Amazon EC2 scanning”
- L'istanza non è esclusa dalle scansioni tramite i tag di esclusione di Amazon EC2 Inspector.
- 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 EC2 di vulnerabilità delle istanze nelle seguenti situazioni:

- Quando avvii una nuova istanza. EC2
- Quando installi un nuovo software su un' EC2 istanza esistente (Linux e Mac).
- Quando Amazon Inspector aggiunge un nuovo elemento CVE (Common Vulnerabilities and Exposures) al suo database e quel CVE è pertinente alla tua EC2 istanza (Linux e Mac).

Amazon Inspector aggiorna il campo Ultima scansione per un' EC2 istanza quando viene completata una scansione iniziale. Dopodiché, il campo Ultima scansione viene aggiornato quando Amazon Inspector valuta l'inventario SSM (ogni 30 minuti per impostazione predefinita) 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' EC2 istanza 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' EC2 istanza Amazon 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 dispone dell'autorizzazione per 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 EC2 istanze create da alcune Amazon Machine Images ()AMIs. Per ulteriori informazioni, consulta Informazioni su SSM Agent nella Guida per l'AWS Systems Manager utente. 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' EC2 istanza Amazon 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 EC2 Inspector.

> **Note**
>
> Puoi anche automatizzare la gestione SSM di tutte le tue EC2 istanze, 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 all'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.

Risorse SSM create per la scansione

Amazon Inspector richiede una serie di risorse SSM nel tuo account per eseguire le scansioni 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 Amazon Inspector La scansione EC2 Amazon è attiva 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 tue 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 EC2 istanze Amazon 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 Impostazione di pianificazioni personalizzate, Windows ad esempio scansioni.

`InspectorLinuxDistributor-do-not-delete`

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

> **Note**
>
> Quando disattivi Amazon Inspector EC2 Amazon Scanning o Deep Inspection, la risorsa `InvokeInspectorLinuxSsmPlugin-do-not-delete` SSM non viene più richiamata.

Scansione senza agenti

Amazon Inspector utilizza il metodo di scansione senza agenti su istanze idonee quando l'account è in modalità di scansione ibrida. La modalità di scansione ibrida include scansioni basate su agenti e senza agenti e viene abilitata automaticamente quando attivi Amazon Scanning. EC2

Per le scansioni senza agenti, Amazon Inspector utilizza le istantanee EBS per raccogliere un inventario software dalle tue istanze. La scansione senza agente analizza le istanze alla ricerca di vulnerabilità del sistema operativo e dei pacchetti del linguaggio di programmazione delle applicazioni.

> **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 dall'utente come parte di. Ispezione approfondita di Amazon Inspector per istanze Amazon basate su Linux EC2 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 EBS direct APIs 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 ulteriori informazioni, consulta la colonna >Supporto per la scansione basata su agenti di. the section called “Sistemi operativi supportati: Amazon EC2 scanning”
- Lo stato dell'istanza è pari a`Unmanaged EC2 instance`, `Stale inventory` o. `No inventory`
- L'istanza è supportata da Amazon EBS e ha uno dei seguenti formati di file system:
  - `ext3`
  - `ext4`
  - `xfs`
- L'istanza non è esclusa dalle scansioni tramite i tag di EC2 esclusione di Amazon.

- Il numero di volumi collegati all'istanza è inferiore a 8 e hanno una dimensione combinata inferiore o uguale a 1200 GB.

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' EC2istanza Amazon ogni volta che esegue la scansione degli snapshot estratti da un'istanza dopo una scansione senza agente.

Puoi verificare quando un' EC2 istanza 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 EC2 scansione determina i metodi di scansione che Amazon Inspector utilizzerà per eseguire le EC2 scansioni nel tuo account. Puoi visualizzare la modalità di scansione del tuo account dalla pagina delle impostazioni di EC2 scansione 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 EC2 le istanze idonee in 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. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su 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 escludere Windows istanze Linux e dalle scansioni di Amazon Inspector etichettando queste istanze con la chiave. `InspectorEc2Exclusion` L'inclusione di un valore di tag è facoltativa. Per informazioni sull'aggiunta di tag, consulta Tagga le tue EC2 risorse Amazon.

Quando tagghi un'istanza per l'esclusione dalle scansioni di Amazon Inspector, Amazon Inspector contrassegna l'istanza come esclusa e non crea risultati per essa. Tuttavia, il plug-in Amazon Inspector SSM continuerà a essere richiamato. Per evitare che il plug-in venga richiamato, devi consentire l'accesso ai tag nei metadati dell'istanza.

> **Note**
>
> Non ti viene addebitato alcun costo per le istanze escluse.

Inoltre, puoi escludere un volume EBS crittografato dalle scansioni senza agente 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 EC2 istanze 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 basate su Linux EC2 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. Valori di stato EC2 delle istanze Amazon

Ispezione approfondita di Amazon Inspector per istanze Amazon basate su Linux EC2

Amazon Inspector amplia la copertura di scansione di EC2 Amazon per includere l'ispezione approfondita. Con un'ispezione approfondita, Amazon Inspector rileva le vulnerabilità dei pacchetti dei linguaggi di programmazione delle applicazioni nelle istanze Amazon basate su Linux. EC2 Amazon Inspector analizza i percorsi predefiniti per individuare le librerie di pacchetti dei linguaggi di programmazione. Tuttavia, puoi configurare percorsi personalizzati oltre ai percorsi che Amazon Inspector analizza per impostazione predefinita.

> **Note**
>
> Puoi utilizzare l'ispezione approfondita con l'impostazione Default Host Management Configuration. Tuttavia, è necessario creare o utilizzare un ruolo configurato con le `ssm:GetParameter` autorizzazioni `ssm:PutInventory` e.

Per eseguire scansioni di ispezione approfondita per le tue istanze Amazon basate su Linux, EC2 Amazon Inspector utilizza i dati raccolti con il plug-in Amazon Inspector SSM. Per gestire il plug-in Amazon Inspector SSM ed eseguire un'ispezione approfondita per Linux, Amazon Inspector crea automaticamente l'associazione SSM nel tuo account. `InvokeInspectorLinuxSsmPlugin-do-not-delete` Amazon Inspector raccoglie l'inventario aggiornato delle applicazioni dalle tue istanze Amazon basate su Linux ogni 6 ore. EC2

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

Questa sezione descrive come gestire l'ispezione approfondita di Amazon Inspector per EC2 le istanze Amazon, incluso come impostare percorsi personalizzati per la scansione di Amazon Inspector.

Argomenti

- Accesso o disattivazione dell'ispezione approfondita
- Percorsi personalizzati per l'ispezione approfondita di Amazon Inspector
- Pianificazioni personalizzate per l'ispezione approfondita di Amazon Inspector
- Linguaggi di programmazione compatibili

Accesso o disattivazione dell'ispezione approfondita

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

Per gestire l'ispezione approfondita

1. Accedi utilizzando le tue credenziali, quindi apri la console Amazon Inspector su v2/home https://console.aws.amazon.com/inspector/
2. Dal pannello di navigazione, scegli Impostazioni generali, quindi scegli Impostazioni di EC2 scansione Amazon.
3. Nell'ambito dell'ispezione approfondita dell' EC2 istanza Amazon, puoi impostare percorsi personalizzati per la tua organizzazione o per il tuo account.

Puoi controllare lo stato di attivazione a livello di codice per un singolo account con l'API GetEc2DeepInspectionConfiguration. Puoi controllare lo stato di attivazione a livello di codice per più account con l'API. BatchGetMemberEc2DeepInspectionStatus

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 l'API per attivare BatchUpdateMemberEc2DeepInspectionStatusl'ispezione approfondita 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

Percorsi personalizzati per l'ispezione approfondita di Amazon Inspector

Puoi impostare percorsi personalizzati per la scansione di Amazon Inspector durante l'ispezione approfondita delle tue istanze Amazon EC2 Linux. Quando imposti un percorso personalizzato, Amazon Inspector analizza i pacchetti in quella directory e in tutte le sue sottodirectory.

Tutti gli account possono definire fino a 5 percorsi personalizzati. L'amministratore delegato di un'organizzazione può definire 10 percorsi personalizzati.

Amazon Inspector analizza tutti i percorsi personalizzati oltre ai seguenti percorsi predefiniti, che Amazon Inspector analizza 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, ad esempio montaggi di Network File System o supporti di file system Amazon S3.

Formattazione di percorsi personalizzati

Un percorso personalizzato non può contenere più di 256 caratteri. Di seguito è riportato un esempio di come potrebbe apparire un percorso personalizzato:

Percorso di esempio

```
/home/usr1/project01
```

> **Note**
>
> Il limite di pacchetti per istanza è 5.000. Il tempo massimo di raccolta dell'inventario dei pacchi è di 15 minuti. Amazon Inspector consiglia di scegliere percorsi personalizzati per evitare questi limiti.

Impostazione di un percorso personalizzato nella console Amazon Inspector e con l'API Amazon Inspector

Le seguenti procedure descrivono come impostare un percorso personalizzato per l'ispezione approfondita di Amazon Inspector nella console Amazon Inspector e con l'API Amazon Inspector. Dopo aver impostato un percorso personalizzato, Amazon Inspector lo include nella successiva ispezione approfondita.

Console

1. Accedi AWS Management Console come amministratore delegato e apri la console Amazon Inspector su v2/home https://console.aws.amazon.com/inspector/
2. Usa il Regione AWS selettore per scegliere la regione in cui desideri attivare la scansione standard Lambda.
3. Dal pannello di navigazione, scegli Impostazioni generali, quindi scegli Impostazioni di EC2 scansione.
4. In Percorsi personalizzati per il tuo account, scegli Modifica.
5. Nelle caselle di testo dei percorsi, inserisci i percorsi personalizzati.
6. Scegli Save (Salva).

API

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

Pianificazioni personalizzate per l'ispezione approfondita di Amazon Inspector

Per impostazione predefinita, Amazon Inspector raccoglie un inventario delle applicazioni dalle EC2 istanze Amazon ogni 6 ore. Tuttavia, puoi eseguire i seguenti comandi per controllare la frequenza con cui Amazon Inspector esegue questa operazione.

Comando di esempio 1: elenca le associazioni per visualizzare l'ID dell'associazione e l'intervallo corrente

Il comando seguente mostra l'ID dell'associazione`InvokeInspectorLinuxSsmPlugin-do-not-delete`.

```
aws ssm list-associations \
--association-filter-list "key=AssociationName,value=InvokeInspectorLinuxSsmPlugin-do-not-delete" \
--region your-Region
```

Comando di esempio 2: Aggiorna l'associazione per includere un nuovo intervallo

Il comando seguente utilizza l'ID dell'associazione per l'associazione`InvokeInspectorLinuxSsmPlugin-do-not-delete`. È possibile impostare la frequenza `schedule-expression` da 6 ore a un nuovo intervallo, ad esempio 12 ore.

```
aws ssm update-association \
--association-id "your-association-ID" \
--association-name "InvokeInspectorLinuxSsmPlugin-do-not-delete" \
--schedule-expression "rate(6 hours)" \
--region your-Region
```

> **Note**
>
> A seconda del caso d'uso, se imposti la frequenza `schedule-expression` da 6 ore a un intervallo di 30 minuti, puoi superare il limite giornaliero di inventario ssm. Ciò causa un ritardo nei risultati e potresti riscontrare EC2 istanze Amazon con stati di errore parziali.

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 e i pacchetti del sistema operativo.

Per le istanze Mac e Windows, l'ispezione approfondita di Amazon Inspector può produrre risultati solo per i pacchetti del sistema operativo.

Per ulteriori informazioni sui linguaggi di programmazione supportati, consulta Linguaggi di programmazione supportati: Amazon EC2 deep inspection.

Scansione Windows EC2 delle istanze con Amazon Inspector

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 e linguaggi di programmazione supportati da Amazon Inspector. Amazon Inspector esegue le Windows scansioni a intervalli regolari. Windowsle istanze vengono scansionate al momento del rilevamento e successivamente ogni 6 ore. Tuttavia, è possibile regolare l'intervallo di scansione predefinito dopo la prima scansione.

Quando Amazon EC2 scan è attivato, Amazon Inspector crea le seguenti associazioni SSM per le tue Windows risorse:`InspectorDistributor-do-not-delete`, `InspectorInventoryCollection-do-not-delete` e. `InvokeInspectorSsmPlugin-do-not-delete` Per installare il plug-in Amazon Inspector SSM sulle tue Windows istanze, l'associazione SSM utilizza il documento `InspectorDistributor-do-not-delete` SSM e il pacchetto `AWS-ConfigureAWSPackage` SSM Distributor. `AmazonInspector2-InspectorSsmPlugin` Per ulteriori informazioni, consulta il plugin Amazon Inspector SSM per. Windows Per raccogliere dati sulle istanze e generare risultati di Amazon Inspector, l'associazione `InvokeInspectorSsmPlugin-do-not-delete` SSM esegue il plug-in Amazon Inspector SSM a intervalli di 6 ore. Tuttavia, puoi personalizzare questa impostazione utilizzando un cron o un'espressione rate.

> **Note**
>
> Amazon Inspector inserisce i file di definizione Open Vulnerability and Assessment Language (OVAL) aggiornati nel bucket S3. `inspector2-oval-prod-`*`your-AWS-Region`* Il bucket Amazon S3 contiene le definizioni OVAL utilizzate nelle scansioni. Queste definizioni OVAL non devono essere modificate. In caso contrario, Amazon Inspector non ne cercherà di nuovi al CVEs momento del rilascio.

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, vedereValori di stato EC2 delle istanze Amazon.
- 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`

Impostazione di pianificazioni personalizzate, Windows ad esempio scansioni

Puoi personalizzare l'intervallo tra le scansioni delle tue EC2 istanze Windows Amazon 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 per Windows le 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 AWS CLI comando seguente:

```
$ 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 Elastic Container Registry con Amazon Inspector

Amazon Inspector analizza le immagini dei container archiviate in Amazon Elastic Container Registry alla ricerca di vulnerabilità del software per generare risultati sulle vulnerabilità dei pacchetti. Quando attivi la scansione Amazon ECR, imposti Amazon Inspector come servizio di scansione preferito per il tuo registro privato.

> **Note**
>
> Amazon ECR utilizza una politica di registro per concedere le autorizzazioni a un AWS principale. Questo principale dispone delle autorizzazioni necessarie per chiamare Amazon APIs Inspector per la scansione. Quando imposti l'ambito della politica del registro, non devi aggiungere l'`ecr:*`azione o `PutRegistryScanningConfiguration` entrare. `deny` Ciò

comporta errori a livello di registro durante l'attivazione e la disabilitazione della scansione per Amazon ECR.

Con la scansione di base, puoi configurare i tuoi repository per eseguire scansioni istantanee o eseguire scansioni manuali. Con la scansione avanzata, è possibile eseguire la scansione delle vulnerabilità del sistema operativo e dei pacchetti dei linguaggi di programmazione a livello di registro. Per un side-by-side confronto delle differenze tra la scansione di base e quella avanzata, consulta le domande frequenti su Amazon Inspector.

> **Note**
>
> La scansione di base viene fornita e fatturata tramite Amazon ECR. Per ulteriori informazioni, consulta i prezzi di Amazon Elastic Container Registry. La scansione avanzata viene fornita e fatturata tramite Amazon Inspector. Per ulteriori informazioni, consulta Prezzi di Amazon Inspector.

Per informazioni su come attivare la scansione Amazon ECR, consultaAttivazione di un tipo di scansione. Per informazioni su come visualizzare i risultati, consultaGestione dei risultati in Amazon Inspector. Per informazioni su come visualizzare i risultati a livello di immagine, consulta Image scanning nella Amazon Elastic Container Registry User Guide. Puoi anche gestire i risultati Servizi AWS non disponibili per la scansione di base, come Amazon AWS Security Hub e Amazon EventBridge.

Questa sezione fornisce informazioni sulla scansione di Amazon ECR e descrive come configurare la scansione avanzata per i repository Amazon ECR.

Comportamenti di scansione per la scansione Amazon ECR

Quando attivi per la prima volta la scansione Amazon ECR, Amazon Inspector rileva le immagini inviate negli ultimi 14 giorni. Amazon Inspector esegue quindi la scansione delle immagini e imposta gli stati di scansione su. `active` Se la scansione continua è abilitata, Amazon Inspector monitora le immagini a condizione che siano state inviate entro 14 giorni (per impostazione predefinita), che la last-in-use data sia entro 14 giorni (per impostazione predefinita) o che le immagini vengano scansionate entro la durata di nuova scansione configurata. Per gli account Amazon Inspector creati prima del 16 maggio 2025, la configurazione predefinita prevede una nuova scansione

per monitorare le immagini se sono state inviate o recuperate negli ultimi 90 giorni. Per ulteriori informazioni, consulta Configurazione della durata della nuova scansione di Amazon 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.

Mappatura delle immagini dei container ai container in esecuzione

Amazon Inspector offre una gestione completa della sicurezza dei container mappando le immagini dei container ai container in esecuzione su Amazon Elastic Container Service (Amazon ECS) e Amazon Elastic Kubernetes Service (Amazon EKS). Queste mappature forniscono informazioni sulle vulnerabilità delle immagini sui container in esecuzione.

> **Note**
>
> La policy gestita `AWSReadOnlyAccess` da sola non fornisce autorizzazioni sufficienti per visualizzare la mappatura tra le immagini di Amazon ECR e i container in esecuzione. Sono necessarie sia le politiche `AWSInspector2ReadOnlyAccess` gestite che quelle

`AWSReadOnlyAccess` gestite per visualizzare le informazioni sulla mappatura delle immagini dei container.

Con questa funzionalità, puoi dare priorità agli sforzi di riparazione in base ai rischi operativi e mantenere la copertura di sicurezza nell'intero ecosistema di container. Puoi monitorare le immagini dei container attualmente in uso e l'ultima volta che le immagini dei container sono state utilizzate su un cluster Amazon ECS o Amazon EKS nelle ultime 24 ore. Per nuove immagini o account, possono essere necessarie fino a 36 ore prima che i dati siano disponibili. Successivamente, questi dati vengono aggiornati una volta ogni 24 ore. Queste informazioni saranno disponibili nei risultati tramite la console Amazon Inspector nella schermata dei dettagli dei risultati relativi all'immagine del contenitore e con l'API Amazon Inspector tramite `ecrImageInUseCount` i filtri e. `ecrImageLastInUseAt`

> **Note**
>
> Questi dati vengono inviati automaticamente ai risultati di Amazon ECR quando attivi la scansione Amazon ECR e configuri il tuo repository per la scansione continua. La scansione continua deve essere configurata a livello di repository Amazon ECR. Per ulteriori informazioni, consulta la sezione Scansione avanzata nella Guida per l'utente di Amazon Elastic Container Registry.

Puoi anche scansionare nuovamente le immagini dei container dai cluster in base alla loro last-in-use data.

Questa funzionalità è supportata anche su Amazon ECS Amazon EKS Fargate.

Sistemi operativi e tipi di supporti supportati

Per informazioni sui sistemi operativi supportati, vedereSistemi operativi supportati: scansione Amazon ECR con Amazon Inspector.

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

Manifesto dell'immagine

- `"application/vnd.oci.image.manifest.v1+json"`

- `"application/vnd.docker.distribution.manifest.v2+json"`

Configurazione dell'immagine

- `"application/vnd.docker.container.image.v1+json"`
- `"application/vnd.oci.image.config.v1+json"`

Livelli di immagine

- `"application/vnd.docker.image.rootfs.diff.tar"`
- `"application/vnd.docker.image.rootfs.diff.tar.gzip"`
- `"application/vnd.docker.image.rootfs.foreign.diff.tar.gzip"`
- `"application/vnd.oci.image.layer.v1.tar"`
- `"application/vnd.oci.image.layer.v1.tar+gzip"`
- `"application/vnd.oci.image.layer.v1.tar+zstd"`
- `"application/vnd.oci.image.layer.nondistributable.v1.tar"`
- `"application/vnd.oci.image.layer.nondistributable.v1.tar+gzip"`

> **Note**
>
> Amazon Inspector non supporta il tipo di supporto per la `"application/vnd.docker.distribution.manifest.list.v2+json"` scansione dei repository Amazon ECR.

Configurazione della durata della nuova scansione di Amazon ECR

L'impostazione della durata della nuova scansione di Amazon 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 dell'immagine, la data dell'ultima estrazione e la last-in-use data di invio. Come procedura ottimale, configura la durata della nuova scansione per adattarla al meglio al tuo ambiente.

Se crei immagini spesso, scegli una durata di scansione più breve. Per le immagini utilizzate per lunghi periodi di tempo, scegliete una durata di scansione più lunga. La durata di scansione predefinita per i nuovi account, inclusi i nuovi account aggiunti a un'organizzazione, è di 14 giorni.

Amazon Inspector continuerà a monitorare e ripetere la scansione di un'immagine fino all'ultima volta che è stata utilizzata su un cluster o inviata entro 14 giorni (per impostazione predefinita). Se un'immagine non è stata inviata o utilizzata l'ultima volta su un contenitore in esecuzione entro le date di push e ultimo utilizzo configurate, Amazon Inspector interrompe il monitoraggio. Se necessario, è possibile modificare l'impostazione per monitorare le immagini in base alla data dell'ultima estrazione anziché alla data di ultimo utilizzo. Quando Amazon Inspector interrompe il monitoraggio di un'immagine, imposta il codice di stato della scansione dell'immagine su inattivo e il codice motivo su scaduto. Amazon Inspector pianifica quindi la chiusura di tutti i risultati associati alle immagini.

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.

> **Note**
>
> Quando configuri la durata della nuova scansione da un account amministratore delegato, Amazon Inspector applica l'impostazione a tutti gli account membri dell'organizzazione. Se l'account amministratore delegato non abilita la scansione Amazon ECR, non può visualizzare i cluster per un'immagine API.

> **Note**
>
> Tutte le impostazioni della durata della nuova scansione configurate prima del 16 maggio 2025 rimarranno invariate. È possibile continuare a utilizzare tutte le impostazioni predefinite precedentemente configurate.

Durata della nuova scansione dell'immagine

La durata della nuova scansione dell'immagine determina per quanto tempo Amazon Inspector monitorerà le immagini. La durata della nuova scansione dell'immagine include due modalità: data di ultimo utilizzo (impostazione predefinita) o Data ultima estrazione. Scegli Data di ultimo utilizzo

(impostazione predefinita) se desideri utilizzare la data di ultimo utilizzo dell'attività del cluster Amazon ECS/Amazon EKS. Scegli Ultima data di estrazione se desideri utilizzare la data dell'ultima estrazione delle tue immagini Amazon ECR per scansionare nuovamente le immagini. Le seguenti opzioni sono disponibili come durate di nuova scansione:

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

Durata della data di invio dell'immagine

La durata della data di invio dell'immagine determina per quanto tempo Amazon Inspector monitorerà continuamente le immagini dopo essere state inviate ai repository. Le seguenti opzioni sono disponibili come durate di nuova scansione:

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

Per configurare la durata della nuova scansione di Amazon ECR

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Seleziona Regione AWS dove desideri configurare la durata della nuova scansione di Amazon ECR.
3. Dal pannello di navigazione, scegli Impostazioni generali, quindi scegli Impostazioni di scansione ECR.
4. In Durata della nuova scansione ECR, scegli la modalità di nuova scansione dell'immagine, quindi scegli la durata corrispondente.
5. In Data push dell'immagine, scegli la data di invio dell'immagine.

6. Scegli Save (Salva).

AWS Lambda Funzioni di scansione con Amazon Inspector

Il supporto di Amazon Inspector per AWS Lambda funzioni e livelli fornisce valutazioni automatiche e continue delle vulnerabilità di sicurezza. Amazon Inspector offre due tipi di scansione della funzione Lambda:

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 i livelli per individuare le vulnerabilità dei pacchetti.

Scansione del codice Amazon Inspector Lambda

Questo tipo di scansione analizza il codice dell'applicazione personalizzato nella funzione Lambda e nei livelli per individuare eventuali vulnerabilità del codice. È possibile attivare la scansione standard Lambda o attivare la scansione standard Lambda con la scansione del codice Lambda.

Quando attivi la scansione della funzione Lambda, Amazon Inspector crea i AWS CloudTrail seguenti canali collegati ai servizi nel tuo account: e. `cloudtrail:CreateServiceLinkedChannel` `cloudtrail:DeleteServiceLinkedChannel` Amazon Inspector gestisce questi canali e li utilizza per monitorare i tuoi CloudTrail eventi per le scansioni. Questi canali ti consentono di vedere CloudTrail gli eventi nel tuo account come se avessi una traccia. CloudTrail Ti consigliamo di creare un percorso personalizzato CloudTrail per gestire gli eventi del tuo account.

Per informazioni su come attivare la scansione della funzione Lambda, vedere Attivazione di un tipo di scansione. Questa sezione fornisce informazioni sulla scansione della funzione Lambda.

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 aggiungere tag alle funzioni Lambda, in modo da escluderle dalle scansioni standard di Amazon Inspector Lambda. L'esclusione di funzioni dalle scansioni può impedire avvisi non utilizzabili. Quando si contrassegna una funzione per l'esclusione, il tag deve avere la seguente coppia chiave-valore.

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

Questo argomento descrive come etichettare una funzione per l'esclusione dalle scansioni. Per ulteriori informazioni sull'aggiunta di tag in Lambda, consulta Uso dei tag nelle funzioni Lambda.

Per escludere una funzione dalle scansioni

1. Accedi utilizzando le tue credenziali, quindi apri la console Lambda all'indirizzo. https://console.aws.amazon.com/lambda/
2. Dal pannello di navigazione, scegli Funzioni.
3. Scegli il nome della funzione che desideri escludere dalle scansioni standard di Amazon Inspector Lambda.
4. Scegli Configuration (Configurazione), quindi Tags (Tag).
5. Scegli Gestisci tag, quindi Aggiungi nuovo tag.
   a. In Chiave, inserire `InspectorExclusion`.
   b. In Valore, inserire `LambdaStandardScanning`.
6. Seleziona Salva.

Scansione del codice Amazon Inspector Lambda

> **Important**
> Questa funzionalità acquisisce frammenti di funzioni Lambda per evidenziare le vulnerabilità rilevate. Questi frammenti possono mostrare credenziali codificate e altri materiali sensibili.

Con questa funzionalità, Amazon Inspector analizza il codice dell'applicazione in una funzione Lambda alla ricerca di vulnerabilità del codice in base alle migliori pratiche di AWS sicurezza per rilevare fughe di dati, difetti di iniezione, crittografia mancante e crittografia debole. Amazon Inspector utilizza il ragionamento automatico e l'apprendimento automatico per valutare il codice applicativo della funzione Lambda. Utilizza inoltre rilevatori interni sviluppati in collaborazione con Amazon CodeGuru per identificare le violazioni e le vulnerabilità delle politiche. Per ulteriori informazioni, consulta la CodeGuru Detector Library.

Amazon Inspector genera una vulnerabilità del codice quando rileva una vulnerabilità nel codice dell'applicazione della funzione Lambda. Questo tipo di ricerca include un frammento di codice che mostra il problema e dove è possibile trovarlo nel codice. Suggerisce inoltre come risolvere il problema. Il suggerimento include blocchi di plug-and-play codice che è possibile utilizzare per sostituire righe di codice vulnerabili. Queste correzioni al codice vengono fornite in aggiunta alle indicazioni generali sulla correzione del codice per questo tipo di risultato.

I suggerimenti per la correzione del codice si basano su servizi di ragionamento automatico e intelligenza artificiale generativa. Alcuni suggerimenti per la correzione del codice potrebbero non funzionare come previsto. Sei responsabile dei suggerimenti per la correzione del codice che adotti. Esamina sempre i suggerimenti per la correzione del codice prima di adottarli. Potrebbe essere necessario modificarli per assicurarti che il codice funzioni come previsto. Per ulteriori informazioni, consulta la Politica sull'IA responsabile.

La scansione del codice Lambda può essere attivata da sola o insieme alla scansione standard Lambda. Per ulteriori informazioni, consulta Attivazione di un tipo di scansione. Per informazioni su quali dispositivi Regioni AWS supportano questa funzionalità, vedereDisponibilità di funzionalità specifiche per ogni regione.

Crittografia del codice nei risultati delle vulnerabilità del codice

CodeGuru memorizza frammenti di codice rilevati in relazione a una vulnerabilità del codice rilevata mediante la scansione del codice Lambda. Per impostazione predefinita, CodeGuru controlla la chiave AWS proprietaria utilizzata 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

Esclusione delle funzioni dalla scansione del codice Lambda

Puoi aggiungere tag alle funzioni Lambda, in modo da escluderle dalle scansioni del codice di Amazon Inspector Lambda. L'esclusione di funzioni dalle scansioni può impedire avvisi non utilizzabili. Quando si contrassegna una funzione per l'esclusione, il tag deve avere la seguente coppia chiave-valore.

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

Questo argomento descrive come etichettare una funzione per l'esclusione dalle scansioni del codice. Per ulteriori informazioni sull'aggiunta di tag in Lambda, consulta Uso dei tag nelle funzioni Lambda.

Per escludere una funzione dalle scansioni del codice

1. Accedi utilizzando le tue credenziali, quindi apri la console Lambda all'indirizzo. https://console.aws.amazon.com/lambda/
2. Dal pannello di navigazione, scegli Funzioni.
3. Scegli il nome della funzione che desideri escludere dalle scansioni del codice Amazon Inspector Lambda.
4. Scegli Configuration (Configurazione), quindi Tags (Tag).
5. Scegli Gestisci tag, quindi Aggiungi nuovo tag.
   a. In Chiave, inserire `InspectorCodeExclusion`.
   b. In Valore, inserire `LambdaCodeScanning`.
6. Seleziona Salva.

Disattivazione di un tipo di scansione in Amazon Inspector

Quando si disattiva un tipo di scansione, si perde l'accesso a tutti i risultati prodotti dal tipo di scansione. Se riattivi il tipo di scansione, Amazon Inspector analizza tutte le risorse idonee per generare nuove scoperte. Se desideri tenere un registro dei risultati, puoi esportarli in un bucket Amazon Simple Storage Service (Amazon S3) come rapporto sui risultati. Per ulteriori informazioni, consulta Esportazione dei report dei risultati di Amazon Inspector. Quando disattivi un tipo di scansione, potresti riscontrare le seguenti modifiche nell' AWS account in cui hai disattivato il tipo di scansione:

EC2 Scansione Amazon

Quando disattivi Amazon Inspector EC2 Amazon Scanning per un account, vengono eliminate le seguenti associazioni SSM:

- `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 viene rimosso da tutti gli host. Windows Per ulteriori informazioni, consulta Istanza di scansione Windows EC2 .

Scansione Amazon ECR

Quando disattivi la scansione Amazon ECR per un account, l'account del tipo di scansione Amazon ECR passa da Scansione avanzata con Amazon Inspector a scansione di base con Amazon ECR.

Scansione standard Lambda

Quando si disattiva la scansione standard Lambda per un account, si disattiva la scansione del codice Lambda se il tipo di scansione è stato attivato. Inoltre, elimini il canale CloudTrail collegato al servizio creato da Amazon Inspector quando attivi la scansione standard Lambda.

Codice di sicurezza di Amazon Inspector

Quando disattivi Code Security per il tuo account, elimini tutte le integrazioni, i progetti e le configurazioni di scansione ad esso associate. Se il tuo account è l'amministratore delegato di un'organizzazione, disattivi solo Code Security per il tuo account e gli account dei membri diventano account autonomi.

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. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su 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 l'account per IDs cui stai disattivando le scansioni e `resourceTypes` fornisci una o più di, `EC2` `ECR``LAMBDA`, o per `LAMBDA_CODE` disattivare le scansioni.

Center for Internet Security (CIS) esegue scansioni per i sistemi operativi di EC2 istanze Amazon

Le scansioni CIS di Amazon Inspector (scansioni CIS) eseguono benchmark dei sistemi operativi delle istanze EC2 Amazon per assicurarsi che siano configurati in base alle raccomandazioni delle best practice stabilite dal Center for Internet Security. CIS Security Benchmarks fornisce linee guida di configurazione standard del settore e best practice per configurare un sistema in modo sicuro. Puoi eseguire o pianificare scansioni CIS dopo aver abilitato la scansione Amazon EC2 Inspector per un account. Per informazioni su come attivare Amazon EC2 Scanning, consulta Attivazione di un tipo di scansione.

> **Note**
>
> Gli standard CIS sono destinati ai sistemi operativi x86_64. Alcuni controlli potrebbero non essere valutati o restituire istruzioni di riparazione non valide su risorse basate su ARM.

Amazon Inspector esegue scansioni CIS su istanze Amazon di destinazione in base ai tag EC2 delle istanze e alla pianificazione di scansione definita. Amazon Inspector esegue una serie di controlli delle istanze su ciascuna istanza di destinazione. Ogni controllo valuta se la configurazione del sistema soddisfa le raccomandazioni specifiche di CIS Benchmark. Ogni controllo ha un ID e un titolo di controllo CIS, che corrispondono a una raccomandazione CIS Benchmark per quella piattaforma. Al termine di una scansione CIS, è possibile visualizzare i risultati per vedere quali controlli di istanza sono stati superati, ignorati o non riusciti per quel sistema.

> **Note**
>
> Per eseguire o pianificare le scansioni CIS, è necessario disporre di una connessione Internet sicura. Tuttavia, se si desidera eseguire scansioni CIS su istanze private, è necessario utilizzare un endpoint VPC.

Argomenti

- Requisiti delle EC2 istanze Amazon per le scansioni CIS di Amazon Inspector
- Esecuzione di scansioni CIS

- Considerazioni sulla gestione delle scansioni CIS di Amazon Inspector con AWS Organizations
- Bucket Amazon S3 di proprietà di Amazon Inspector utilizzati per le scansioni CIS di Amazon Inspector
- Creazione di una configurazione di scansione CIS
- Visualizzazione dei risultati della scansione CIS
- Modifica di una configurazione di scansione CIS
- Scaricamento dei risultati di una scansione CIS

Requisiti delle EC2 istanze Amazon per le scansioni CIS di Amazon Inspector

Per eseguire una scansione CIS sulla tua EC2 istanza Amazon, l' EC2 istanza Amazon deve soddisfare i seguenti criteri:

- Il sistema operativo dell'istanza è uno dei sistemi operativi supportati per le scansioni CIS. Per ulteriori informazioni, consulta Sistemi operativi e linguaggi di programmazione supportati da Amazon Inspector.
- L'istanza è un'istanza EC2 di Amazon Systems Manager. Per ulteriori informazioni, consulta Working with the SSM Agent nella Guida per l'AWS Systems Manager utente.
- Il plug-in Amazon Inspector SSM è installato sull'istanza. Amazon Inspector installa automaticamente questo plug-in su istanze gestite.
- 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 policy Amazon SSMManaged InstanceCore and AmazonInspector2 a un ruolo IAM. Quindi collega il ruolo IAM 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**
>
> Non è necessario abilitare l'ispezione approfondita di Amazon Inspector prima di eseguire una scansione CIS sulla tua istanza Amazon. EC2 Se disabiliti l'ispezione approfondita di Amazon Inspector, Amazon Inspector installa automaticamente l'agente SSM, ma l'agente SSM non verrà più richiamato per eseguire l'ispezione approfondita. Tuttavia, di

conseguenza, l'`InspectorLinuxDistributor-do-not-delete`associazione è presente nel tuo account.

Requisiti degli endpoint Amazon Virtual Private Cloud per l'esecuzione di scansioni CIS su istanze Amazon private EC2

Puoi eseguire scansioni CIS su EC2 istanze Amazon su una rete Amazon. Tuttavia, se desideri eseguire scansioni CIS su EC2 istanze Amazon private, devi creare endpoint Amazon VPC. I seguenti endpoint sono necessari per creare endpoint Amazon VPC per Systems Manager:

- `com.amazonaws.`*`region`*`.ec2messages`
- `com.amazonaws.`*`region`*`.inspector2`
- `com.amazonaws.`*`region`*`.s3`
- `com.amazonaws.`*`region`*`.ssm`
- `com.amazonaws.`*`region`*`.ssmmessages`

Per ulteriori informazioni, consulta Creazione di endpoint Amazon VPC per Systems Manager nella Guida per l'AWS Systems Manager utente.

> **Note**
>
> Attualmente, alcuni Regioni AWS non supportano l'`amazonaws.com.`*`region`*`.inspector2`endpoint.

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.

Considerazioni sulla gestione delle scansioni CIS di Amazon Inspector con AWS Organizations

Quando esegui scansioni CIS in un'organizzazione, gli amministratori delegati e gli account dei membri di Amazon Inspector interagiscono con le configurazioni e i risultati delle scansioni CIS in modo diverso.

In che modo gli amministratori delegati di Amazon Inspector possono interagire con le configurazioni e i risultati delle scansioni CIS

Quando l'amministratore delegato crea una configurazione di scansione, per tutti gli account o per uno specifico account membro, l'organizzazione è proprietaria della configurazione. Le configurazioni di scansione di proprietà di un'organizzazione hanno un ARN che specifica l'ID dell'organizzazione come proprietario:

`arn:aws:inspector2:Region:111122223333:owner/OrganizationId/cis-configuration/scanId`

L'amministratore delegato può gestire le configurazioni di scansione di proprietà di un'organizzazione, anche se sono state create da un altro account.

L'amministratore delegato può visualizzare i risultati della scansione per qualsiasi account della propria organizzazione.

Se l'amministratore delegato crea una configurazione di scansione e lo specifica `SELF` come account di destinazione, l'amministratore delegato è proprietario della configurazione di scansione, anche se lascia l'organizzazione. Tuttavia, l'amministratore delegato non può modificare la destinazione di una configurazione di scansione utilizzando come destinazione. `SELF`

> **Note**
>
> L'amministratore delegato non può aggiungere tag alle configurazioni di scansione CIS di proprietà dell'organizzazione.

In che modo gli account membri di Amazon Inspector possono interagire con le configurazioni e i risultati delle scansioni CIS

Quando un account membro crea una configurazione di scansione CIS, è proprietario della configurazione. Tuttavia, l'amministratore delegato può visualizzare la configurazione. Se un account membro lascia l'organizzazione, l'amministratore delegato non sarà in grado di visualizzare la configurazione.

> **Note**
>
> L'amministratore delegato non può modificare una configurazione di scansione creata dall'account membro.

Gli account membro, gli amministratori delegati che hanno `SELF` come destinazione e gli account autonomi possiedono tutti le configurazioni di scansione che creano. Queste configurazioni di scansione hanno un ARN che mostra l'ID dell'account come proprietario:

`arn:aws:inspector2:Region:111122223333:owner/111122223333/cis-configuration/scanId`

Un account membro può visualizzare i risultati delle scansioni nel proprio account, inclusi i risultati delle scansioni CIS pianificate dall'amministratore delegato.

Bucket Amazon S3 di proprietà di Amazon Inspector utilizzati per le scansioni CIS di Amazon Inspector

Open Vulnerability and Assessment Language (OVAL) è uno strumento di sicurezza delle informazioni che standardizza le modalità di valutazione e segnalazione dello stato delle macchine dei sistemi informatici. La tabella seguente elenca tutti i bucket Amazon S3 di proprietà di Amazon Inspector con definizioni OVAL utilizzati per le scansioni CIS. Amazon Inspector archivia i file di definizione OVAL necessari per le scansioni CIS. I bucket Amazon S3 di proprietà di Amazon Inspector dovrebbero essere inseriti nell'elenco consentito, se necessario. VPCs

> **Note**
>
> I dettagli per ciascuno dei seguenti bucket Amazon S3 di proprietà di Amazon Inspector non sono soggetti a modifiche. Tuttavia, la tabella potrebbe essere aggiornata in base alle nuove funzionalità supportate. Regioni AWS Non puoi utilizzare i bucket Amazon S3 di proprietà di Amazon Inspector 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)
`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)

Bucket CIS	Regione AWS
`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)
`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)

Creazione di una configurazione di scansione CIS

Questo argomento descrive come creare una configurazione di scansione CIS.

Per eseguire una scansione CIS

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Utilizza il Regione AWS menu a discesa per selezionare il Regione AWS punto in cui desideri eseguire una scansione CIS.
3. Dal riquadro di navigazione, scegli Scansioni su richiesta, quindi scegli Scansioni CIS.
4. Scegli Crea nuova scansione.
5. Per Nome di configurazione della scansione, inserisci un nome di configurazione della scansione.
6. Per i tag delle risorse di Target, inserisci una chiave e un valore corrispondente per le istanze che desideri scansionare. Puoi specificare fino a cinque valori diversi per ogni chiave e un totale di 25 tag da includere nella scansione.
7. Per il 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.
8. Per gli account Target, specifica quali account includere nella scansione CIS. Per ulteriori informazioni, consulta Considerazioni sulla gestione delle scansioni CIS di Amazon Inspector con AWS Organizations.

   Se il tuo account è l'account amministratore delegato, puoi selezionare Tutti gli account o Specificare gli account. L'opzione Tutti gli account si rivolge a tutti gli account dell'organizzazione. L'opzione Specificare gli account si rivolge solo ai singoli account dell'organizzazione. Se si sceglie questa opzione, è possibile specificare più di un account separando i numeri di conto con una virgola. Puoi anche inserire `SELF` al posto di un ID account per creare una configurazione di scansione per il tuo account

   Se il tuo account è un account autonomo o un account membro di un'organizzazione, puoi selezionare Self per creare una configurazione di scansione per il tuo account.
9. Per Pianificazione, scegli Scansione unica, che viene eseguita non appena hai finito di creare la configurazione di scansione, o Scansioni ricorrenti, che viene eseguita all'ora specificata.
10. Conferma le tue scelte, quindi scegli Crea.

Visualizzazione dei risultati della scansione CIS

Amazon Inspector crea un processo di scansione per ogni configurazione di scansione che viene eseguita e raccoglie i risultati di una scansione con un ID di scansione univoco. I risultati della scansione CIS sono disponibili per 90 giorni. È possibile visualizzare i risultati della scansione CIS tramite i relativi controlli o risorse scansionate:

- Risultati della scansione aggregati per controlli: raggruppa i risultati di una scansione per ogni singolo controllo eseguito durante la scansione. Per ogni controllo, viene visualizzato un rapporto sul numero di risorse non riuscite, ignorate o superate.
- Risultati della scansione aggregati per risorse analizzate: raggruppa i risultati di una scansione per ogni risorsa scansionata a cui è destinata la scansione durante la scansione. Per ogni risorsa, viene visualizzato un rapporto sul numero di controlli non riusciti, ignorati o superati da una risorsa.

Questo argomento descrive come visualizzare i risultati di una scansione CIS.

Per visualizzare i risultati della scansione

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Utilizza il Regione AWS menu a discesa per selezionare Regione AWS dove hai creato la configurazione di scansione CIS.
3. Dal pannello di navigazione, scegli Scansioni su richiesta, quindi scegli Scansioni CIS.
4. Scegli la scheda Risultati della scansione.
5. Nella colonna Pianificato per, scegli l'ID della pianificazione di scansione che desideri visualizzare. Oppure seleziona la riga con l'ID della pianificazione di scansione che desideri visualizzare, quindi scegli Visualizza dettagli.
6. Scegli Controlli per visualizzare ogni controllo eseguito o Risorse scansionate per visualizzare ogni risorsa scansionata presa di mira durante la scansione.

È inoltre possibile visualizzare i dettagli delle scansioni CIS pianificate.

Per visualizzare i dettagli delle scansioni CIS pianificate

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.

2. Utilizza il Regione AWS menu a discesa per selezionare Regione AWS dove hai creato la configurazione di scansione CIS.
3. Dal pannello di navigazione, scegli Scansioni su richiesta, quindi scegli Scansioni CIS.
4. Scegli la scheda Pianificato.
5. Nella colonna Nome della configurazione di scansione, scegli il nome della configurazione di scansione che desideri visualizzare. Oppure seleziona la riga con la configurazione di scansione che desideri visualizzare, quindi scegli Visualizza dettagli.

Modifica di una configurazione di scansione CIS

Questo argomento descrive come modificare una configurazione di scansione CIS.

Per modificare una configurazione di scansione CIS

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Utilizza il Regione AWS menu a discesa per selezionare Regione AWS dove hai creato la configurazione di scansione CIS.
3. Dal pannello di navigazione, scegli Scansioni su richiesta, quindi scegli Scansioni CIS.
4. Scegli la scheda Pianificato.
5. Seleziona la riga con la configurazione di scansione che desideri modificare, quindi scegli Modifica.

Scaricamento dei risultati di una scansione CIS

Puoi scaricare un PDF o CSV di una scansione CIS utilizzando la console o l'API di Amazon Inspector.

> **Note**
>
> Puoi scaricare solo un file CSV dei risultati delle scansioni CIS per le scansioni CIS raccolte dopo il 05/03/2024.

Questo argomento descrive come scaricare una scansione CIS utilizzando la console Amazon Inspector.

Per scaricare i risultati della scansione CIS dalla console

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Utilizza il Regione AWS menu a discesa per selezionare Regione AWS dove hai creato la configurazione di scansione CIS.
3. Dal pannello di navigazione, scegli Scansioni su richiesta, quindi scegli Scansioni CIS.
4. Scegli la scheda Risultati della scansione.
5. Nella colonna Pianificato da, scegli l'ID della pianificazione di scansione che desideri visualizzare. Oppure seleziona la riga con l'ID della pianificazione di scansione che desideri visualizzare, quindi scegli Visualizza dettagli.
6. Scegli Scarica, quindi scegli PDF o CSV. Se il tuo account è l'account amministratore delegato, puoi scegliere Seleziona account per scaricare i risultati per un account membro specifico.

Codice di sicurezza di Amazon Inspector

Amazon Inspector è un servizio di gestione delle vulnerabilità che rileva automaticamente i carichi di lavoro e li analizza continuamente per individuare vulnerabilità del software ed esposizione involontaria alla rete. Con Code Security, Amazon Inspector analizza il codice sorgente dell'applicazione proprietaria, le dipendenze delle applicazioni di terze parti e Infrastructure as Code alla ricerca di vulnerabilità. Puoi attivare Code Security nella console Amazon Inspector o con l'API Amazon Inspector. Una volta attivato Code Security, puoi creare e applicare una configurazione di scansione al tuo repository di codice per determinare con quale frequenza e quando verrà scansionato. È possibile visualizzare, modificare ed eliminare la configurazione di scansione in qualsiasi momento. Per informazioni sui paesi Regioni AWS in cui è disponibile Code Security, consulta Regioni ed endpoint. Per informazioni sui prezzi, consulta i prezzi di Amazon Inspector.

> **Note**
>
> I risultati di sicurezza generati da Amazon Inspector Code Security non sono disponibili per l'integrazione di Amazon Inspector con Security Hub. Tuttavia, puoi accedere a questi risultati particolari nella console Amazon Inspector e tramite l'API Amazon Inspector.

Prerequisiti per la sicurezza del codice

Prima di iniziare a utilizzare Code Security, è necessario attivare Code Security e decidere come crittografare i dati. Possono trattarsi di informazioni come credenziali di integrazione, codice o qualsiasi altra informazione relativa alle integrazioni, agli archivi di codice e ai progetti. Per impostazione predefinita, i dati sono crittografati con una AWS chiave proprietaria. Ciò significa che la chiave viene creata, posseduta e gestita dal servizio. Se desideri possedere e gestire la chiave utilizzata per crittografare i tuoi dati, puoi creare una chiave KMS gestita dal cliente.

Attivazione della sicurezza del codice

Code Security viene attivato nello stesso modo in cui si attivano tutti i tipi di scansione automatica. Per ulteriori informazioni, vedere Attivazione di un tipo di scansione.

Creazione di una chiave di accesso gestita dal cliente AWS KMS

Per impostazione predefinita, i dati sono crittografati con una chiave AWS proprietaria. Ciò significa che la chiave viene creata, posseduta e gestita dal servizio. Se desideri possedere e gestire la

chiave utilizzata per crittografare i tuoi dati, puoi creare una chiave KMS gestita dal cliente. Amazon Inspector non interagisce con i tuoi dati. Amazon Inspector acquisisce solo i metadati dai repository del tuo provider di codice sorgente. Per informazioni su come creare una chiave KMS gestita dal cliente, consulta Creare una chiave KMS nella Guida per l'utente.AWS Key Management Service

Esempio di policy

Quando crei la tua chiave gestita dai clienti, utilizza la seguente politica di esempio.

```
{
    "Version": "2012-10-17",
    "Id": "key-policy",
    "Statement": [
        {
            "Sid": "Allow Q to use Encrypt Decrypt GenerateDataKey and
 GenerateDataKeyWithoutPlaintext",
            "Effect": "Allow",
            "Principal": {
                "Service": "q.amazonaws.com"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "aws:SourceAccount": "111122223333"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:qdeveloper:codesecurity-scope":
 "111122223333"
                },
                "ArnLike": {
                    "aws:SourceArn":
 "arn:aws:inspector2:Region:111122223333:codesecurity-integration/*"
                }
            }
        },
        {
            "Sid": "Allow Q to use DescribeKey",
```

```
            "Effect": "Allow",
            "Principal": {
                "Service": "q.amazonaws.com"
            },
            "Action": "kms:DescribeKey",
            "Resource": "*"
        },
        {
            "Sid": "Allow Inspector to use Encrypt Decrypt GenerateDataKey and
 GenerateDataKeyWithoutPlaintext using FAS",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{111122223333}:role/inspectorCodeSecurity"
            },
            "Action": [
                "kms:Encrypt",
                "kms:Decrypt",
                "kms:GenerateDataKey",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "inspector2.Region.amazonaws.com"
                },
                "StringLike": {
                    "kms:EncryptionContext:aws:qdeveloper:codesecurity-scope":
 "111122223333"
                }
            }
        },
        {
            "Sid": "Allow Inspector to use DescribeKey using FAS",
            "Effect": "Allow",
            "Principal": {
                "AWS": "arn:aws:iam::{111122223333}:role/inspectorCodeSecurity"
            },
            "Action": [
                "kms:DescribeKey"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "kms:ViaService": "inspector2.Region.amazonaws.com"
```

```
                }
            }
        }
    ]
}
```

Dopo aver creato la tua chiave KMS, puoi utilizzare il seguente Amazon APIs Inspector.

- UpdateEncryptionKey — Da utilizzare con `CODE_REPOSITORY` for `resourceType` e `CODE` come tipo di scansione per configurare l'uso della chiave KMS gestita dal cliente.
- GetEncryptionKey — Da utilizzare con `CODE_REPOSITORY` for `resourceType` e `CODE` come tipo di scansione per configurare il recupero della configurazione della chiave KMS.
- ResetEncryptionKey — Da utilizzare con `CODE_REPOSITORY` per `resourceType` `CODE` ripristinare la configurazione della chiave KMS e per utilizzare una AWS chiave KMS di proprietà.

Creazione di un'integrazione tra Amazon Inspector, il tuo repository di codice

Questa sezione include argomenti che descrivono come creare un'integrazione tra Amazon Inspector e il tuo repository di codice. Quando crei un'integrazione, tutti gli archivi di codice vengono elencati come progetti nella console Amazon Inspector nella pagina Code Security. Altri argomenti di questa sezione descrivono come accedere alle integrazioni e ai progetti.

Code Security importa solo fino a 100.000 progetti e viene monitorato solo il ramo predefinito per ogni repository. Un progetto può essere associato a un massimo di tre configurazioni di scansione predefinite.

Code Security supporta solo un massimo di 100 integrazioni per account. Le integrazioni di Code Security non hanno alcun concetto di relazione tra account amministratore account/member delegato.

Per evitare restrizioni, consigliamo di non utilizzare lo stesso host per un'integrazione più di una volta.

Le integrazioni con GitHub SaaS e GitHub Enterprise Server richiedono GitHub Enterprise Cloud l'accesso pubblico a Internet.

> **Important**
>
> Le integrazioni di terze parti potrebbero essere disattivate temporaneamente o permanentemente senza preavviso per qualsiasi motivo, ad esempio per risolvere problemi di sicurezza.

Creazione di un'integrazione tra Amazon Inspector e GitHub

Questo argomento descrive come creare un'integrazione tra Amazon Inspector e. GitHub

> **Note**
>
> Se è la prima volta che crei un'integrazione, ti verrà richiesto di creare una configurazione di scansione predefinita nella Fase 2. Quando crei una configurazione di scansione, scegli la frequenza di scansione, l'analisi di scansione e gli archivi da scansionare. La creazione di una configurazione di scansione predefinita equivale a creare una configurazione di scansione generale. Tuttavia, la configurazione di scansione predefinita viene associata automaticamente a tutti i progetti nuovi ed esistenti importati in Amazon Inspector. Se desideri creare una configurazione di scansione predefinita, scegli Continua con questa configurazione. È possibile creare una configurazione di scansione predefinita solo una volta. Se si crea una configurazione di scansione predefinita, non verrà richiesto di creare nuovamente una configurazione di scansione predefinita. È possibile creare una configurazione di scansione predefinita solo una volta per account e una volta per organizzazione. Se non desideri configurare una configurazione di scansione predefinita, scegli Ignora configurazione. Tuttavia, verrà richiesto di creare una configurazione di scansione predefinita alla successiva creazione di un'integrazione. Dopo aver creato una configurazione di scansione predefinita o aver saltato la creazione di una configurazione di scansione predefinita, verrai indirizzato alla Fase 3 del flusso di lavoro di integrazione in cui inserisci i dettagli dell'integrazione.

Le integrazioni con GitHub SaaS e GitHub Enterprise Server richiedono GitHub Enterprise Cloud l'accesso pubblico a Internet.

> **Note**
>
> Amazon Inspector scansiona e monitora solo la filiale predefinita. Se crei un nuovo ramo predefinito, Amazon Inspector analizza e aggiorna il nuovo ramo predefinito.

> **Important**
>
> Prima di completare la creazione dell'integrazione, ti viene richiesto di autorizzare la connessione tra Amazon Inspector GitHub e. È necessario completare questo passaggio per completare la procedura. Se chiudi il pop-up, non potrai procedere.

Per creare un'integrazione tra Amazon Inspector e GitHub

1. Accedi utilizzando le tue credenziali. Apri la console Amazon Inspector su v2/home. https://console.aws.amazon.com/inspector/
2. Dal pannello di navigazione, scegli Code Security. Scegli Connect a e scegliGitHub.
3. In Dettagli di integrazione, inserisci il nome dell'integrazione e scegli Connetti a GitHub.
4. Scegli Autorizza nel pop-up per creare una connessione tra Amazon Inspector e. GitHub
5. Nel banner di successo, scegli Vai alla pagina di creazione della GitHub connessione.
6. Immettete l'ID di installazione dell'GitHubapplicazione. Se hai installato l'GitHubapplicazione, puoi trovare l'ID GitHub di installazione nella pagina GitHub App o alla fine dell'URL dell'GitHubapplicazione. Se non hai installato l'GitHubapplicazione, scegli Installa una nuova app. Questo ti indirizza verso GitHub dove selezionare l'GitHuborganizzazione e specificare l'ambito del repository.
7. Scegli Connect a GitHub.

Dopo aver creato l'integrazione, è possibile che Amazon Inspector non sia in grado di aggiornare il token di accesso. Ciò può verificarsi se l'host di integrazione non è disponibile o se Amazon Inspector riscontra altri problemi di comunicazione. Per risolvere il problema, puoi riautenticare la connessione dalla scheda Integrazioni nella pagina Code Security. Nella colonna Stato, l'integrazione viene visualizzata come Inattiva e Amazon Inspector offre la possibilità di effettuare nuovamente l'autenticazione. Scegli Riautentica. Verrai reindirizzato al flusso di lavoro di integrazione dove puoi completare la configurazione della connessione.

Se elimini le impostazioni di sistema per l'integrazione, puoi perdere la connessione a tempo indeterminato. In tal caso, è necessario eliminare l'integrazione e creare una nuova integrazione. Quando si elimina un'integrazione, si perdono tutti i progetti e le configurazioni di scansione associate all'integrazione.

Creazione di un'integrazione tra Amazon Inspector e GitLab Self Managed

Questo argomento descrive come creare un'integrazione tra Amazon Inspector e il tuo repository di codice in. GitLab Self Managed

Informazioni obbligatorie

Per creare una connessione è necessario quanto segue:

- Nome dell'integrazione: si tratta del nome aggiunto al corpo dell'integrazione.
- URL dell'endpoint: è l'URL utilizzato per accedere all'GitLab Self Managedistanza.
- Token di accesso personale: il token di accesso personale viene creato GitLab Self Managed da un account amministratore e deve includere i seguenti ambiti:`api`, `read_apiread_repository`, e. `write_repository`

> **Note**
>
> Amazon Inspector scansiona e monitora solo la filiale predefinita. Se crei un nuovo ramo predefinito, Amazon Inspector analizza e aggiorna il nuovo ramo predefinito.

Creazione di un'integrazione tra Amazon Inspector e GitLab Self Managed

La procedura seguente descrive come creare una connessione tra Amazon Inspector e il tuo repository di codice in. GitLab Self Managed

> **Note**
>
> Se è la prima volta che crei un'integrazione, ti verrà richiesto di creare una configurazione di scansione predefinita nella Fase 2. Quando si crea una configurazione di scansione, si sceglie la frequenza di scansione, l'analisi di scansione e gli archivi da scansionare. La creazione di una configurazione di scansione predefinita equivale a creare una configurazione di scansione generale. Tuttavia, la configurazione di scansione predefinita

viene associata automaticamente a tutti i progetti nuovi ed esistenti importati in Amazon Inspector. Se desideri creare una configurazione di scansione predefinita, scegli Continua con questa configurazione. È possibile creare una configurazione di scansione predefinita solo una volta. Se si crea una configurazione di scansione predefinita, non verrà richiesto di creare nuovamente una configurazione di scansione predefinita. È possibile creare una configurazione di scansione predefinita solo una volta per account e una volta per organizzazione. Se non desideri configurare una configurazione di scansione predefinita, scegli Ignora configurazione. Tuttavia, ti verrà richiesto di creare una configurazione di scansione predefinita la prossima volta che crei un'integrazione. Dopo aver creato una configurazione di scansione predefinita o aver saltato la creazione di una configurazione di scansione predefinita, verrai indirizzato alla Fase 3 del flusso di lavoro di integrazione in cui inserisci i dettagli dell'integrazione.

Important

Prima di completare la creazione dell'integrazione, ti viene richiesto di autorizzare la connessione tra Amazon Inspector e Self ManagedGitLab. È necessario completare questo passaggio per completare la procedura. Se chiudi il pop-up, non potrai procedere.

Per creare una connessione con GitLab Self Managed

1. Accedi utilizzando le tue credenziali. Apri la console Amazon Inspector su v2/home. https://console.aws.amazon.com/inspector/
2. Dal pannello di navigazione, scegli Code Security. Scegli Connect to e scegli GitLab Self Managed.
3. In Dettagli di integrazione, inserisci quanto segue:
   a. Per Nome dell'integrazione, inserisci il nome aggiunto al corpo dell'integrazione.
   b. Per Endpoint URL, inserisci l'URL utilizzato per accedere all'istanza GitLab autogestita.
   c. Per Token di accesso personale, inserisci il tuo token di accesso personale con gli ambiti richiesti.
4. Scegli Connetti a. GitLab
5. Scegli Autorizza nella finestra pop-up per completare la creazione di una connessione tra Amazon Inspector e. GitLab

Dopo aver creato l'integrazione, è possibile che si verifichi uno scenario in cui Amazon Inspector non è in grado di aggiornare il token di accesso. Ciò può verificarsi se l'host di integrazione non è disponibile o se Amazon Inspector riscontra altri problemi di comunicazione. Per risolvere il problema, puoi riautenticare la connessione dalla scheda Integrazioni nella pagina Code Security. Nella colonna Stato, l'integrazione viene visualizzata come Inattiva e Amazon Inspector offre la possibilità di effettuare nuovamente l'autenticazione. Scegli Re-autenticate. Verrai reindirizzato al flusso di lavoro di integrazione dove puoi completare la configurazione della connessione.

Se elimini le impostazioni di sistema per l'integrazione, puoi perdere la connessione a tempo indeterminato. In tal caso, è necessario eliminare l'integrazione e creare una nuova integrazione. Quando si elimina un'integrazione, si perdono tutti i progetti e le configurazioni di scansione associate all'integrazione.

Visualizzazione delle integrazioni con gli archivi di codice

Questo argomento descrive come visualizzare le integrazioni nella console Amazon Inspector.

Per visualizzare le integrazioni nella console Amazon Inspector

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Dal pannello di navigazione, scegli Code Security.
3. Scegli Integrations (Integrazioni). Da questa scheda, puoi esaminare tutte le integrazioni configurate e consultare le informazioni di base su tutte le integrazioni. Queste informazioni includono il nome dell'integrazione, lo stato dell'integrazione e il nome del provider del codice sorgente.

Effettua nuovamente l'autenticazione con il provider

Dopo aver creato l'integrazione, è possibile che si verifichi uno scenario in cui Amazon Inspector non è in grado di aggiornare il token di accesso. Ciò può verificarsi se l'host di integrazione non è disponibile o se Amazon Inspector riscontra altri problemi di comunicazione. Per risolvere il problema, puoi riautenticare la connessione dalla scheda Integrazioni nella pagina Code Security. Nella colonna Stato, l'integrazione viene visualizzata come Inattiva e Amazon Inspector offre la possibilità di effettuare nuovamente l'autenticazione. Scegli Re-autenticate. Verrai reindirizzato al flusso di lavoro di integrazione dove puoi completare la configurazione della connessione.

Se elimini le impostazioni di sistema per l'integrazione, puoi perdere la connessione a tempo indeterminato. In tal caso, è necessario eliminare l'integrazione e creare una nuova integrazione. Quando si elimina un'integrazione, si perdono tutti i progetti e le configurazioni di scansione associate all'integrazione.

Visualizzazione degli archivi di codice

L'argomento descrive come visualizzare gli archivi di codice nella console Amazon Inspector.

Per visualizzare gli archivi di codice nella console Amazon Inspector

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Dal pannello di navigazione, scegli Code Security.
3. Scegli Code repositories. Da questa scheda, puoi esaminare tutti i tuoi repository di codice, elencati come progetti, e rivedere le informazioni di base su di essi. Queste informazioni includono il nome e lo stato di scansione di ogni progetto. Puoi anche rivedere le configurazioni associate ai tuoi progetti e la data dell'ultima scansione dei tuoi progetti. Puoi persino filtrare i tuoi progetti nella barra di ricerca.

Visualizzazione dei dettagli di un progetto

Questo argomento descrive come visualizzare i dettagli di un progetto nella console Amazon Inspector. Se il tuo account è l'amministratore delegato di un'organizzazione, puoi visualizzare i dettagli dei progetti che appartengono agli account dei membri.

Per visualizzare i progetti di codice nella console Amazon Inspector

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Dal pannello di navigazione, scegli Code Security.
3. Scegli Code repositories. Da questa scheda, puoi esaminare tutti i tuoi repository di codice, elencati come progetti, e rivedere le informazioni di base su di essi. Queste informazioni includono il nome e lo stato di scansione di ogni progetto. Puoi anche rivedere le configurazioni associate ai tuoi progetti e la data dell'ultima scansione dei tuoi progetti. Puoi persino filtrare i tuoi progetti nella barra di ricerca.

4. Scegliere un progetto. Oppure seleziona un progetto e scegli Visualizza dettagli. Dalla schermata dei dettagli del progetto, puoi visualizzare le informazioni di base sul progetto. Queste informazioni includono il nome e l'ID del progetto, nonché l'ARN di integrazione. Include informazioni su quando il progetto è stato scansionato e sul tipo di fornitura. È anche possibile esaminare i risultati associati al progetto, esportare i risultati e creare regole di soppressione per i risultati.

Eliminazione di un'integrazione

La procedura seguente descrive come eliminare un'integrazione nella console Amazon Inspector. Quando elimini un'integrazione, perdi tutti i progetti e le configurazioni di scansione associate all'integrazione.

Per eliminare un'integrazione nella console Amazon Inspector.

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Dal pannello di navigazione, scegli Code Security.
3. Scegli Integrations (Integrazioni). Da questa scheda, puoi esaminare tutte le integrazioni configurate e consultare le informazioni di base su tutte le integrazioni. Queste informazioni includono il nome dell'integrazione, lo stato dell'integrazione e il tipo di provider di integrazione.
4. Seleziona un'integrazione e scegli Elimina.

Creazione di una configurazione di scansione

Prima di creare una configurazione di scansione, devi creare un'integrazione con Amazon Inspector. La prima volta che crei un'integrazione, ti viene richiesto di creare una configurazione di scansione predefinita. Questo argomento descrive come creare una configurazione di scansione generale. La differenza tra una configurazione di scansione predefinita e una configurazione di scansione generale è che una configurazione di scansione predefinita viene associata automaticamente ai nuovi progetti. È possibile saltare la creazione di una configurazione di scansione predefinita.

Code Security supporta solo un massimo di 500 configurazioni di scansione generali. Code security supporta solo 1 configurazione di scansione predefinita per account e per organizzazione. Una configurazione di scansione può essere associata solo a un massimo di 100.000 progetti.

Un progetto può essere associato a un massimo di 4 configurazioni di scansione in totale. Ciò include una configurazione di scansione predefinita se è stata creata una configurazione di scansione predefinita. Le configurazioni di scansione per un'organizzazione non possono essere contrassegnate.

Se l'amministratore delegato di un'organizzazione crea una configurazione di scansione, la configurazione di scansione viene creata a livello di organizzazione e applicata a tutti gli account membri dell'organizzazione. Lo stesso accade se l'amministratore delegato crea una configurazione di scansione predefinita.

Quando si crea una configurazione di scansione, si sceglie la frequenza di scansione, l'analisi di scansione e gli archivi da scansionare. La frequenza di scansione può essere modificata in base a modifiche periodiche o personalizzate. La scansione periodica e basata sulle modifiche offre la possibilità di abilitare la scansione periodica. Se si abilita la scansione periodica, si imposta la frequenza di scansione sul giorno della settimana o del mese in cui viene eseguita la scansione. La scansione personalizzata offre la possibilità di abilitare la scansione quando il codice viene modificato e la scansione periodica. Se si abilita la scansione quando il codice viene modificato, si specifica il trigger di scansione da includere nelle richieste di unione e estrazione.

Le scansioni possono essere ignorate se un ID di commit non viene modificato entro un determinato periodo di tempo. Per la scansione periodica, le scansioni vengono ignorate se un ID di commit non è cambiato tra le scansioni in 1 settimana. Per le scansioni su richiesta, le scansioni vengono ignorate se un ID di commit non viene modificato tra una scansione e l'altra entro 24 ore.

> **Note**
>
> Se una configurazione di scansione prevede solo trigger per richieste di unione e richieste pull, solo i primi 25 risultati saranno visibili solo nella piattaforma di gestione del codice sorgente. Nessuno sarà visibile in Amazon Inspector.

Per creare una configurazione di scansione generale

1. Accedi utilizzando le tue credenziali. Apri la console Amazon Inspector su v2/home. https://console.aws.amazon.com/inspector/
2. Dal pannello di navigazione, scegli Code Security.
3. Scegli Configurazioni, quindi scegli Crea configurazione di scansione.
4. In Dettagli di scansione, procedi come segue:

- Per Nome di configurazione, immettere un nome per la configurazione di scansione.

5. In Frequenza di scansione, specificate la frequenza di scansione del codice selezionando la scansione periodica e basata sulle modifiche o i tipi e i trigger di scansione personalizzati.

   a. (Opzione 1) Se scegli la scansione periodica e basata sulle modifiche, scegli Abilita scansione periodica o Disattiva scansione periodica.

      - . Se scegli Abilita scansione periodica, imposta la frequenza di scansione scegliendo la settimana e il giorno in cui desideri che il codice venga scansionato.

   b. (Opzione 2) Se scegliete la scansione personalizzata, decidete se abilitare la scansione quando il codice viene modificato e la scansione periodica.

      i. Scegli Abilita la scansione quando il codice viene modificato o Disabilita la scansione quando il codice viene modificato. Se scegli Abilita la scansione quando il codice viene modificato, specifica quando vengono attivate le scansioni dal menu a discesa.

      ii. Scegli Abilita scansione periodica o Disabilita scansione periodica. Se scegli Abilita la scansione periodica, imposta la frequenza di scansione scegliendo la settimana e il giorno in cui desideri che il codice venga scansionato. Puoi anche eseguire la scansione su trigger basati su eventi. Questi eventi includono quando viene aperta una richiesta pull sul ramo predefinito e quando un commit viene inviato al ramo predefinito.

6. In Analisi di scansione, decidi se configurare un'analisi di scansione completa o un'analisi di scansione personalizzata:

   a. (Opzione 1) Se scegliete Analisi di scansione completa, applicate tutte le seguenti analisi di scansione:

      - Test statici di sicurezza delle applicazioni: analizza il codice sorgente alla ricerca di vulnerabilità.
      - Scansione IaC: analizza gli script e il codice che configurano e forniscono l'infrastruttura.
      - Analisi statica della composizione del software: esamina i pacchetti open source nelle applicazioni.

   b. (Opzione 2) Se si sceglie Analisi di scansione personalizzata, è necessario scegliere almeno un tipo dei tipi di analisi di scansione menzionati in precedenza dal menu a discesa:

7. (Facoltativo) Per i tag, create una coppia chiave-valore da applicare al progetto. Puoi creare fino a 50 tag.

8. Scegli Next (Successivo).

9. In Selezione archivio, scegli Tutti gli archivi o Archivi specifici.
    a. (Opzione 1) Se scegli Tutti gli archivi, la scansione è abilitata per tutti gli archivi esistenti.
    b. (Opzione 2) Se si sceglie Archivi specifici, la scansione è abilitata solo per i repository specificati.
10. Scegli Next (Successivo).
11. Rivedi le tue scelte, quindi scegli Crea configurazione di scansione.

> **Note**
>
> Le configurazioni di scansione generali vengono applicate solo a tutti gli archivi di codice esistenti. Non verranno applicate ai nuovi repository di codice.

Visualizzazione delle configurazioni di scansione

La procedura seguente descrive come visualizzare le configurazioni di scansione nella console Amazon Inspector.

> **Note**
>
> Quando visualizzi la configurazione di scansione a livello di organizzazione, alcuni dettagli nella schermata Code Security differiranno in base alla tua. Account AWS

Per visualizzare i dettagli di una configurazione di scansione

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Dal pannello di navigazione, scegli Code Security.
3. Scegli Configurazioni per visualizzare un elenco delle configurazioni di scansione. Se sei l'amministratore delegato, l'elenco include le configurazioni di scansione della tua organizzazione. Puoi vedere il nome di ogni configurazione di scansione e chi ha creato ogni configurazione di scansione (Account AWS ID o ID dell'organizzazione). È inoltre possibile visualizzare i tipi di scansione e il tipo di analisi della scansione applicati alla configurazione. È anche possibile filtrare la configurazione di scansione in base a diversi campi nella barra di ricerca.

Visualizzazione dei dettagli per una configurazione di scansione

La procedura seguente descrive come visualizzare i dettagli di una configurazione di scansione nella console Amazon Inspector.

Per visualizzare i dettagli di una configurazione di scansione

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Dal pannello di navigazione, scegli Code Security.
3. Scegli Configurazioni.
4. Scegli la configurazione di cui desideri visualizzare i dettagli. La schermata dei dettagli della configurazione della scansione fornisce una panoramica della configurazione della scansione. Da questa schermata, è possibile visualizzare la configurazione di scansione ARN, quali tipi di frequenza di scansione sono abilitati e quali tipi di analisi di scansione sono abilitati. È inoltre possibile eliminare la configurazione di scansione da questa schermata. Se stai visualizzando una configurazione di scansione che appartiene alla tua organizzazione, puoi modificarla anche da questa schermata.

Modifica di una configurazione di scansione

È possibile modificare una configurazione di scansione in qualsiasi momento. Quando si modifica una configurazione di scansione, è possibile modificare la frequenza di scansione, l'analisi di scansione, i tag e gli archivi da scansionare. Ad esempio, si modifica una configurazione di scansione per sospendere la scansione di un particolare repository. La procedura seguente descrive come modificare una configurazione di scansione.

Per modificare una configurazione di scansione

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Dal pannello di navigazione, scegli Code Security.
3. Scegli Configurazioni.
4. Seleziona la configurazione che desideri modificare, quindi scegli Modifica. Puoi anche scegliere la configurazione che desideri modificare e quindi scegliere Modifica.

Eliminazione di una configurazione di scansione

È possibile eliminare una configurazione di scansione in qualsiasi momento. Questo argomento descrive come eliminare una configurazione di scansione.

Per eliminare una configurazione di scansione

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Dal pannello di navigazione, scegli Code security.
3. Scegli Configurazioni.
4. Seleziona la configurazione che desideri eliminare, quindi scegli Elimina. Oppure scegli la configurazione che desideri eliminare, quindi scegli Elimina.

Esecuzione di una scansione su richiesta

Puoi eseguire un'operazione su richiesta per i tuoi progetti. Quando si esegue una scansione su richiesta, al progetto selezionato viene applicata un'unione di tutte le configurazioni di scansione configurate. Se il tuo account è l'account amministratore delegato di un'organizzazione, puoi eseguire una scansione su richiesta per i progetti che appartengono agli account dei membri. La procedura seguente descrive come eseguire una scansione su richiesta nella console Amazon Inspector.

Per eseguire una scansione su richiesta

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Dal pannello di navigazione, scegli Code security.
3. Scegli Code repositories.
4. Seleziona il progetto che desideri scansionare, quindi scegli Scansione su richiesta.

Lingue supportate per la sicurezza del codice Amazon Inspector

Questo argomento include le lingue supportate per Amazon Inspector Code Security.

Lingue supportate per SAST

- C#(sono consigliate tutte le versioni tranne la .Net 6.0 e successive)

- C(C11 o versioni precedenti)
- C++(C++17 o precedenti)
- Go(solo Go 1.18)
- Java(Java17 o versioni precedenti)
- JavaScript(EMCMAScript 2021 o precedenti)
- JSX(React 17 o versioni precedenti)
- Kotlin(Kotlin2.0 o precedente)
- PHP(PHP8.2 o precedente)
- Python(Python3.11 o precedente nella serie Python 3)
- Ruby(solo Ruby 2.7 e 3.2)
- Rust
- Scala(Scala3.2.2 o versioni precedenti)
- Shell
- TSX
- TypeScript (tutte le versioni)

Linguaggi supportati per l'analisi della composizione del software

- Go(solo Go 1.18)
- Java(Java17 o versioni precedenti)
- JavaScript(EMCMAScript 2021 o precedenti)
- PHP(PHP8.2 o versioni precedenti)
- Python(Python3.11 o precedente nella serie Python 3)
- .Net
- Ruby(solo Ruby 2.7 e 3.2)
- Rust

Linguaggi per l'infrastruttura come codice

- AWS CDK (PythoneTypeScript)
- AWS CloudFormation (2010-09-09)
- Terraform(1.6.2 o versioni precedenti)

Disattivazione di Code Security

Per ulteriori informazioni sulla disattivazione di Code Security, consulta Disattivazione di un tipo di scansione.

Comprendere i risultati di Amazon Inspector

Amazon Inspector genera un risultato quando rileva una vulnerabilità nelle EC2 istanze Amazon, nelle immagini dei contenitori Amazon ECR e nelle funzioni Lambda. Genera inoltre risultati sulle vulnerabilità del codice rilevate nel codice sorgente di applicazioni di prime parti, nelle dipendenze delle applicazioni di terze parti e nell'infrastruttura come codice. Un risultato è un rapporto dettagliato su una vulnerabilità che interessa una delle tue risorse. AWS

I risultati prendono il nome dalle vulnerabilità e forniscono valutazioni di gravità, informazioni sulle AWS risorse interessate e non, e dettagli che descrivono come correggere AWS le vulnerabilità rilevate. Amazon Inspector archivia tutti i risultati attivi fino a quando non li correggi.

Quando una risorsa viene eliminata, terminata o non è più idonea per la scansione, Amazon Inspector chiude automaticamente i risultati associati alla risorsa e quindi li elimina dopo 3 giorni. Se i risultati vengono chiusi per qualsiasi altro motivo, vengono eliminati dopo 30 giorni.

> **Note**
>
> Amazon Inspector riaprirà un problema risolto entro sette giorni dalla sua chiusura se il problema che ha causato la vulnerabilità si ripresenta.

Se disabiliti Amazon Inspector, i risultati vengono rimossi dopo 24 ore. Se una risorsa viene interrotta, qualsiasi risultato relativo alla risorsa viene rimosso dopo 3 giorni. Lo stesso vale per qualsiasi risultato associato a una risorsa per cui la scansione non è più idonea. Se AWS sospende il tuo account, i risultati vengono rimossi dopo 90 giorni. I risultati relativi alle istanze interrotte rimangono attivi.

I risultati affermano

Amazon Inspector classifica i risultati nei seguenti stati.

Active (Attivo)

Amazon Inspector classifica come Attivo un risultato che non è stato corretto.

Soppresso

Amazon Inspector classifica un risultato soggetto a una o più regole di soppressione come Soppresso.

Closed

Una volta risolto un problema, Amazon Inspector lo classifica come Chiuso.

Argomenti

- Tipi di ricerca di Amazon Inspector
- Visualizzazione dei risultati di Amazon Inspector
- Visualizzazione dei dettagli relativi ai risultati di Amazon Inspector
- Visualizzazione del punteggio di Amazon Inspector e comprensione dei dettagli di vulnerability intelligence
- Comprensione dei livelli di gravità dei risultati di Amazon Inspector

Tipi di ricerca di Amazon Inspector

Questa sezione descrive i diversi tipi di ricerca in Amazon Inspector.

Argomenti

- Vulnerabilità del pacchetto
- Vulnerabilità del codice
- Raggiungibilità della rete

Vulnerabilità del pacchetto

I risultati delle vulnerabilità dei pacchetti identificano i pacchetti software presenti AWS nell'ambiente che sono esposti a vulnerabilità ed esposizioni comuni (). CVEs 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/.

Amazon Inspector può generare rilevamenti di vulnerabilità dei pacchetti per EC2 istanze, 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 aiutano a identificare le righe di codice che possono essere sfruttate. Le vulnerabilità del codice includono crittografia mancante, fughe di dati, difetti di iniezione e crittografia debole. Amazon Inspector genera risultati di vulnerabilità del codice tramite la scansione della funzione Lambda e la funzionalità Code Security.

Amazon Inspector valuta il codice applicativo della funzione Lambda utilizzando il ragionamento automatico e l'apprendimento automatico per analizzare 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

La scansione del codice acquisisce frammenti di codice per evidenziare le vulnerabilità rilevate. Ad esempio, un frammento di codice potrebbe mostrare credenziali codificate o altri materiali sensibili in testo non crittografato. CodeGuru memorizza frammenti di codice associati a vulnerabilità del codice. Per impostazione predefinita, il codice è crittografato con una AWS chiave proprietaria. Tuttavia, puoi creare una chiave gestita dal cliente per crittografare il codice se desideri un maggiore controllo su queste informazioni. Per ulteriori informazioni, consulta Crittografia inattiva per il codice contenuto nei tuoi risultati.

> **Note**
>
> L'amministratore delegato di un'organizzazione non può visualizzare frammenti di codice che appartengono agli account dei membri.

Raggiungibilità della rete

I risultati sulla raggiungibilità della rete indicano che nel tuo ambiente esistono percorsi di rete aperti verso EC2 le istanze Amazon. 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 solo risultati sulla raggiungibilità della rete per le istanze Amazon. EC2 Amazon Inspector esegue scansioni per rilevare la raggiungibilità della rete ogni 12 ore una volta abilitato Amazon Inspector.

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

- EC2 Istanze Amazon
- 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

Visualizzazione dei risultati di Amazon Inspector

Puoi visualizzare i risultati di Amazon Inspector nella console Amazon Inspector e con l'API Amazon Inspector. `ListFindings` Nella console Amazon Inspector, puoi visualizzare i risultati nella dashboard di Amazon Inspector e nella schermata Findings. Puoi anche visualizzare i risultati in AWS Security Hub Amazon Elastic Container Registry (Amazon ECR). Per impostazione predefinita, il pannello di controllo e la schermata Findings di Amazon Inspector mostrano i risultati attivi. Puoi anche visualizzare i risultati per categoria. Le procedure in questa sezione descrivono come visualizzare i risultati nella console Amazon Inspector e con l'API Amazon Inspector.

Console

Per visualizzare i risultati di Amazon Inspector

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. (Facoltativo) Dal pannello di navigazione, scegli Dashboard. La dashboard mostra una panoramica della copertura per l'ambiente e mostra solo i risultati critici.
3. (Facoltativo) Dal riquadro di navigazione, scegli Findings. La schermata Risultati mostra tutti i risultati attivi in una tabella in cui è possibile filtrare i risultati per stato e criteri di filtro. Puoi anche creare regole di soppressione per escludere i risultati dalla visualizzazione. È possibile visualizzare i dettagli di un risultato scegliendo il nome del risultato.
4. (Facoltativo) Dal riquadro di navigazione, scegli una delle seguenti opzioni per visualizzare i risultati per categoria:
   - Per vulnerabilità: mostra le vulnerabilità più critiche.
   - Per account: mostra tutti gli account, la copertura della scansione e il numero totale di risultati con livelli di gravità critici e elevati.

     > **Note**
     > Questa categoria è disponibile solo per gli amministratori delegati.

   - Per esempio: mostra le EC2 istanze Amazon più vulnerabili.

     > **Note**
     > I risultati raggruppati in questa categoria non includono informazioni sulla disponibilità della rete.

   - Per immagine del contenitore: mostra le immagini dei container Amazon ECR più vulnerabili.
   - Per repository di container: mostra i repository più vulnerabili.
   - Per funzione Lambda: mostra le funzioni Lambda più vulnerabili.

API

Per visualizzare i risultati di Amazon Inspector

- Esegui l'operazione ListFindingsAPI. Nella richiesta, specifica FilterCriteria per restituire risultati specifici.

Visualizzazione dei dettagli relativi ai risultati di Amazon Inspector

La procedura in questa sezione descrive come visualizzare i dettagli dei risultati di Amazon Inspector.

Per visualizzare i dettagli di una scoperta

1. Accedi utilizzando le tue credenziali, quindi apri la console Amazon Inspector su v2/home https://console.aws.amazon.com/inspector/
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. Comprensione dei livelli di gravità dei 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 EC2 le istanze, le immagini dei contenitori ECR e le funzioni Lambda. Per ulteriori informazioni, consulta Vulnerabilità del pacchetto.

I risultati delle vulnerabilità dei pacchetti includono Visualizzazione del punteggio di Amazon Inspector e comprensione dei dettagli di vulnerability intelligence anche.

Questo tipo di risultato presenta 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 delle EC2 istanze 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 dal documento Common Vulnerabilities and Exposures (CVEs) 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, come 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, vedereComprensione dei livelli di gravità dei risultati di Amazon Inspector. Sono inclusi i seguenti punteggi, inclusi i vettori di punteggio per ciascuno di essi:
  - Punteggio Exploit Prediction Scoring System (EPSS)
  - Punteggio Inspector
  - CVSS 3.1 di Amazon CVE
  - CVSS 3.1 di NVD
  - CVSS 2.0 di NVD (se applicabile, per versioni precedenti) CVEs
- Vulnerabilità correlate: specifica altre vulnerabilità relative alla scoperta. In genere si tratta di altre versioni CVEs che influiscono sulla stessa versione del pacchetto o altre CVEs appartenenti allo stesso gruppo del CVE trovante, 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 libreria Q Detector.
- Tag del rilevatore: i CodeGuru tag associati al rilevatore CodeGuru utilizzano i tag per classificare i rilevamenti.
- CWE pertinenti: IDs 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 EC2 le istanze. 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' EC2 istanza.
- Percorsi di rete aperti: mostra il percorso di accesso aperto all' EC2 istanza. Seleziona un elemento sul percorso per ulteriori informazioni.
- Correzione: consiglia un metodo per chiudere il percorso di rete aperto.

Visualizzazione del punteggio di Amazon Inspector e comprensione dei dettagli di vulnerability intelligence

Amazon Inspector crea un punteggio per i risultati delle istanze di Amazon Elastic Compute Cloud (Amazon EC2). Puoi visualizzare il punteggio di Amazon Inspector e i dettagli sulle vulnerabilità nella console Amazon Inspector. Il punteggio di Amazon Inspector fornisce dettagli che puoi confrontare con le metriche del Common Vulnerability Scoring System. Questi dettagli sono disponibili solo per

le rilevazioni di vulnerabilità dei pacchetti. Questa sezione descrive come interpretare il punteggio di Amazon Inspector e comprendere i dettagli della vulnerability intelligence.

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 di base e il punteggio di 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.

Privilegio richiesto

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.

Intelligenza 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 CVEs.

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

ATT&CK

Questa sezione mostra le tattiche, le tecniche e le procedure MITRE (TTPs) associate al CVE. TTPs Vengono mostrate le associate, se ce ne sono più di due applicabili TTPs 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.

Comprensione dei livelli di gravità dei risultati di Amazon Inspector

Quando Amazon Inspector genera un risultato, assegna un grado di gravità al risultato. Le valutazioni di gravità ti aiutano a valutare e dare priorità ai risultati. Il grado di gravità di un risultato corrisponde a un punteggio e a un livello numerici: informativo, basso, medio, alto e critico. Amazon Inspector determina il grado di gravità di un risultato in base al tipo di risultato. Questa sezione descrive come Amazon Inspector determina un livello di gravità per ogni tipo di risultato.

Gravità della vulnerabilità dei pacchetti software

Amazon Inspector utilizza il NVD/CVSS punteggio come base per il punteggio di gravità per le vulnerabilità dei pacchetti software. Il NVD/CVSS punteggio è il punteggio di gravità delle vulnerabilità pubblicato da NVD e definito dal CVSS. Il NVD/CVSS punteggio è una composizione di metriche di sicurezza, come la complessità degli attacchi, la maturità del codice degli 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 il riferimento relativo alla scoperta URLs 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, reti peer e VPCs AWS Direct Connect reti. Tutti gli altri servizi, porte e protocolli esposti hanno una classificazione di gravità informativa.

Servizio	Porte TCP	Porte UDP	Classificazione 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

Con Amazon Inspector, puoi gestire i risultati in diversi modi. Puoi filtrare i risultati in base al loro stato. Puoi cercare i risultati in base a criteri di filtro. È possibile creare regole di soppressione per escludere i risultati dall'elenco dei risultati. Puoi anche esportare i risultati in AWS Security Hub Amazon e Amazon EventBridge Simple Storage Service (Amazon S3).

Argomenti

- Filtraggio dei risultati di Amazon Inspector
- Eliminazione dei risultati di Amazon Inspector
- Esportazione dei report dei risultati di Amazon Inspector
- Creazione di risposte personalizzate ai risultati di Amazon Inspector con Amazon EventBridge

Filtraggio dei risultati di Amazon Inspector

Puoi filtrare i risultati di Amazon Inspector utilizzando criteri di filtro. Se un risultato non corrisponde ai criteri di filtro, Amazon Inspector lo esclude dalla visualizzazione. Questa sezione descrive come filtrare i risultati di Amazon Inspector utilizzando criteri di filtro.

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. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su 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. Scegli 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

È possibile creare regole di soppressione per nascondere i risultati che corrispondono ai criteri. Ad esempio, è possibile creare una regola di soppressione per nascondere i risultati in base ai relativi livelli di gravità. Se Amazon Inspector genera un risultato che corrisponde alla tua regola di soppressione, Amazon Inspector elimina il risultato e lo nasconde alla vista. Amazon Inspector archivia i risultati soppressi fino a quando non vengono corretti. Una volta corretto un risultato soppresso, Amazon Inspector chiude il risultato. Puoi visualizzare i risultati soppressi nella console.

Crei regole di soppressione per dare priorità ai risultati più importanti. Le regole di soppressione non hanno alcun impatto sui risultati, poiché si limitano a nasconderli alla vista. Non è possibile creare una regola di soppressione che chiuda o corregga i risultati. Puoi anche eliminare i risultati indesiderati AWS Security Hub con una EventBridge regola Amazon. Le procedure in questa sezione descrivono come creare, visualizzare, modificare ed eliminare una regola di soppressione.

> **Note**
>
> Solo l'amministratore delegato di un'organizzazione può creare e gestire le 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. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su 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, inserisci 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. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.

2. Nel riquadro di navigazione, seleziona Regole di soppressione.
3. Nell'elenco delle regole di soppressione, seleziona il titolo della regola.

Modifica di una regola di soppressione

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

Per modificare le regole di soppressione

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Dal pannello di navigazione, scegli Regole di soppressione.
3. Scegliete il nome della regola di soppressione che desiderate modificare, quindi scegliete Modifica.
4. Apportate le modifiche desiderate, quindi scegliete Salva.

Eliminazione di una regola 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. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su 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 di Amazon Inspector

Un rapporto sui risultati è un file CSV o JSON che fornisce un'istantanea dettagliata dei risultati. Puoi esportare un report dei risultati su Amazon e Amazon EventBridge Simple Storage Service (Amazon S3). AWS Security Hub Quando configuri un rapporto sui risultati, specifichi quali risultati includere in esso. Per impostazione predefinita, il rapporto sui risultati include i dati per tutti i risultati attivi. Se sei l'amministratore delegato di un'organizzazione, il rapporto sui risultati include i dati per tutti gli account dei membri dell'organizzazione. Per personalizzare un rapporto sui risultati, crea e applica un filtro.

Quando esporti un report sui risultati, Amazon Inspector crittografa i dati dei risultati con un AWS KMS key metodo da te specificato. Dopo che Amazon Inspector ha crittografato i dati dei risultati, archivia il report dei risultati in un bucket Amazon S3 da te specificato. La AWS KMS chiave deve essere utilizzata nello Regione AWS stesso bucket Amazon S3. La tua policy AWS KMS chiave deve consentire ad Amazon Inspector di utilizzarlo e la tua policy sui bucket Amazon S3 deve consentire ad Amazon Inspector di aggiungervi oggetti. Dopo aver esportato il report dei risultati, puoi scaricarlo dal tuo bucket Amazon S3 o trasferirlo in una nuova posizione. Puoi anche usare il tuo bucket Amazon S3 come repository per altri report sui risultati esportati.

Questa sezione descrive come esportare un report dei risultati nella console Amazon Inspector. Le seguenti attività richiedono la verifica delle autorizzazioni, la configurazione di un bucket Amazon S3, la configurazione, la configurazione e l'esportazione di AWS KMS key un report sui risultati.

> **Note**
>
> Se esporti un report sui risultati con l'CreateFindingsReportAPI Amazon Inspector, puoi visualizzare solo i risultati attivi. Se desideri visualizzare i risultati eliminati o chiusi, devi specificarli `SUPPRESSED` o inserirli `CLOSED` nei criteri di filtro.

Attività

- Passaggio 1: verifica le tue 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

Passaggio 1: verifica le tue autorizzazioni

> **Note**
>
> Dopo aver esportato un rapporto sui risultati per la prima volta, i passaggi da 1 a 3 sono facoltativi. La procedura da seguire dipende dal fatto che si desideri utilizzare lo stesso bucket Amazon S3 e AWS KMS key per altri report sui risultati esportati. Se desideri esportare un report dei risultati in modo programmatico dopo aver completato i passaggi 1-3, utilizza il CreateFindingsReportfunzionamento dell'API Amazon Inspector.

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 venga utilizzata da Amazon Inspector 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 dati 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. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com Amazon S3 all'indirizzo /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:::amzn-s3-demo-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:

   - *amzn-s3-demo-bucket*è il nome del bucket.
   - *111122223333*è l'ID dell'account per il tuo Account AWS.
   - *Region*è l' Regione AWS applicazione 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 (Bahrein), che ha il codice regionaleme-`south-1`, `inspector2.amazonaws.com` sostituiscilo con nell'istruzione. `inspector2.me-south-1.amazonaws.com`

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 (ARNs) 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.

> **Note**
>
> La procedura seguente serve per aggiornare una chiave esistente per consentire ad Amazon Inspector di utilizzarla. Se non disponi di una chiave esistente, consulta Creating keys nella AWS Key Management Service Developer Guide.

Per aggiornare la politica chiave

1. Accedi utilizzando le tue credenziali, quindi apri la AWS KMS console all'indirizzo https://console.aws.amazon.com/kms.
2. Nel riquadro di navigazione, scegli Chiavi gestite dal cliente.
3. Scegli la chiave KMS che desideri utilizzare per crittografare il rapporto. La chiave deve essere una chiave di crittografia simmetrica (SYMMETRIC_DEFAULT).
4. Nella scheda Policy della chiave, seleziona Modifica. Se non viene visualizzata una politica chiave con il pulsante Modifica, è necessario prima selezionare Passa alla visualizzazione dei criteri.
5. 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/*"
        }
    }
}
```

6. 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.

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

   - *111122223333*è l'ID dell'account per il tuo Account AWS.
   - *Region*è l'opzione 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 (Bahrein), 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 questa condizione ARNs per ogni account aggiuntivo. 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.

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

Fase 4: Configurare ed esportare un rapporto sui risultati

> **Note**
> È possibile esportare solo un rapporto sui risultati alla volta. Se è attualmente in corso un'esportazione, è necessario attendere il completamento dell'esportazione prima di esportare un altro 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. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Nel riquadro 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 contengono i dettagli del punteggio e i riferimenti URLs per ogni risultato. Di seguito è riportato un esempio delle intestazioni CSV di un rapporto sui risultati:

AWS ID dell'account	Tipo di ricerca	Titolo	Descrizione	Primo visualizzato	Ultima visualizzazione	Correzione disponibile	Severità	Stato	Tipo di risorsa	ID risorsa	Tag risorsa	Regione	Dettagli del punteggio	Vettore di attacco	Vettore di attacco CVSS v4	Vettore di attacco CVSS v3	Vettore di attacco CVSS v2	Punteggio base CVSS v4	Punteggio base CVSS v3	Punteggio base CVSS v2	Punteggio di priorità	Punteggio di sfruttabilità	URL di correzione	URL di aggiornamento	URL di aggiornamento Lambda

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 in Amazon EventBridge per i risultati di nuova generazione e i risultati aggregati. Amazon Inspector crea anche un evento per eventuali modifiche allo stato di un risultato. Ciò significa che Amazon Inspector crea un nuovo evento per un risultato quando intraprendi azioni come il riavvio di una risorsa o la modifica dei tag associati a una risorsa. Quando Amazon Inspector crea un nuovo evento per un risultato aggiornato, il risultato `id` rimane invariato.

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

Quando utilizzi EventBridge gli eventi con Amazon Inspector, puoi automatizzare le attività per aiutarti a rispondere ai problemi di sicurezza rivelati dai risultati. Per ricevere notifiche sui risultati di Amazon Inspector in base EventBridge agli eventi, devi creare una EventBridge regola e specificare un obiettivo per Amazon Inspector. La EventBridge regola consente di EventBridge inviare notifiche per i risultati di Amazon Inspector e la destinazione specifica dove inviare le notifiche.

Amazon Inspector invia eventi al bus degli eventi predefinito nel luogo in Regione AWS cui utilizzi attualmente Amazon Inspector. Ciò significa che devi configurare le regole degli eventi per ognuna delle Regione AWS quali hai attivato Amazon Inspector e configurato Amazon Inspector per ricevere eventi. EventBridge Amazon Inspector emette eventi con la massima diligenza possibile.

Questa sezione fornisce un esempio di schema di eventi e descrive come creare una regola. EventBridge

Schema degli eventi

Di seguito è riportato un esempio del formato di evento Amazon Inspector per un evento di EC2 ricerca. Per uno schema di esempio di altri tipi di ricerca e tipi di eventi, vediEventBridge 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 pannello 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. Scegliere Create Subscription (Crea iscrizione).

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 pannello 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 Amazon Q Developer nel client di applicazioni di chat

1. Accedi alla console delle applicazioni di chat di Amazon Q Developer 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 Amazon Q Developer nelle applicazioni di chat per accedere 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 finestra delle AWS Management Console applicazioni di chat di Amazon Q Developer, incolla l'ID del canale che hai copiato da Slack nel campo ID 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 Amazon Q Developer nelle applicazioni di chat. 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 Amazon Q Developer nel client di applicazioni di chat

1. Accedi alla console delle applicazioni di chat di Amazon Q Developer 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 finestra delle AWS Management Console applicazioni di chat di Amazon Q Developer, incolla l'URL che hai copiato nel campo URL 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 Amazon Q Developer nelle applicazioni di chat. 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. Accedi utilizzando le tue credenziali.
2. Apri la EventBridge console Amazon all'indirizzo https://console.aws.amazon.com/events/.
3. Seleziona Regole dal riquadro di navigazione, quindi seleziona Crea regola.
4. Inserisci un nome e una descrizione facoltativa per la regola.
5. Seleziona Regola con uno schema di eventi, quindi Avanti.
6. Nel riquadro Event Pattern, scegli Modelli personalizzati (editor JSON).
7. 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.

8. Nella pagina Seleziona obiettivi, scegli Servizio AWS. Quindi, per Seleziona il tipo di destinazione, scegli l'argomento SNS.
9. Per Argomento, seleziona il nome dell'argomento SNS che hai creato nel passaggio 1. Quindi scegli Successivo.
10. Aggiungi tag opzionali se necessario e scegli Avanti.
11. 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.

Utilizzo del pannello di controllo in Amazon Inspector

La dashboard fornisce un'istantanea delle statistiche aggregate per le risorse scansionate da Amazon Inspector. Utilizza la dashboard per conoscere la copertura del tuo ambiente e i risultati critici.

> **Note**
>
> Se il tuo account è l'account amministratore delegato di un'organizzazione, la dashboard mostra le informazioni relative al tuo account e a tutti gli altri account dell'organizzazione.

Questo argomento descrive come visualizzare la dashboard e comprendere i componenti che la compongono.

Argomenti

- Visualizzazione del pannello di controllo
- Comprensione dei componenti del dashboard e interpretazione dei dati

Visualizzazione del pannello di controllo

La dashboard mostra una panoramica della copertura per l'ambiente in uso e dei risultati critici. La dashboard aggiorna automaticamente i dati ogni cinque minuti. Puoi aggiornare i dati manualmente scegliendo l'icona di aggiornamento nell'angolo in alto a destra dello schermo. È possibile visualizzare i dati di supporto per un elemento selezionando l'elemento.

> **Note**
>
> Se il tuo account è l'account amministratore delegato di un'organizzazione, puoi visualizzare le statistiche aggregate relative a un account membro inserendo l'ID dell'account membro nel campo Account.

Per visualizzare la dashboard:

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.

2. Dal pannello di navigazione, scegli Dashboard.

Comprensione dei componenti del dashboard e interpretazione dei dati

Ogni sezione del pannello di controllo fornisce informazioni dettagliate sulle metriche e sui risultati chiave, in modo da poter comprendere il livello di vulnerabilità delle AWS risorse esistenti. 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 EC2 istanze Amazon, 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, EC2 istanze Amazon 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 di 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 della scansione del codice di Amazon Inspector
- Risultati delle EC2 istanze Amazon
- Risultati delle immagini dei container Amazon ECR
- Risultati della funzione Lambda

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 EC2 istanze Amazon 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' EC2 istanza Amazon interessata.

Amazon Machine Images (AMI) con i risultati più critici

La sezione Amazon Machine Images (AMIs) con i risultati più critici mostra i primi cinque AMIs risultati del tuo ambiente con i risultati più critici. La visualizzazione mostra l'identificatore AMI, l'identificatore dell' AWS account, il numero di EC2 istanze 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 potrebbero richiedere la ricostruzione. AMIs

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 .

Scansione del codice di Amazon Inspector con i risultati più critici

La sezione Progetti con le vulnerabilità del codice più critiche mostra i primi cinque progetti con risultati critici. Puoi scegliere un progetto per visualizzare i dettagli sui risultati. Quando scegli un progetto, vieni indirizzato al repository in cui si trovano i risultati. La scheda dei risultati mostra i nomi dei risultati e i relativi livelli di gravità. Mostra il tipo di analisi utilizzata per generare i risultati. Mostra anche quanti anni hanno i risultati e il loro stato.

Ricerca nel database delle vulnerabilità di Amazon Inspector

Puoi cercare vulnerabilità ed esposizioni comuni (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 visualizzare questi dettagli nella schermata dei dettagli CVE. Amazon Inspector monitora e fornisce informazioni sulle vulnerabilità del software nel database delle vulnerabilità. Amazon Inspector supporta solo CVEs le piattaforme elencate nella sezione Piattaforme di rilevamento della schermata dei dettagli CVE. Questa sezione descrive come effettuare ricerche nel database delle vulnerabilità di Amazon Inspector utilizzando un ID CVE.

> **Note**
>
> 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. Accedi utilizzando le tue credenziali, quindi apri la console Amazon Inspector su v2/home 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.

Esportazione SBOMs con Amazon Inspector

Una distinta base del software (SBOM) è un inventario annidato di tutti i componenti software open source e di terze parti presenti nella codebase. Amazon Inspector fornisce SBOMs risorse individuali nel tuo ambiente. Puoi utilizzare la console Amazon Inspector o l'API Amazon Inspector per SBOMs generare per le tue risorse. Puoi esportare tutte SBOMs le risorse supportate e monitorate da Amazon Inspector. Exported SBOMs fornisce informazioni sulla fornitura di software. È possibile verificare lo stato delle risorse valutando la copertura dell'ambiente. AWS Questa sezione descrive come configurare ed esportare SBOMs.

> **Note**
>
> Attualmente, Amazon Inspector non supporta l'esportazione per istanze Amazon SBOMs Windows. EC2

Formati Amazon Inspector

Amazon Inspector supporta l'esportazione SBOMs in formati compatibili con CycloneDX 1.4 e SPDX 2.3. Amazon Inspector esporta SBOMs come `JSON` file nel bucket Amazon S3 scelto dall'utente.

> **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 SBOMs

Quando esporti, SBOMs puoi includere filtri per creare report per sottoinsiemi specifici di risorse. Se non fornisci un filtro, vengono esportate tutte SBOMs 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 SBOMs per esportare qualsiasi risorsa associata a un ID account specifico.
- EC2 tag di istanza: questo filtro può essere utilizzato SBOMs per esportare EC2 istanze con tag specifici.
- Nome funzione: questo filtro può essere utilizzato SBOMs per esportare funzioni Lambda specifiche.
- Tag immagine: questo filtro può essere utilizzato SBOMs per esportare immagini di contenitori con tag specifici.

- Tag funzione Lambda: questo filtro può essere utilizzato per esportare funzioni SBOMs 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 SBOMs per generare immagini di contenitori in repository specifici.

Configura ed esporta SBOMs

Per esportare SBOMs, devi prima configurare un bucket Amazon S3 e una AWS KMS chiave che Amazon Inspector possa utilizzare. Puoi utilizzare i filtri SBOMs per esportare sottoinsiemi specifici delle tue risorse. SBOMs Per esportare 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. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su 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. SBOMs
4. (Facoltativo) Nella SBOMs pagina Esporta, 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

- SBOMs Per esportare 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

- SBOMs Per esportare le tue risorse usando il AWS Command Line Interface comando seguente:

```
aws inspector2 create-sbom-export --report-format
FORMAT --s3-destination bucketName=amzn-s3-demo-
bucket1,keyPrefix=PREFIX,kmsKeyArn=arn:aws:kms:Region:111122223333:key/123
```

Nella richiesta, *FORMAT* sostituiscilo con il formato che preferisci, `CYCLONEDX_1_4` oppure`SPDX_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.

Schema di EventBridge eventi Amazon per gli eventi Amazon Inspector

Amazon EventBridge fornisce un flusso di dati in tempo reale da applicazioni e altro Servizi AWS alle destinazioni, come AWS Lambda funzioni, argomenti di Amazon Simple Notification Service e flussi di dati in Amazon Kinesis Data Streams. Per supportare l'integrazione con altre applicazioni, servizi e sistemi, Amazon Inspector pubblica automaticamente i risultati su come eventi. EventBridge Puoi utilizzare Amazon Inspector per pubblicare eventi per risultati, copertura e scansioni. Questa sezione fornisce schemi di esempio per gli eventi. EventBridge

Argomenti

- Schema EventBridge di base Amazon per Amazon Inspector
- Esempio di schema di eventi di ricerca di Amazon Inspector
- Esempio di schema di eventi completo per la scansione iniziale di Amazon Inspector
- Esempio di schema degli eventi di copertura di Amazon Inspector
- Esempio di schema di attivazione automatica di Amazon Inspector

Schema EventBridge di base Amazon per Amazon Inspector

Di seguito è riportato un esempio dello schema di base di 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 inclusi 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:

- `detail-type`è impostato su`Inspector2 Finding`.
- `detail`descrive il risultato.
- `detail.resources.tags`è dove vengono archiviati i dati chiave-valore.

Puoi filtrare le schede per visualizzare la ricerca di schemi di eventi per diverse risorse e tipi di ricerca.

Amazon EC2 package vulnerability finding

```
{
    "version": "0",
    "id": "4d621919-f1f4-4201-a0e2-37e4e330ff51",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2024-09-04T17:00:36Z",
    "region": "eu-central-1",
    "resources": [
        "i-12345678901234567"
    ],
    "detail": {
        "awsAccountId": "123456789012",
        "description": "In snapd versions prior to 2.62, snapd failed to properly
 check the destination of symbolic links when extracting a snap. The snap format
 is a squashfs file-system image and so can contain symbolic links and other file
 types. Various file entries within the snap squashfs image (such as icons and
 desktop files etc) are directly read by snapd when it is extracted. An attacker who
```

```
 could convince a user to install a malicious snap which contained symbolic links
 at these paths could then cause snapd to write out the contents of the symbolic
 link destination into a world-readable directory. This in-turn could allow an
 unprivileged user to gain access to privileged information.",
        "epss": {
            "score": 0.00043
        },
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:eu-
central-1:123456789012:finding/FINDING_ID",
        "firstObservedAt": "Wed Sep 04 16:59:44.356 UTC 2024",
        "fixAvailable": "YES",
        "inspectorScore": 4.8,
        "inspectorScoreDetails": {
            "adjustedCvss": {
                "adjustments": [],
                "cvssSource": "UBUNTU_CVE",
                "score": 4.8,
                "scoreSource": "UBUNTU_CVE",
                "scoringVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Wed Sep 04 16:59:44.476 UTC 2024",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 4.8,
                    "scoringVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:L/I:L/A:L",
                    "source": "UBUNTU_CVE",
                    "version": "3.1"
                },
                {
                    "baseScore": 7.3,
                    "scoringVector": "CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H",
                    "source": "NVD",
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
                "https://www.cve.org/CVERecord?id=CVE-2024-29069",
                "https://ubuntu.com/security/notices/USN-6940-1"
            ],
            "relatedVulnerabilities": [
```

```
                "USN-6940-1"
            ],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2024/
CVE-2024-29069.html",
            "vendorCreatedAt": "Thu Jul 25 20:15:00.000 UTC 2024",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2024-29069",
            "vulnerablePackages": [
                {
                    "arch": "ALL",
                    "epoch": 0,
                    "fixedInVersion": "0:2.63+22.04ubuntu0.1",
                    "name": "snapd",
                    "packageManager": "OS",
                    "remediation": "apt-get update && apt-get upgrade",
                    "version": "2.63"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsEc2Instance": {
                        "iamInstanceProfileArn":
 "arn:aws:iam::123456789012:instance-profile/AmazonSSMRoleForInstancesQuickSetup",
                        "imageId": "ami-02ff980600c693b38",
                        "ipV4Addresses": [
                            "1.23.456.789",
                            "123.45.67.890"
                        ],
                        "ipV6Addresses": [],
                        "launchedAt": "Wed Sep 04 16:57:40.000 UTC 2024",
                        "platform": "UBUNTU_22_04",
                        "subnetId": "subnet-12345678",
                        "type": "t2.small",
                        "vpcId": "vpc-12345678"
                    }
                },
```

```
                "id": "i-12345678901234567",
                "partition": "aws",
                "region": "eu-central-1",
                "type": "AWS_EC2_INSTANCE"
            }
        ],
        "severity": "MEDIUM",
        "status": "CLOSED",
        "title": "CVE-2024-29069 - snapd",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Wed Sep 04 17:00:36.951 UTC 2024"
    }
}
```

Amazon EC2 network reachability finding

```
{
    "version": "0",
    "id": "9eb1603b-4263-19ec-8be2-33184694cb92",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2024-09-05T13:06:56Z",
    "region": "eu-central-1",
    "resources": ["i-12345678901234567"],
    "detail": {
        "awsAccountId": "123456789012",
        "description": "On the instance i-12345678901234567, the port range
 22-22 is reachable from the InternetGateway igw-261bab4d from an attached ENI
 eni-094ad651219472857.",
        "findingArn": "arn:aws:inspector2:eu-
central-1:123456789012:finding/FINDING_ID",
        "firstObservedAt": "Thu Sep 05 13:06:56.334 UTC 2024",
        "lastObservedAt": "Thu Sep 05 13:06:56.334 UTC 2024",
        "networkReachabilityDetails": {
            "networkPath": {
                "steps": [{
                    "componentId": "igw-261bab4d",
                    "componentType": "AWS::EC2::InternetGateway"
                }, {
                    "componentId": "acl-171b527d",
```

```
                    "componentType": "AWS::EC2::NetworkAcl"
                }, {
                    "componentId": "sg-0d34debf87410f2d9",
                    "componentType": "AWS::EC2::SecurityGroup"
                }, {
                    "componentId": "eni-094ad651219472857",
                    "componentType": "AWS::EC2::NetworkInterface"
                }, {
                    "componentId": "i-12345678901234567",
                    "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::123456789012:instance-
profile/AmazonSSMRoleForInstancesQuickSetup",
                    "imageId": "ami-02ff980600c693b38",
                    "ipV4Addresses": ["1.23.456.789", "123.45.67.890"],
                    "ipV6Addresses": [],
                    "launchedAt": "Wed Sep 04 17:41:24.000 UTC 2024",
                    "platform": "UBUNTU_22_04",
                    "subnetId": "subnet-12345678",
                    "type": "t2.small",
                    "vpcId": "vpc-12345678"
                }
            },
            "id": "i-12345678901234567",
            "partition": "aws",
            "region": "eu-central-1",
            "type": "AWS_EC2_INSTANCE"
        }],
```

```
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "Port 22 is reachable from an Internet Gateway - TCP",
        "type": "NETWORK_REACHABILITY",
        "updatedAt": "Thu Sep 05 13:06:56.334 UTC 2024"
    }
}
```

Amazon ECR package vulnerability finding

```
{
    "version": "0",
    "id": "5325facf-a1aa-7d97-6bce-25fde6f6d2fc",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2024-09-04T16:55:38Z",
    "region": "eu-central-1",
    "resources": [
        "arn:aws:ecr:eu-central-1:123456789012:repository/inspector2/
sha256:84f507df33c6864d49c296fb734192696e4cb6f78166ac51ac8b9b118181085d"
    ],
    "detail.resources.tags.testkey": "allow",
    "detail": {
        "awsAccountId": "123456789012",
        "description": "Possible denial of service in X.509 name checks",
        "epss": {
            "score": 0.00045
        },
        "exploitAvailable": "NO",
        "findingArn": "arn:aws:inspector2:eu-
central-1:123456789012:finding/FINDING_ID",
        "firstObservedAt": "Wed Sep 04 16:55:38.411 UTC 2024",
        "fixAvailable": "YES",
        "lastObservedAt": "Wed Sep 04 16:55:38.411 UTC 2024",
        "packageVulnerabilityDetails": {
            "cvss": [],
            "referenceUrls": [
                "https://www.cve.org/CVERecord?id=CVE-2024-6119",
                "https://ubuntu.com/security/notices/USN-6986-1"
            ],
```

```
            "relatedVulnerabilities": [
                "USN-6986-1"
            ],
            "source": "UBUNTU_CVE",
            "sourceUrl": "https://people.canonical.com/~ubuntu-security/cve/2024/
CVE-2024-6119.html",
            "vendorCreatedAt": "Tue Sep 03 00:00:00.000 UTC 2024",
            "vendorSeverity": "medium",
            "vulnerabilityId": "CVE-2024-6119",
            "vulnerablePackages": [
                {
                    "arch": "ARM64",
                    "epoch": 0,
                    "fixedInVersion": "0:3.0.13-0ubuntu3.4",
                    "name": "libssl3t64",
                    "packageManager": "OS",
                    "release": "0ubuntu3.2",
                    "remediation": "apt-get update && apt-get upgrade",
                    "sourceLayerHash":
 "sha256:1567e7ea90b67fc95ccdeeec39bdc3045098dee7e0c604975b957a9f8c0e9616",
                    "version": "3.0.13"
                },
                {
                    "arch": "ARM64",
                    "epoch": 0,
                    "fixedInVersion": "0:3.0.13-0ubuntu3.4",
                    "name": "openssl",
                    "packageManager": "OS",
                    "release": "0ubuntu3.2",
                    "remediation": "apt-get update && apt-get upgrade",
                    "sourceLayerHash":
 "sha256:1567e7ea90b67fc95ccdeeec39bdc3045098dee7e0c604975b957a9f8c0e9616",
                    "version": "3.0.13"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
```

```
                    "awsEcrContainerImage": {
                        "architecture": "arm64",
                        "imageHash":
 "sha256:84f507df33c6864d49c296fb734192696e4cb6f78166ac51ac8b9b118181085d",
                        "imageTags": [
                            "ubuntu_latest"
                        ],
                        "platform": "UBUNTU_24_04",
                        "pushedAt": "Wed Sep 04 16:55:28.000 UTC 2024",
                        "registry": "123456789012",
                        "repositoryName": "inspector2"
                    }
                },
                "id": "arn:aws:ecr:eu-central-1:123456789012:repository/inspector2/
sha256:84f507df33c6864d49c296fb734192696e4cb6f78166ac51ac8b9b118181085d",
                "partition": "aws",
                "region": "eu-central-1",
                "type": "AWS_ECR_CONTAINER_IMAGE"
            }
        ],
        "severity": "MEDIUM",
        "status": "ACTIVE",
        "title": "CVE-2024-6119 - libssl3t64, openssl",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Wed Sep 04 16:55:38.411 UTC 2024"
    }
}
```

Lambda package vulnerability finding

```
{
    "version": "0",
    "id": "9eadd71a-e49c-9864-6ba9-2a5d3f83c88f",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2024-09-04T16:50:37Z",
    "region": "eu-central-1",
    "resources": [
        "arn:aws:lambda:eu-central-1:123456789012:function:VulnerableFunction:
$LATEST"
```

```
    ],
    "detail": {
        "awsAccountId": "123456789012",
        "description": "Flask is a lightweight WSGI web application framework. When
 all of the following conditions are met, a response containing data intended for
 one client may be cached and subsequently sent by the proxy to other clients. If
 the proxy also caches `Set-Cookie` headers, it may send one client's `session`
 cookie to other clients. The severity depends on the application's use of the
 session and the proxy's behavior regarding cookies. The risk depends on all these
 conditions being met.\n\n1. The application must be hosted behind a caching proxy
 that does not strip cookies or ignore responses with cookies. 2. The application
 sets `session.permanent = True` 3. The application does not access or modify the
 session at any point during a request. 4. `SESSION_REFRESH_EACH_REQUEST` enabled
 (the default). 5. The application does not set a `Cache-Control` header to indicate
 that a page is private or should not be cached.\n\nThis happens because vulnerable
 versions of Flask only set the `Vary: Cookie` header when the session is ac",
        "epss": {
            "score": 0.00208
        },
        "exploitAvailable": "YES",
        "exploitabilityDetails": {
            "lastKnownExploitAt": "Sat Aug 31 00:04:50.000 UTC 2024"
        },
        "findingArn": "arn:aws:inspector2:eu-
central-1:123456789012:finding/FINDING_ID",
        "firstObservedAt": "Wed Sep 04 16:50:37.627 UTC 2024",
        "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:H/I:N/A:N",
                "version": "3.1"
            }
        },
        "lastObservedAt": "Wed Sep 04 16:50:37.627 UTC 2024",
        "packageVulnerabilityDetails": {
            "cvss": [
                {
                    "baseScore": 7.5,
                    "scoringVector": "CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:N/A:N",
                    "source": "NVD",
```

```
                    "version": "3.1"
                }
            ],
            "referenceUrls": [
                "https://www.debian.org/security/2023/dsa-5442",
                "https://lists.debian.org/debian-lts-announce/2023/08/msg00024.html"
            ],
            "relatedVulnerabilities": [],
            "source": "NVD",
            "sourceUrl": "https://nvd.nist.gov/vuln/detail/CVE-2023-30861",
            "vendorCreatedAt": "Tue May 02 18:15:52.000 UTC 2023",
            "vendorSeverity": "HIGH",
            "vendorUpdatedAt": "Sun Aug 20 21:15:09.000 UTC 2023",
            "vulnerabilityId": "CVE-2023-30861",
            "vulnerablePackages": [
                {
                    "epoch": 0,
                    "filePath": "requirements.txt",
                    "fixedInVersion": "2.3.2",
                    "name": "flask",
                    "packageManager": "PIP",
                    "version": "2.0.0"
                }
            ]
        },
        "remediation": {
            "recommendation": {
                "text": "None Provided"
            }
        },
        "resources": [
            {
                "details": {
                    "awsLambdaFunction": {
                        "architectures": [
                            "X86_64"
                        ],
                        "codeSha256": "O7jkFEmfPB+CK3Y6Pby5zW9gjG
+zusAaqRRMGS8B27c=",
                        "executionRoleArn": "arn:aws:iam::123456789012:role/service-
role/VulnerableFunction-role-f9vs5mq8",
                        "functionName": "VulnerableFunction",
                        "lastModifiedAt": "Wed Sep 04 16:50:20.000 UTC 2024",
                        "packageType": "ZIP",
```

```
                        "runtime": "PYTHON_3_11",
                        "version": "$LATEST"
                    }
                },
                "id": "arn:aws:lambda:eu-
central-1:123456789012:function:VulnerableFunction:$LATEST",
                "partition": "aws",
                "region": "eu-central-1",
                "type": "AWS_LAMBDA_FUNCTION"
            }
        ],
        "severity": "HIGH",
        "status": "ACTIVE",
        "title": "CVE-2023-30861 - flask",
        "type": "PACKAGE_VULNERABILITY",
        "updatedAt": "Wed Sep 04 16:50:37.627 UTC 2024"
    }
}
```

Lambda code vulnerability finding

```
{
    "version": "0",
    "id": "e764f7be-f931-ff1b-204b-8cab2d91724b",
    "detail-type": "Inspector2 Finding",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2024-09-04T16:51:01Z",
    "region": "eu-central-1",
    "resources": [
        "arn:aws:lambda:eu-central-1:123456789012:function:VulnerableFunction:
$LATEST"
    ],
    "detail": {
        "awsAccountId": "123456789012",
        "codeVulnerabilityDetails": {
            "cwes": [
                "CWE-798"
            ],
            "detectorId": "python/hardcoded-credentials@v1.0",
            "detectorName": "Hardcoded credentials",
```

```
            "detectorTags": [
                "secrets",
                "security",
                "owasp-top10",
                "top25-cwes",
                "cwe-798",
                "Python"
            ],
            "filePath": {
                "endLine": 6,
                "fileName": "lambda_function.py",
                "filePath": "lambda_function.py",
                "startLine": 6
            },
            "ruleId": "python-detect-hardcoded-aws-credentials"
        },
        "description": "Access credentials, such as passwords and access keys,
 should not be hardcoded in source code. Hardcoding credentials may cause leaks even
 after removing them. This is because version control systems might retain older
 versions of the code. Credentials should be stored securely and obtained from the
 runtime environment.",
        "findingArn": "arn:aws:inspector2:eu-
central-1:123456789012:finding/FINDING_ID",
        "firstObservedAt": "Wed Sep 04 16:51:01.869 UTC 2024",
        "lastObservedAt": "Wed Sep 04 16:51:01.869 UTC 2024",
        "remediation": {
            "recommendation": {
                "text": "Your code uses hardcoded AWS credentials which might
 allow unauthorized users access to your AWS account. These attacks can occur
 a long time after the credentials are removed from the code. We recommend that
 you set AWS credentials with environment variables or an AWS profile instead.
 You should consider deleting the affected account or rotating the secret key
 and then monitoring Amazon CloudWatch for unexpected activity.\n[https://
boto3.amazonaws.com/v1/documentation/api/latest/guide/credentials.html](https://
boto3.amazonaws.com/v1/documentation/api/latest/guide/credentials.html)"
            }
        },
        "resources": [
            {
                "details": {
                    "awsLambdaFunction": {
                        "architectures": [
                            "X86_64"
                        ],
```

```
                        "codeSha256": "O7jkFEmfPB+CK3Y6Pby5zW9gjG
+zusAaqRRMGS8B27c=",
                        "executionRoleArn": "arn:aws:iam::123456789012:role/service-
role/VulnerableFunction-role-f9vs5mq8",
                        "functionName": "VulnerableFunction",
                        "lastModifiedAt": "Wed Sep 04 16:50:20.000 UTC 2024",
                        "packageType": "ZIP",
                        "runtime": "PYTHON_3_11",
                        "version": "$LATEST"
                    }
                },
                "id": "arn:aws:lambda:eu-
central-1:123456789012:function:VulnerableFunction:$LATEST",
                "partition": "aws",
                "region": "eu-central-1",
                "type": "AWS_LAMBDA_FUNCTION"
            }
        ],
        "severity": "CRITICAL",
        "status": "ACTIVE",
        "title": "CWE-798 - Hardcoded credentials",
        "type": "CODE_VULNERABILITY",
        "updatedAt": "Wed Sep 04 16:51:01.869 UTC 2024"
    }
}
```

> **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"
    }
}
```

Esempio di schema di attivazione automatica di Amazon Inspector

L'evento di attivazione automatica viene inviato all'amministratore delegato quando Amazon Inspector non è in grado di supportare il numero di membri di un'organizzazione. I seguenti campi identificano un evento di attivazione automatica:

- Il `detail-type` campo è impostato su. `Inspector2 AutoEnable`
- L'`detail`oggetto descrive il motivo per cui l'evento di attivazione automatica non è riuscito.

```
{
    "version": "0",
    "id": "85fc3613-e913-7fc4-a80c-a3753e4aa9ae",
    "detail-type": "Inspector2 AutoEnable",
    "source": "aws.inspector2",
    "account": "123456789012",
    "time": "2024-08-21T02:36:48Z",
    "region": "us-east-1",
    "detail": {
        “version”: “1.0.0”,
        “AutoEnableStatus”: “Failed”,
        “Reason”: "The number of member accounts enabled with AWS Inspector has reached
 the maximum limit of 10,000"
        }
}
```

Il plug-in Amazon Inspector SSM per Linux e Windows

Questo argomento descrive il plug-in Amazon Inspector SSM per Linux e Windows istanze.

Il plug-in Amazon Inspector SSM per Linux

Amazon Inspector utilizza il plug-in Amazon Inspector SSM per eseguire scansioni di ispezione approfondite su istanze Linux. Il plug-in Amazon Inspector SSM viene installato automaticamente sulle istanze Linux presenti nella directory. `/opt/aws/inspector/bin` Il nome dell'eseguibile è. `inspectorssmplugin`

Amazon Inspector utilizza Systems Manager Distributor per distribuire il plug-in sulla tua istanza. Per eseguire scansioni di ispezione approfondita, Systems Manager Distributor e Amazon Inspector devono supportare il sistema operativo delle istanze EC2 Amazon. Per informazioni sui sistemi operativi supportati da Systems Manager Distributor, vedere Piattaforme e architetture di pacchetti supportate nella Guida per l'AWS Systems Manager utente.

Amazon Inspector crea directory di file per gestire i dati raccolti per l'ispezione approfondita dal plug-in Amazon Inspector SSM. Queste directory di file includono e. `/opt/aws/inspector/var/input` `/opt/aws/inspector/var/output`

Il `packages.txt` file `/opt/aws/inspector/var/output` memorizza i percorsi completi dei pacchetti rilevati da Deep Inspection. Se Amazon Inspector rileva lo stesso pacchetto più volte sull'istanza, il `packages.txt` 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 SSM `InspectorLinuxDistributor-do-not-delete` proverà a reinstallare il file all'intervallo di scansione successivo. `inspectorssmplugin`

Se disattivi Amazon EC2 Scanning, il plugin verrà automaticamente disinstallato da tutti gli host Linux.

Il plug-in Amazon Inspector SSM per Windows

Il plug-in Amazon Inspector SSM è necessario per consentire ad Amazon Inspector di eseguire la scansione del Windows istanze. Il plug-in Amazon Inspector SSM viene installato automaticamente sul 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.

> **Note**
>
> È possibile utilizzare… Windows istanze con l'impostazione Default Host Management Configuration. Tuttavia, è necessario creare o utilizzare un ruolo configurato con le `ssm:GetParameter` autorizzazioni `ssm:PutInventory` e.

Disinstallazione del plug-in Amazon Inspector SSM

Se il `InspectorSsmPlugin.exe` file viene eliminato inavvertitamente, l'`InspectorDistributor-do-not-delete`associazione lo reinstallerà al momento successivo `InspectorSsmPlugin.exe` Windows intervallo di scansione. Se desideri disinstallare il plug-in Amazon Inspector SSM, puoi utilizzare l'azione di disinstallazione nel documento. `AmazonInspector2-ConfigureInspectorSsmPlugin` Tuttavia, il plug-in Amazon Inspector SSM verrà disinstallato automaticamente da tutti Windows host se disattivi Amazon Scan EC2 .

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

Generatore SBOM Amazon Inspector

Una Software Bill of Materials (SBOM) è un elenco formalmente strutturato di componenti, librerie e moduli necessari per creare un software. Amazon Inspector SBOM Generator (Sbomgen) è uno strumento che produce un SBOM per archivi, immagini di container, directory, sistemi locali, compilati e binari. Go Rust Sbomgenanalizza i file che contengono informazioni sui pacchetti installati. Quando Sbomgen trova un file pertinente, estrae i nomi dei pacchetti, le versioni e altri metadati. Sbomgenquindi trasforma i metadati del pacchetto in un SBOM. CycloneDX Puoi utilizzarlo Sbomgen per generare lo CycloneDX SBOM come file o in STDOUT e inviarlo ad Amazon SBOMs Inspector per il rilevamento delle vulnerabilità. Puoi anche utilizzarlo Sbomgen come parte dell' CI/CD integrazione, che scansiona automaticamente le immagini dei container come parte della tua pipeline di distribuzione.

Tipi di pacchetti supportati

Sbomgenraccoglie l'inventario per i seguenti tipi di pacchi:

- Alpine APK
- Debian/Ubuntu DPKG
- Red Hat RPM
- C#
- Go
- Java
- Node.js
- PHP
- Python
- Ruby
- Rust

Controlli di configurazione dell'immagine del contenitore supportati

Sbomgenpuò scansionare file Dockerfile autonomi e creare una cronologia da immagini esistenti per individuare problemi di sicurezza. Per ulteriori informazioni, consulta Amazon Inspector Dockerfile checks.

Installazione di Sbomgen

Sbomgenè disponibile solo per i sistemi operativi Linux.

È necessario averlo Docker installato se si desidera analizzare Sbomgen le immagini memorizzate nella cache locale. Dockernon è necessario analizzare le immagini esportate come `.tar` file o le immagini ospitate in registri di container remoti.

Amazon Inspector consiglia l'esecuzione Sbomgen da un sistema con almeno le seguenti specifiche hardware:

- CPU a 4 core
- 8 GB RAM

Per installare Sbomgen

1. Scarica il file Sbomgen zip più recente 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

   In alternativa, puoi scaricare le versioni precedenti del file zip di Amazon Inspector SBOM Generator.
2. Decomprimi il download utilizzando il seguente comando:

   ```
   unzip inspector-sbomgen.zip
   ```
3. Verificate la presenza dei seguenti file nella directory estratta:

   - `inspector-sbomgen`— Questo è lo strumento che eseguirete per generare SBOMs.
   - `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 dello Sbomgen strumento.
   - `sbom.json`— Questa è una CycloneDX SBOM per lo strumento. Sbomgen

- `WhatsNew.txt`— Questo file contiene un registro delle modifiche riepilogativo, in modo da poter visualizzare rapidamente le principali modifiche e miglioramenti tra le Sbomgen versioni.

4. (Facoltativo) Verifica l'autenticità e l'integrità dello strumento utilizzando il seguente comando:

   ```
   sha256sum < inspector-sbomgen
   ```

   - Confrontate i risultati con il contenuto del `checksums.txt` file.

5. Concedi le autorizzazioni eseguibili allo strumento utilizzando il seguente comando:

   ```
   chmod +x inspector-sbomgen
   ```

6. Verificate che Sbomgen sia installato correttamente utilizzando il seguente comando:

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

   L'output dovrebbe essere simile al seguente:

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

Uso di Sbomgen

Questa sezione descrive diversi modi di utilizzoSbomgen. Puoi saperne di più su come utilizzare Sbomgen tramite esempi incorporati. Per visualizzare questi esempi, esegui il `list-examples` comando:

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

Genera un SBOM per un'immagine del contenitore e restituisci il risultato

È possibile Sbomgen utilizzarlo per generare immagini SBOMs per il contenitore e inviare il risultato in un file. Questa funzionalità può essere abilitata utilizzando il `container` sottocomando.

Comando della di esempio

Nel frammento seguente, puoi sostituirlo *`image:tag`* con l'ID dell'immagine e *`output_path.json`* con il percorso dell'output che desideri salvare.

```
# generate SBOM for container image
./inspector-sbomgen container --image image:tag -o output_path.json
```

> **Note**
>
> Il tempo e le prestazioni di scansione dipendono dalle dimensioni dell'immagine e dal numero ridotto di livelli. Immagini più piccole non solo migliorano Sbomgen le prestazioni, ma riducono anche la potenziale superficie di attacco. Le immagini più piccole migliorano anche i tempi di creazione, download e caricamento delle immagini.

Quando viene utilizzata Sbomgen con `ScanSbom`, l'API Amazon Inspector Scan non elabora prodotti SBOMs contenenti più di 5.000 pacchetti. In questo scenario, l'API Amazon Inspector Scan restituisce una risposta HTTP 400.

Se un'immagine include file o directory multimediali in blocco, valuta la possibilità di escluderli dall'Sbomgenutilizzo dell'argomento. `--skip-files`

Esempio: casi di errore comuni

La scansione delle immagini dei contenitori può fallire a causa dei seguenti errori:

- `InvalidImageFormat`— Si verifica durante la scansione di immagini di contenitori non valide con intestazioni TAR, file manifest o file di configurazione danneggiati.
- `ImageValidationFailure`— Si verifica quando la convalida del checksum o della lunghezza del contenuto non riesce per i componenti dell'immagine del contenitore, ad esempio intestazioni Content-Length non corrispondenti, digest del manifesto errati o verifica del checksum non riuscita. SHA256
- `ErrUnsupportedMediaType`— Si verifica quando i componenti dell'immagine includono tipi di supporti non supportati. Per informazioni sui tipi di file multimediali supportati, consultate Sistemi operativi e tipi di supporti supportati.

Amazon Inspector non supporta questo tipo di `application/vnd.docker.distribution.manifest.list.v2+json` supporto. Tuttavia, Amazon Inspector supporta gli elenchi di manifest. Durante la scansione di immagini che utilizzano elenchi manifest, puoi specificare in modo esplicito quale piattaforma utilizzare con l'`--platform`argomento. Se l'`--platform`argomento non è specificato, Amazon Inspector SBOM Generator seleziona automaticamente il manifesto in base alla piattaforma su cui è in esecuzione.

Genera un SBOM da directory e archivi

È possibile utilizzarlo Sbomgen per generare a SBOMs partire da cartelle e archivi. Questa funzionalità può essere abilitata utilizzando i `directory` `archive` sottocomandi o. Amazon Inspector consiglia di utilizzare questa funzionalità quando desideri generare un SBOM da una cartella di progetto, ad esempio un repository git scaricato.

Comando di esempio 1

Il frammento seguente mostra un sottocomando che genera un SBOM da un file di directory.

```
# generate SBOM from directory
./inspector-sbomgen directory --path /path/to/dir -o /tmp/sbom.json
```

Esempio di comando 2

Il frammento seguente mostra un sottocomando che genera un SBOM da un file di archivio. Gli unici formati di archivio supportati sono, e. `.zip` `.tar` `.tar.gz`

```
# generate SBOM from archive file (tar, tar.gz, and zip formats only)
./inspector-sbomgen archive --path testData.zip -o /tmp/sbom.json
```

Genera un SBOM da Go o Rust compilati file binari

È possibile utilizzarlo Sbomgen per generare SBOMs da file compilati Go e binari. Rust È possibile abilitare questa funzionalità tramite il sottocomando: `binary`

```
./inspector-sbomgen binary --path /path/to/your/binary
```

Genera un SBOM dai volumi montati

Puoi utilizzare Amazon Inspector SBOM Generator per generare SBOMs da volumi montati. Questa funzionalità può essere abilitata utilizzando il sottocomando. `volume` Ti consigliamo di utilizzare questa funzionalità quando desideri analizzare volumi di storage, come i volumi Amazon EBS che sono stati montati sul tuo sistema. A differenza del sottocomando directory, la scansione dei volumi montati rileva i pacchetti del sistema operativo e le informazioni sul sistema operativo.

Puoi scansionare un volume Amazon EBS collegandolo a un' EC2 istanza Amazon in cui è installato Amazon Inspector SBOM Generator e montandolo su quell'istanza. Per i volumi Amazon EBS

attualmente utilizzati da altre EC2 istanze Amazon, puoi creare uno snapshot Amazon EBS del volume e quindi creare un nuovo volume Amazon EBS da quello snapshot per scopi di scansione. Per ulteriori informazioni su Amazon EBS, consulta What is Amazon EBS? nella Guida per l'utente di Amazon Elastic Block Store.

Comando della di esempio

Il seguente frammento mostra un sottocomando che genera un SBOM da un volume montato. L'`--path`argomento deve specificare la directory principale in cui è montato il volume.

```
# generate SBOM from mounted volume
./inspector-sbomgen volume --path /mount/point/of/volume/root
```

Comando della di esempio

Il frammento seguente mostra un sottocomando che genera un SBOM da un volume montato escludendo percorsi di file specifici con l'argomento. `--exclude-suffix` L'`--exclude-suffix`argomento è particolarmente utile quando un volume contiene file di massa (come file di registro o file multimediali). I file e le directory i cui percorsi terminano con i suffissi specificati verranno esclusi dalla scansione, il che può ridurre i tempi di scansione e l'utilizzo della memoria.

```
# generate SBOM from mounted volume with exclusions
./inspector-sbomgen volume --path /mount/point/of/volume/root \
--exclude-suffix .log \
--exclude-suffix cache
```

Tutti i percorsi dei file nel volume di destinazione vengono normalizzati ai percorsi originali. Ad esempio, durante la scansione di un volume montato su `/mnt/volume` che contiene un file in`/mnt/volume/var/lib/rpm/rpmdb.sqlite`, il percorso verrà normalizzato a quello contenuto `/var/lib/rpm/rpmdb.sqlite` nella SBOM generata.

Invia un SBOM ad Amazon Inspector per l'identificazione delle vulnerabilità

Oltre a generare un SBOM, puoi inviare un SBOM per la scansione con un solo comando dall'API Amazon Inspector Scan. Amazon Inspector valuta i contenuti dello SBOM alla ricerca di vulnerabilità prima di restituire i risultati. Sbomgen A seconda dell'input, i risultati possono essere visualizzati o scritti su un file.

> **Note**
>
> È necessario disporre di un account attivo Account AWS con autorizzazioni di lettura `InspectorScan-ScanSbom` per utilizzare questa funzionalità.

Per abilitare questa funzionalità, si passa l'`--scan-sbom`argomento alla Sbomgen CLI. È inoltre possibile passare l'`--scan-sbom`argomento a uno dei seguenti Sbomgen sottocomandi:`archive`,,, `binarycontainer`,`directory`. `localhost`

> **Note**
>
> L'API Amazon Inspector Scan non elabora SBOMs con più di 2.000 pacchetti. In questo scenario, l'API Amazon Inspector Scan restituisce una risposta HTTP 400.

Puoi autenticarti su Amazon Inspector tramite AWS un profilo o un ruolo IAM con i AWS CLI seguenti argomenti:

```
--aws-profile profile
--aws-region region
--aws-iam-role-arn role_arn
```

Puoi anche autenticarti su Amazon Inspector fornendo le seguenti variabili di ambiente a. Sbomgen

```
AWS_ACCESS_KEY_ID=$access_key \
AWS_SECRET_ACCESS_KEY=$secret_key \
AWS_DEFAULT_REGION=$region \
./inspector-sbomgen arguments
```

Per specificare il formato della risposta, usa l'`--scan-sbom-output-format cyclonedx`argomento o `--scan-sbom-output-format inspector` l'argomento.

Esempio di comando 1

Questo comando crea un SBOM per l'ultima Alpine Linux versione, analizza lo SBOM e scrive i risultati della vulnerabilità in un file JSON.

```
./inspector-sbomgen container --image alpine:latest \
                          --scan-sbom \
                          --aws-profile your_profile \
                          --aws-region your_region \
                          --scan-sbom-output-format cyclonedx \
                          --outfile /tmp/inspector_scan.json
```

Esempio di comando 2

Questo comando esegue l'autenticazione su Amazon Inspector AWS utilizzando credenziali come variabili di ambiente.

```
AWS_ACCESS_KEY_ID=$your_access_key \
AWS_SECRET_ACCESS_KEY=$your_secret_key \
AWS_DEFAULT_REGION=$your_region \
./inspector-sbomgen container --image alpine:latest \
                          -o /tmp/sbom.json \
                          --scan-sbom \
                          --scan-sbom-output-format inspector
```

Esempio di comando 3

Questo comando esegue l'autenticazione su Amazon Inspector utilizzando l'ARN per un ruolo IAM.

```
./inspector-sbomgen container --image alpine:latest \
                          --scan-sbom \
                          --aws-profile your_profile \
                          --aws-region your_region \
                          --outfile /tmp/inspector_scan.json
                          --aws-iam-role-arn arn:aws:iam::123456789012:role/your_role
```

Utilizza scanner aggiuntivi per migliorare le capacità di rilevamento

Amazon Inspector SBOM Generator applica scanner predefiniti in base al comando utilizzato.

Gruppi di scanner predefiniti

Ogni sottocomando di Amazon Inspector SBOM Generator applica automaticamente i seguenti gruppi di scanner predefiniti.

- Per il `directory` sottocomando: binary, dockerfile scanner groups programming-language-packages
- Per il `localhost` sottocomando: os,, programming-language-packages extra-ecosystems scanner groups
- Per il `container` sottocomando: os, extra-ecosystems, programming-language-packages dockerfile, binary scanner groups

Scanner speciali

Per includere scanner oltre ai gruppi di scanner predefiniti, utilizzate l'`--additional-scanners`opzione seguita dal nome dello scanner da aggiungere. Di seguito è riportato un comando di esempio che mostra come eseguire questa operazione.

```
# Add WordPress installation scanner to directory scan
./inspector-sbomgen directory --path /path/to/directory/ --additional-scanners
 wordpress-installation -o output.json
```

Di seguito è riportato un comando di esempio che mostra come aggiungere più scanner con un elenco separato da virgole.

```
./inspector-sbomgen container --image image:tag --additional-scanners scanner1,scanner2
 -o output.json
```

Ottimizza le scansioni dei contenitori regolando la dimensione massima del file da scansionare

Quando si analizza ed elabora l'immagine di un contenitore, per impostazione predefinita esegue la Sbomgen scansione di file di dimensioni pari o inferiori a 200 MB. I file di dimensioni superiori a 200 MB contengono raramente metadati dei pacchetti. È possibile che si verifichino errori quando si effettua l'inventario di un Rust file binario Go di dimensioni superiori a 200 MB. Per modificare il limite di dimensione, usa l'argomento. `--max-file-size` Ciò consente di aumentare il limite per includere file di grandi dimensioni e di diminuirlo per ridurre l'utilizzo delle risorse escludendo i file di grandi dimensioni.

Esempio

L'esempio seguente mostra come utilizzare l'`--max-file-size`argomento per aumentare le dimensioni del file.

```
# Increase the file size limit to scan files up to 300 MB
./inspector-sbomgen container --image alpine:latest \
--outfile /tmp/sbom.json \
--max-file-size 300000000
```

La regolazione di questa impostazione consente di controllare l'utilizzo del disco, il consumo di memoria e la durata complessiva della scansione.

Disattiva l'indicatore di avanzamento

Sbomgenvisualizza un indicatore di avanzamento della rotazione che può causare un numero eccessivo di caratteri barra negli CI/CD ambienti.

```
INFO[2024-02-01 14:58:46]coreV1.go:53: analyzing artifact
|
\
/
|
\
/
INFO[2024-02-01 14:58:46]coreV1.go:62: executing post-processors
```

È possibile disabilitare l'indicatore di avanzamento utilizzando l'`--disable-progress-bar`argomento:

```
./inspector-sbomgen container --image alpine:latest \
--outfile /tmp/sbom.json \
--disable-progress-bar
```

Autenticazione in registri privati con Sbomgen

Fornendo le credenziali di autenticazione del registro privato, è possibile eseguire la generazione a SBOMs partire da contenitori ospitati in registri privati. È possibile fornire queste credenziali tramite i seguenti metodi:

Autenticazione tramite credenziali memorizzate nella cache (scelta consigliata)

Con questo metodo, ci si autentica nel registro dei contenitori. Ad esempio, se si utilizzaDocker, è possibile autenticarsi nel registro dei contenitori utilizzando il comando di registrazione:Docker. `docker login`

1. Effettua l'autenticazione nel registro dei contenitori. Ad esempio, se si utilizzaDocker, è possibile autenticarsi nel registro utilizzando il Docker `login` comando:
2. Dopo l'autenticazione nel registro dei contenitori, utilizzala Sbomgen su un'immagine del contenitore presente nel registro. Per utilizzare l'esempio seguente, sostituiscilo *`image:tag`* con il nome dell'immagine da scansionare:

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

Effettua l'autenticazione utilizzando il metodo interattivo

Per questo metodo, fornite il vostro nome utente come parametro e vi Sbomgen richiederà l'immissione sicura della password quando necessario.

Per utilizzare l'esempio seguente, *`image:tag`* sostituiscilo con il nome dell'immagine che desideri scansionare e *`your_username`* con un nome utente che abbia accesso all'immagine:

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

Effettua l'autenticazione utilizzando il metodo non interattivo

Per questo metodo, memorizza la password o il token di registro in un `.txt` file.

> **Note**
>
> L'utente corrente dovrebbe essere in grado di leggere solo questo file. Il file deve contenere anche la password o il token su una sola riga.

Per utilizzare l'esempio seguente, *your_username* sostituiscilo con il tuo nome utente, *password.txt* con il `.txt` file che include la password o il token su un'unica riga e *image:tag* 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"
        }
      ]
    }
  ]
}
```

Versioni precedenti di Amazon Inspector SBOM Generator

Questo argomento fornisce collegamenti alle versioni più recenti e precedenti di Amazon Inspector SBOM Generator. Per informazioni sull'installazione di Sbomgen, consulta Installazione di Sbomgen.

Versione più recente

- https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/amd64/inspector-sbomgen.zip
- https://amazon-inspector-sbomgen.s3.amazonaws.com/latest/linux/arm64/inspector-sbomgen.zip

Sbomgen1.8.0

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.8.0/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.8.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.7.3

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.7.3/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.7.3/linux/arm64/inspector-sbomgen.zip

Sbomgen1.7.2

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.7.2/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.7.2/linux/arm64/inspector-sbomgen.zip

Sbomgen1.7.1

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.7.1/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.7.1/linux/arm64/inspector-sbomgen.zip

Sbomgen1.7.0

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.7.0/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.7.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.6.3

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.3/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.3/linux/arm64/inspector-sbomgen.zip

Sbomgen1.6.2

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.2/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.2/linux/arm64/inspector-sbomgen.zip

Sbomgen1.6.1

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.1/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.1/linux/arm64/inspector-sbomgen.zip

Sbomgen1.6.0

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.0/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.6.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.5.5

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.5/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.5/linux/arm64/inspector-sbomgen.zip

Sbomgen1.5.4

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.4/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.4/linux/arm64/inspector-sbomgen.zip

Sbomgen1.5.3

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.3/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.3/linux/arm64/inspector-sbomgen.zip

Sbomgen1.5.2

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.2/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.2/linux/arm64/inspector-sbomgen.zip

Sbomgen1.5.1

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.1/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.1/linux/arm64/inspector-sbomgen.zip

Sbomgen1.5.0

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.0/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.5.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.4.0

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.4.0/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.4.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.3.2

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.3.2/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.3.2/linux/arm64/inspector-sbomgen.zip

Sbomgen1.3.1

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.3.1/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.3.1/linux/arm64/inspector-sbomgen.zip

Sbomgen1.3.0

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.3.0/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.3.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.2.1

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.2.1/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.2.1/linux/arm64/inspector-sbomgen.zip

Sbomgen1.2.0

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.2.0/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.2.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.1.1

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.1.1/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.1.1/linux/arm64/inspector-sbomgen.zip

Sbomgen1.1.0

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.1.0/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.1.0/linux/arm64/inspector-sbomgen.zip

Sbomgen1.0.0

- Linux AMD64: -sbomgen.zip https://amazon-inspector-sbomgen.s3.amazonaws.com/1.0.0/ linux/amd64/inspector
- Linux ARM64: https://amazon-inspector-sbomgen.s3.amazonaws.com/1.0.0/linux/arm64/inspector-sbomgen.zip

Raccolta completa di sistemi operativi Amazon Inspector SBOM Generator

Amazon Inspector SBOM Generator esegue la scansione di diversi sistemi operativi per garantire un'analisi affidabile e dettagliata dei componenti del sistema. La generazione di un SBOM ti aiuta a comprendere la composizione del tuo sistema operativo, in modo da poter identificare le vulnerabilità nei pacchetti gestiti dal sistema. Questo argomento descrive le caratteristiche principali delle diverse

raccolte di pacchetti del sistema operativo supportate da Amazon Inspector SBOM Generator. Per informazioni sui sistemi operativi supportati da Amazon Inspector, consulta Sistemi operativi e linguaggi di programmazione supportati per Amazon Inspector.

Artefatti del sistema operativo supportati

Amazon Inspector SBOM Generator supporta i seguenti elementi del sistema operativo:

Piattaforma	Binario	Origine	Flusso
Alma Linux	N/D	Sì	Sì
Alpine Linux	Sì	Sì	N/D
Amazon Linux	N/D	Sì	N/D
CentOS	N/D	Sì	N/D
Chainguard	Sì	Sì	N/D
Debian	Sì	Sì	N/D
Distroless	Sì	Sì	N/D
Fedora	N/D	Sì	N/D
MinimOS	Sì	Sì	N/D
OpenSUSE	N/D	Sì	N/D
Oracle Linux	N/D	Sì	N/D
Photon OS	N/D	Sì	N/D
RHEL	N/D	Sì	Sì
Rocky Linux	N/D	Sì	Sì
SLES	N/D	Sì	N/D
Ubuntu	Sì	Sì	N/D

Raccolta di pacchetti del sistema operativo basata su APK

Questa sezione include le piattaforme supportate e le funzionalità chiave per la raccolta di pacchetti APK basati sul sistema operativo. Per ulteriori informazioni, vedere Alpine Package Keeper sul Alpine Linux sito Web.

Piattaforme supportate

Le seguenti sono le piattaforme supportate.

- Alpine Linux

> **Note**
>
> Per i sistemi APK basati, Amazon Inspector SBOM Generator raccoglie i metadati dei pacchetti dal file. `/lib/apk/db/`

Funzionalità principali

- Raccolta di nomi di pacchetto: estrae il nome di ogni pacchetto installato
- Raccolta di versioni: estrae la versione di ogni pacchetto installato
- Identificazione del pacchetto sorgente: identifica il pacchetto sorgente per ogni pacchetto installato

Esempio

Il seguente frammento è un esempio di file di database. APK

```
C:Q1JlboSJkrN4qkDcokr4zenpcWEXQ=
P:zlib
V:1.2.13-r1
A:x86_64
S:54253
I:110592
T:A compression/decompression Library
U:https://zlib.net/
L:Zlib
o:zlib
```

Raccolta di pacchetti del sistema operativo basata su DPKG

Questa sezione include le piattaforme supportate e le funzionalità chiave per la raccolta di pacchetti DPKG basati sul sistema operativo. Per ulteriori informazioni, vedere Debian Package sul Debian sito web.

Piattaforme supportate

Sono supportate le seguenti piattaforme.

- Debian
- Ubuntu

> **Note**
>
> Per i sistemi DPKG basati, Amazon Inspector SBOM Generator raccoglie i metadati dei pacchetti dal file. `/var/lib/dpkg/status`

Funzionalità principali

Di seguito sono riportate le caratteristiche principali dei pacchetti OS basati su sistemi operativi. DPKG

- Raccolta di nomi di pacchetto: estrae il nome di ogni pacchetto installato
- Raccolta di versioni: estrae la versione di ogni pacchetto installato
- Identificazione del pacchetto sorgente: identifica il pacchetto sorgente per ogni pacchetto installato

Esempio

Il seguente frammento è un esempio di file. `/var/lib/dpkg/`

```
Package: zlib1g
Status: install ok installed
```

```
Priority: optional
Section: libs
Installed-Size: 168
Maintainer: Mark Brown <broonie@debian.org>
Architecture: amd64
Multi-Arch: same
Source: zlib
Version: 1:1.2.13.dfsg-1
Provides: libz1
Depends: libc6 (>= 2.14)
Breaks: libxml2 (<< 2.7.6.dfsg-2), texlive-binaries (<< 2009-12)
Conflicts: zlib1 (<= 1:1.0.4-7)
Description: compression library - runtime
 zlib is a library implementing the deflate compression method found
 in gzip and PKZIP.  This package includes the shared library.
Homepage: http://zlib.net/
```

Raccolta di pacchetti del sistema operativo basata su RPM

Questa sezione include le piattaforme supportate e le funzionalità chiave per la raccolta di pacchetti RPM basati sul sistema operativo. Per ulteriori informazioni, vedere RPM Package Manager sul RPM sito Web.

Piattaforme supportate

Sono supportate le seguenti piattaforme.

- Alma Linux
- Amazon Linux
- CentOS
- Fedora
- OpenSUSE
- Oracle Linux
- PhotonOS
- RedHat Enterprise Linux
- Rocky Linux
- SUSE Linux Enterprise Server

> **Note**
>
> Per i sistemi RPM basati, Amazon Inspector SBOM Generator raccoglie i metadati dei pacchetti dal file. `/var/lib/rpm`

Funzionalità principali

Di seguito sono riportate le funzionalità principali per RPM le raccolte di pacchetti basati su sistemi operativi.

- Raccolta di nomi di pacchetto: estrae il nome di ogni pacchetto installato
- Raccolta di versioni: estrae la versione di ogni pacchetto installato
- Identificazione del pacchetto sorgente: identifica il pacchetto sorgente per ogni pacchetto installato
- Supporto Stream: estrae i metadati dello stream di ogni pacchetto installato

Esempio

Di seguito è riportato un esempio di frammento di file di RPM database.

```
/usr/lib/sysimage/rpm/rpmdb.sqlite
/usr/lib/sysimage/rpm/Packages
/usr/lib/sysimage/rpm/Packages.db
/var/lib/rpm/rpmdb.sqlite
/var/lib/rpm/Packages
/var/lib/rpm/Packages.db
```

Raccolta di pacchetti di immagini Chainguard

Questa sezione include le piattaforme supportate e le funzionalità chiave per la raccolta di pacchetti di Chainguard immagini. Per ulteriori informazioni, consulta Immagini sul Chainguard sito Web.

Piattaforme supportate

Sono supportate le seguenti piattaforme

- Wolfi Linux

> **Note**
>
> Per Chainguard le immagini, Amazon Inspector SBOM Generator raccoglie i metadati del pacchetto dal file. `/lib/apk/db/installed`

Funzionalità principali

Di seguito sono riportate le caratteristiche principali.

- Raccolta di nomi di pacchetto: estrae il nome di ogni pacchetto installato
- Raccolta di versioni: estrae la versione di ogni pacchetto installato
- Identificazione del pacchetto sorgente: identifica il pacchetto sorgente per ogni pacchetto installato

Esempio

Il seguente frammento è un esempio di file di Chainguard immagine.

```
P:wolfi-keys
V:1-r8
A:x86_64
L:MIT
T:Wolfi signing keyring
o:wolfi-keys
```

Raccolta di pacchetti di immagini Distroless

Distrolessi contenitori sono immagini di contenitori che escludono i gestori di pacchetti, le shell e altre utilità nelle distribuzioni. Linux Distrolessi contenitori includono solo le dipendenze essenziali necessarie per eseguire l'applicazione e migliorare le prestazioni e la sicurezza.

> **Note**
>
> Per Distrolessle immagini, Amazon Inspector SBOM Generator raccoglie i metadati del pacchetto dal file. `/var/lib/dpkg/status.d` Sono supportate solo le distribuzioni basate su Debian di Ubuntu esse. Queste possono essere identificate dal `NAME` campo nel `/etc/os-release` file system, che mostra "Debian" o "»Ubuntu.

Funzionalità principali

- Raccolta di nomi di pacchetto: estrae il nome di ogni pacchetto installato
- Raccolta di versioni: estrae la versione di ogni pacchetto installato

Esempio

Di seguito è riportato un esempio di file di Distroless immagine.

```
Package: tzdata
Version: 2021a-1+deb11u10
Architecture: all
Maintainer: GNU Libc Maintainers <debian-glibc@lists.debian.org>
Installed-Size: 3413
Depends: debconf (>= 0.5) | debconf-2.0
Provides: tzdata-bullseye
Section: localization
Priority: required
Multi-Arch: foreign
Homepage: https://www.iana.org/time-zones
Description: time zone and daylight-saving time data
 This package contains data required for the implementation of
 standard local time for many representative locations around the
 globe. It is updated periodically to reflect changes made by
 political bodies to time zone boundaries, UTC offsets, and
 daylight-saving rules.
```

Raccolta di pacchetti MiniMOS

Questa sezione include le piattaforme supportate e le funzionalità chiave per la raccolta di pacchetti di Minimus immagini. Per ulteriori informazioni, consultate il sito Web di Minimus.

Piattaforme supportate

Sono supportate le seguenti piattaforme.

- MinimOS

> **Note**
>
> Per Minimus le immagini, Amazon Inspector SBOM Generator raccoglie i metadati del pacchetto dal file. `/lib/apk/db/installed`

Funzionalità principali

Di seguito sono riportate le caratteristiche principali.

- Raccolta di nomi di pacchetto: estrae il nome di ogni pacchetto installato
- Raccolta di versioni: estrae il nome di ogni pacchetto installato
- Identificazione del pacchetto sorgente: identifica il pacchetto sorgente per ogni pacchetto installato

Quanto segue è un frammento di un Minimus file di immagine.

```
P:ca-certificates-bundle
V:20241121-r1
A:aarch64
L:MPL-2.0 AND MIT
T:
o:ca-certificates
```

Raccolta delle dipendenze del linguaggio di programmazione

Amazon Inspector SBOM Generator supporta diversi linguaggi e framework di programmazione, che costituiscono una raccolta solida e dettagliata di dipendenze. La generazione di un SBOM ti aiuta a comprendere la composizione del tuo software, in modo da poter identificare le vulnerabilità e mantenere la conformità agli standard di sicurezza. Amazon Inspector SBOM Generator supporta i seguenti linguaggi di programmazione e formati di file.

Vai alla scansione delle dipendenze

Linguaggio di programmazione	Programma di gestione dei pacchetti	Artefatti supportati	Supporto Toolchain	Dipendenze di sviluppo	Dipendenze transitive	Bandiera privata	Ricorsivamente
Go	Go	go.mod	N/D	N/D	N/D	N/D	Sì
		go.sum	N/D	N/D	N/D	N/D	Sì
		Go Binaries	Sì	N/D	N/D	N/D	Sì
		GOMODCACHE	N/D	N/D	N/D	N/D	No

go.mod/go.sum

Usa go.sum i file per definire go.mod e bloccare le dipendenze nei progetti. Go Amazon Inspector SBOM Generator gestisce questi file in modo diverso in base alla versione della toolchain. Go

Funzionalità principali

- Raccoglie le dipendenze da go.mod (se la versione della Go toolchain è 1.17 o successiva)
- Raccoglie le dipendenze da go.sum (se la versione della Go toolchain è 1.17 o precedente)
- Analizza go.mod per identificare tutte le dipendenze e le versioni delle dipendenze dichiarate

Esempio di file **go.mod**

Di seguito è riportato un esempio di file. go.mod

```
module example.com/project

go 1.17
```

```
require (
github.com/gin-gonic/gin v1.7.2
golang.org/x/crypto v0.0.0-20210616213533-5cf6c0f8e123
)
```

Esempio di file **`go.sum`**

Quello che segue è un esempio di `go.sum` file.

```
github.com/gin-gonic/gin v1.7.2 h1:VZ7DdRl0sghbA6lVGSkX+UXO2+J0aH7RbsNugG+FA8Q=
github.com/gin-gonic/gin v1.7.2/go.mod h1:ILZ1Ngh2f1pL1ASUj7gGk8lGFeNC8cRTaN2ZhsBNbXU=
golang.org/x/crypto v0.0.0-20210616213533-5cf6c0f8e123 h1:b6rCu+qHze
+BUsmC3CZzH8aNu8LzPZTVsNTo64OypSc=
golang.org/x/crypto v0.0.0-20210616213533-5cf6c0f8e123/go.mod h1:K5Dkpb0Q4ewZW/
EzWlQphgJcUMBCzoWrLfDOVzpTGVQ=
```

> **Note**
>
> Ciascuno di questi file produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Go Binaries

Amazon Inspector SBOM Generator estrae le dipendenze dai Go file binari compilati per garantire il codice in uso.

> **Note**
>
> Amazon Inspector SBOM Generator supporta l'acquisizione e la valutazione delle versioni della toolchain da file binari creati utilizzando il compilatore ufficiale. Go Go Per ulteriori informazioni, consulta Download e installazione sul sito Web. Go Se si utilizza la Go toolchain di un altro fornitore, ad esempio, la valutazione potrebbe non essere accurata a causa di potenziali differenze nella distribuzione e nella disponibilità dei metadati. Red Hat

Funzionalità principali

- Estrae le informazioni sulle dipendenze direttamente dai file binari Go
- Raccoglie le dipendenze incorporate nel file binario
- Rileva ed estrae la versione della Go toolchain utilizzata per compilare il file binario.

GOMODCACHE

Amazon Inspector SBOM Generator analizza la cache del Go modulo per raccogliere informazioni sulle dipendenze installate. Questa cache memorizza i moduli scaricati per garantire che le stesse versioni vengano utilizzate in build diverse.

Funzionalità principali

- Esegue la scansione della `GOMODCACHE` directory per identificare i moduli memorizzati nella cache
- Estrae i metadati dettagliati, inclusi i nomi dei moduli, le versioni e l'origine URLs

Struttura di esempio

Di seguito è riportato un esempio di `GOMODCACHE` struttura.

```
~/go/pkg/mod/
### github.com/gin-gonic/gin@v1.7.2
### golang.org/x/crypto@v0.0.0-20210616213533-5cf6c0f8e123
```

> **Note**
>
> Questa struttura produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Scansione delle dipendenze in Java

Linguaggio di programmazione	Programma di gestione dei pacchetti	Artefatti supportati	Supporto Toolchain	Dipendenze di sviluppo	Dipendenze transitive	Bandiera privata	Ricorsivamente
`Java`	`Maven`	JavaApplicazioni compilate (.jar/.war/.ear) `pom.xml`	N/D N/D	N/D N/D	Sì Sì	N/D N/D	Sì Sì

Amazon Inspector SBOM Generator esegue la scansione delle Java dipendenze analizzando applicazioni e file compilati. Java `pom.xml` Durante la scansione di applicazioni compilate, lo scanner genera hash SHA—1 per la verifica dell'integrità, estrae i file incorporati e analizza i file annidati. `pom.properties` `pom.xml`

Raccolta di hash SHA—1 (per file compilati in formato.jar, .war, .ear)

Amazon Inspector SBOM Generator cerca di raccogliere hash SHA—1 per tutti e `.war` file in un progetto per garantire l'`.ear`integrità `.jar` e la tracciabilità degli artefatti compilati. Java

Funzionalità principali

- Genera hash SHA—1 per tutti gli artefatti compilati Java

Esempio di artefatto

Di seguito è riportato un esempio di artefatto SHA—1.

```
{
  "bom-ref": "comp-52",
  "type": "library",
```

```
  "name": "jul-to-slf4j",
  "version": "2.0.6",
  "hashes": [
    {
      "alg": "SHA-1",
      "content": ""
    }
  ],
  "purl": "pkg:maven/jul-to-slf4j@2.0.6",
  "properties": [
    {
      "name": "amazon:inspector:sbom_generator:source_path",
      "value": "test-0.0.1-SNAPSHOT.jar/BOOT-INF/lib/jul-to-slf4j-2.0.6.jar"
    }
  ]
}
```

> **Note**
>
> Questo artefatto produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

pom.properties

Il `pom.properties` file viene utilizzato nei Maven progetti per archiviare i metadati del progetto, inclusi i nomi e le versioni dei pacchetti. Amazon Inspector SBOM Generator analizza questo file per raccogliere informazioni sul progetto.

Funzionalità principali

- Analizza ed estrae gli elementi, i gruppi di pacchetti e le versioni dei pacchetti

Esempio di file **`pom.properties`**

Di seguito è riportato un esempio di un file `pom.properties`.

```
#Generated by Maven
#Tue Mar 16 15:44:02 UTC 2021

version=1.6.0
groupId=net.datafaker
artifactId=datafaker
```

> **Note**
>
> Questo file produce un output che contiene l'URL del pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Esclusa l'analisi annidata **`pom.xml`**

Se si desidera escludere l'`pom.xml`analisi durante la scansione di Java applicazioni compilate, utilizzare l'argomento. `--skip-nested-pomxml`

pom.xml

Il `pom.xml` file è il file di configurazione principale per i Maven progetti. Contiene informazioni sui progetti e sulle dipendenze dei progetti. Amazon Inspector SBOM Generator analizza pom.xml i file per raccogliere le dipendenze, scansiona i file autonomi nei repository e i file all'interno di file compilati. .jar

Funzionalità principali

- Analizza ed estrae gli elementi dei pacchetti, i gruppi di pacchetti e le versioni dei pacchetti dai file. `pom.xml`

Ambiti e tag supportati Maven

Le dipendenze vengono raccolte con i seguenti ambiti: Maven

- compile
- fornito

- runtime
- test
- sistema
- importare

Le dipendenze vengono raccolte con il seguente Maven tag:`<optional>true</optional>`.

`pom.xml`File di esempio con un ambito

Di seguito è riportato un esempio di `pom.xml` file con un ambito.

```
<dependency>
<groupId>jakarta.servlet</groupId>
<artifactId>jakarta.servlet-api</artifactId>
</version>6.0.0</version>
<scope>provided</scope>
</dependency>
<dependency>
<groupId>mysql</groupId>
<artifactId>mysql-connector-java</artifactId>
<version>8.0.28</version>
<scope>runtime</scope>
</dependency>
```

`pom.xml`File di esempio senza ambito

Di seguito è riportato un esempio di `pom.xml` file senza ambito.

```
<dependency>
<groupId>com.fasterxml.jackson.core</groupId>
<artifactId>jackson-databind</artifactId>
<version>2.17.1</version>
</dependency>

<dependency>
<groupId>org.jenkins-ci.plugins</groupId>
<artifactId>plain-credentials</artifactId>
<version>183.va_de8f1dd5a_2b_</version>
```

```
</dependency>

<dependency>
<groupId>org.jenkins-ci.plugins</groupId>
<artifactId>jackson2-api</artifactId>
<version>2.15.2-350.v0c2f3f8fc595</version>
</dependency>
```

> **Note**
>
> Ciascuno di questi file produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

JavaScript scansione delle dipendenze

Linguaggio di programmazione	Programma di gestione dei pacchetti	Artefatti supportati	Supporto Toolchain	Dipendenze di sviluppo	Dipendenze transitive	Bandiera privata	Ricorsivamente
Javascript	Node Modules	node_modules/*/package.json	N/D	N/D	Sì	Sì	Sì
	NPM		N/D	Sì	N/D	N/D	No
	PNPM		N/D	Sì	N/D	N/D	No
	YARN	package-lock.json (v1, v2, and v3) / npm-	N/D	Sì	N/D	N/D	No

Linguaggio di programmazione	Programma di gestione dei pacchetti	Artefatti supportati	Supporto Toolchain	Dipendenze di sviluppo	Dipendenze transitive	Bandiera privata	Ricorsivamente

		`shrinkwrap.json`
		
		`pnpm-lock.yaml`
		
		`yarn.lock`					

pacchetto.json

Il `package.json` file è un componente fondamentale dei progetti. Node.js Contiene metadati sui pacchetti installati. Amazon Inspector SBOM Generator analizza questo file per identificare i nomi e le versioni dei pacchetti.

Funzionalità principali

- Analizza la struttura dei file JSON per estrarre i nomi e le versioni dei pacchetti
- Identifica i pacchetti privati con valori privati

Esempio di file **`package.json`**

Di seguito è riportato un esempio di un file `package.json`.

```
{
"name": "arrify",
"private": true,
"version": "2.0.1",
"description": "Convert a value to an array",
"license": "MIT",
```

```
"repository": "sindresorhus/arrify"
}
```

> **Note**
>
> Questo file produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

package-lock.json

Il `package-lock.json` file viene generato automaticamente da npm per bloccare le versioni esatte delle dipendenze installate per un progetto. Garantisce la coerenza negli ambienti memorizzando le versioni esatte di tutte le dipendenze e le relative sottodipendenze. Questo file può distinguere tra dipendenze regolari e dipendenze di sviluppo.

Funzionalità principali

- Analizza la struttura dei file JSON per estrarre i nomi e le versioni dei pacchetti
- Supporta il rilevamento delle dipendenze degli sviluppatori

Esempio di file **`package-lock.json`**

Di seguito è riportato un esempio di un file `package-lock.json`.

```
"verror": {
"version": "1.10.0",
"resolved": "https://registry.npmjs.org/verror/-/verror-1.10.0.tgz",
"integrity": "sha1-OhBcoXBTr1XW4nDB+CiGguGNpAA=",
"requires": {
    "assert-plus": "^1.0.0",
    "core-util-is": "1.0.2",
    "extsprintf": "^1.2.0"
}
},
"wrappy": {
```

```
"version": "1.0.2",
"resolved": "https://registry.npmjs.org/wrappy/-/wrappy-1.0.2.tgz",
"integrity": "sha1-tSQ9jz7BqjXxNkYFvA0QNuMKtp8=",
"dev": true
},
"yallist": {
"version": "3.0.2",
"resolved": "https://registry.npmjs.org/yallist/-/yallist-3.0.2.tgz",
"integrity": "sha1-hFK0u36Dx8GI2AQcGoN8dz1ti7k="
}
```

> **Note**
>
> Questo file produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

npm-shrinkwrap.json

npmgenera automaticamente `npm-shrinkwrap.json` file `package-lock.json` e file per bloccare le versioni esatte delle dipendenze installate per un progetto. Ciò garantisce la coerenza negli ambienti memorizzando le versioni esatte di tutte le dipendenze e sottodipendenze. I file distinguono tra dipendenze regolari e dipendenze di sviluppo.

Funzionalità principali

- Analizza `package-lock` le versioni 1, 2 e 3 della struttura del JSON file per estrarre il nome e la versione del pacchetto
- È supportato il rilevamento delle dipendenze degli sviluppatori (`package-lock.jsonacquisisce` le dipendenze di produzione e sviluppo, consentendo agli strumenti di identificare quali pacchetti vengono utilizzati negli ambienti di sviluppo)
- Al `npm-shrinkwrap.json` file viene data la priorità rispetto al file `package-lock.json`

Esempio

Di seguito è riportato un esempio di un file `package-lock.json`.

```
"verror": {
            "version": "1.10.0",
            "resolved": "https://registry.npmjs.org/verror/-/verror-1.10.0.tgz",
            "integrity": "sha1-OhBcoXBTr1XW4nDB+CiGguGNpAA=",
            "requires": {
                "assert-plus": "^1.0.0",
                "core-util-is": "1.0.2",
                "extsprintf": "^1.2.0"
            }
        },
        "wrappy": {
            "version": "1.0.2",
            "resolved": "https://registry.npmjs.org/wrappy/-/wrappy-1.0.2.tgz",
            "integrity": "sha1-tSQ9jz7BqjXxNkYFvA0QNuMKtp8=",
            "dev": true
        },
        "yallist": {
            "version": "3.0.2",
            "resolved": "https://registry.npmjs.org/yallist/-/yallist-3.0.2.tgz",
            "integrity": "sha1-hFK0u36Dx8GI2AQcGoN8dz1ti7k="
}
```

pnpm-yaml.lock

Il `pnpm-lock.yaml` file viene generato da pnpm per mantenere un registro delle versioni di dipendenza installate. Inoltre, tiene traccia delle dipendenze di sviluppo separatamente.

Funzionalità principali

- Analizza la struttura dei file YAML per estrarre i nomi e le versioni dei pacchetti
- Supporta il rilevamento delle dipendenze degli sviluppatori

Esempio

Di seguito è riportato un esempio di un file `pnpm-lock.yaml`.

```
lockfileVersion: 5.3
importers:
my-project:
dependencies:
  lodash: 4.17.21
```

```
devDependencies:
  jest: 26.6.3
specifiers:
  lodash: ^4.17.21
  jest: ^26.6.3
packages:
/lodash/4.17.21:
resolution:
  integrity: sha512-xyz
engines:
  node: '>=6'
dev: false
/jest/26.6.3:
resolution:
  integrity: sha512-xyz
dev: true
```

> **Note**
>
> Questo file produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

yarn.lock

Amazon Inspector SBOM Generator cerca di raccogliere hash SHA—1 e `.war` file in un progetto per garantire l'`.ear`integrità `.jar` e la tracciabilità degli artefatti compilati. Java

Funzionalità principali

- Genera hash SHA—1 per tutti gli artefatti compilati Java

Esempio di artefatto SHA—1

Di seguito è riportato un esempio di artefatto SHA—1.

```
"@ampproject/remapping@npm:^2.2.0":
```

```
version: 2.2.0
resolution: "@ampproject/remapping@npm:2.2.0"
dependencies:
"@jridgewell/gen-mapping": ^0.1.0
"@jridgewell/trace-mapping": ^0.3.9
checksum:
 d74d170d06468913921d72430259424b7e4c826b5a7d39ff839a29d547efb97dc577caa8ba3fb5cf023624e9af9d09
languageName: node
linkType: hard

"@babel/code-frame@npm:^7.0.0, @babel/code-frame@npm:^7.12.13, @babel/code-
frame@npm:^7.18.6, @babel/code-frame@npm:^7.21.4":
version: 7.21.4
resolution: "@babel/code-frame@npm:7.21.4"
dependencies:
"@babel/highlight": ^7.18.6
checksum:
 e5390e6ec1ac58dcef01d4f18eaf1fd2f1325528661ff6d4a5de8979588b9f5a8e852a54a91b923846f7a5c681b217
languageName: node
linkType: hard
```

> **Note**
>
> Questo artefatto produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Scansione delle dipendenze.NET

Linguaggio di programmazione	Programma di gestione dei pacchetti	Artefatti supportati	Supporto Toolchain	Dipendenze di sviluppo	Dipendenze transitive	Bandiera privata	Ricorsivamente
`.NET`	`.NET Core`	`*.deps.json`	N/D	N/D	N/D	N/D	Sì

Linguaggio di programmazione	Programma di gestione dei pacchetti	Artefatti supportati	Supporto Toolchain	Dipendenze di sviluppo	Dipendenze transitive	Bandiera privata	Ricorsivamente
	`Nuget`	`Packages.config`	N/D	N/D	N/D	N/D	Sì
	`Nuget`		N/D	N/D	Sì	N/D	Sì
	`.NET`	`packages.lock.json`	N/D	N/D	N/D	N/D	Sì
		`.csproj`					

Packages.config

Il `Packages.config` file è un file XML utilizzato da una versione precedente di per gestire le dipendenze del progettoNuget. Elenca tutti i pacchetti a cui fa riferimento il progetto, incluse versioni specifiche.

Funzionalità principali

- Analizza la struttura XML per estrarre pacchetti IDs e versioni

Esempio

Di seguito è riportato un esempio di un file `Packages.config`.

```
<?xml version="1.0" encoding="utf-8"? >
<packages>
<package id="FluentAssertions" version="5.4.1" targetFramework="net461" />
<package id="Newtonsoft.Json" version="11.0.2" targetFramework="net461" />
<package id="SpecFlow" version="2.4.0" targetFramework="net461" />
<package id="SpecRun.Runner" version="1.8.0" targetFramework="net461" />
<package id="SpecRun.SpecFlow" version="1.8.0" targetFramework="net461" />
<package id="SpecRun.SpecFlow.2-4-0" version="1.8.0" targetFramework="net461" />
<package id="System.ValueTuple" version="4.5.0" targetFramework="net461" />
</packages>
```

> **Note**
>
> Questo file produce un output che contiene l'URL del pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

*.deps.json

Il `*.deps.json` file viene generato dai .NET Core progetti e contiene informazioni dettagliate su tutte le dipendenze, inclusi percorsi, versioni e dipendenze di runtime. Questo file assicura che il runtime disponga delle informazioni necessarie per caricare le versioni corrette delle dipendenze.

Funzionalità principali

- Analizza la struttura JSON per dettagli completi sulle dipendenze
- Estrae i nomi e le versioni dei pacchetti in un elenco. `libraries`

Esempio di file `.deps.json`

Di seguito è riportato un esempio di un file `.deps.json`.

```
{
"runtimeTarget": {
    "name": ".NETCoreApp,Version=v7.0",
    "signature": ""
},
"libraries": {
    "sample-Nuget/1.0.0": {
        "type": "project",
        "serviceable": false,
        "sha512": ""
    },
    "Microsoft.EntityFrameworkCore/7.0.5": {
        "type": "package",
        "serviceable": true,
```

```
        "sha512": "sha512-
RXbRLHHWP2Z3pq8qcL5nQ6LPeoOyp8hasM5bd0Te8PiQi3RjWQR4tcbdY5XMqQ+oTO9wA8/RLhZRn/
hnxlTDnQ==",
        "path": "microsoft.entityframeworkcore/7.0.5",
        "hashPath": "microsoft.entityframeworkcore.7.0.5.nupkg.sha512"
    },
}
```

> **Note**
>
> Questo file produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

packages.lock.json

Il `packages.lock.json` file viene utilizzato dalle versioni più recenti di Nuget per bloccare le versioni esatte delle dipendenze di un .NET progetto per garantire che le stesse versioni vengano utilizzate in modo coerente in ambienti diversi.

Funzionalità principali

- Analizza la struttura JSON per elencare le dipendenze bloccate
- Supporta dipendenze dirette e transitive
- Estrae il nome del pacchetto e le versioni risolte

Esempio di file **`packages.lock.json`**

Di seguito è riportato un esempio di un file `packages.lock.json`.

```
{
"version": 1,
"dependencies": {
"net7.0": {
  "Microsoft.EntityFrameworkCore": {
    "type": "Direct",
```

```
    "requested": "[7.0.5, )",
    "resolved": "7.0.5",
    "contentHash": "RXbRLHHWP2Z3pq8qcL5nQ6LPeoOyp8hasM5bd0Te8PiQi3RjWQR4tcbdY5XMqQ
+oTO9wA8/RLhZRn/hnxlTDnQ==",
    "dependencies": {
      "Microsoft.EntityFrameworkCore.Abstractions": "7.0.5",
      "Microsoft.EntityFrameworkCore.Analyzers": "7.0.5",
      "Microsoft.Extensions.Caching.Memory": "7.0.0",
      "Microsoft.Extensions.DependencyInjection": "7.0.0",
      "Microsoft.Extensions.Logging": "7.0.0"
    }
  },
  "Newtonsoft.Json": {
    "type": "Direct",
    "requested": "[13.0.3, )",
    "resolved": "13.0.3",
    "contentHash": "HrC5BXdl00IP9zeV+0Z848QWPAoCr9P3bDEZguI+gkLcBKAOxix/tLEAAHC
+UvDNPv4a2d18lOReHMOagPa+zQ=="
  },
  "Microsoft.Extensions.Primitives": {
    "type": "Transitive",
    "resolved": "7.0.0",
    "contentHash": "um1KU5kxcRp3CNuI8o/GrZtD4AIOXDk
+RLsytjZ9QPok3ttLUelLKpilVPuaFT3TFjOhSibUAso0odbOaCDj3Q=="
  }
}
}
}
```


> **Note**
>
> Questo file produce un output che contiene l'URL del pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

.csproj

Il `.csproj` file è scritto in XML e il file di progetto è per i progetti. .NET Include riferimenti a Nuget pacchetti, proprietà del progetto e configurazioni di build.

Funzionalità principali

- Analizza la struttura XML per estrarre i riferimenti ai pacchetti

Esempio di file `.csproj`

Di seguito è riportato un esempio di un file `.csproj`.

```
<Project Sdk="Microsoft.NET.Sdk">
<PropertyGroup>
<TargetFramework>net7.0</TargetFramework>
<RootNamespace>sample_Nuget</RootNamespace>
<ImplicitUsings>enable</ImplicitUsings>
<Nullable>enable</Nullable>
<RestorePackagesWithLockFile>true</RestorePackagesWithLockFile>
</PropertyGroup>
<ItemGroup>
</ItemGroup>
<ItemGroup>
<PackageReference Include="Newtonsoft.Json" Version="13.0.3" />
<PackageReference Include="Microsoft.EntityFrameworkCore" Version="7.0.5" />
</ItemGroup>
</Project>
```

Esempio di file `.csproj`

Di seguito è riportato un esempio di un file `.csproj`.

```
<PackageReference Include="ExamplePackage" Version="6.*" />
<PackageReferencePackageReference Include="ExamplePackage" Version="(4.1.3,)" />
<PackageReference Include="ExamplePackage" Version="(,5.0)" />
<PackageReference Include="ExamplePackage" Version="[1,3)" />
<PackageReference Include="ExamplePackage" Version="[1.3.2,1.5)" />
```

> **Note**
>
> Ciascuno di questi file produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la

generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Scansione delle dipendenze PHP

Linguaggio di programmazione	Programma di gestione dei pacchetti	Artefatti supportati	Supporto Toolchain	Dipendenze di sviluppo	Dipendenze transitive	Bandiera privata	Ricorsivamente
PHP	`Composer`	`composer.lock` `/vendor/composer/installed.json`	N/D N/D	N/D N/D	Sì Sì	N/D N/D	Sì Sì

composer.lock

Il `composer.lock` file viene generato automaticamente quando si eseguono i comandi composer install o composer update. Questo file garantisce che le stesse versioni delle dipendenze siano installate in ogni ambiente. Ciò fornisce un processo di compilazione coerente e affidabile.

Funzionalità principali

- Analizza il formato JSON per i dati strutturati
- Estrae i nomi e le versioni delle dipendenze

Esempio di file **`composer.lock`**

Di seguito è riportato un esempio di un file `composer.lock`.

```
{
"packages": [
    {
        "name": "nesbot/carbon",
        "version": "2.53.1",
        // TRUNCATED
    },
    {
        "name": "symfony/deprecation-contracts",
        "version": "v3.2.1",
        // TRUNCATED
    },
    {
        "name": "symfony/polyfill-mbstring",
        "version": "v1.27.0",
        // TRUNCATED
    }
]
// TRUNCATED
}
```

> **Note**
>
> Questo produce un output che contiene l'URL del pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

/.json vendor/composer/installed

Il `/vendor/composer/installed.json` file si trova nella `vendor/composer` directory e fornisce un elenco completo di tutti i pacchetti installati e delle versioni dei pacchetti.

Funzionalità principali

- Analizza il formato JSON per i dati strutturati
- Estrae i nomi e la versione delle dipendenze

Esempio di file **/vendor/composer/installed.json**

Di seguito è riportato un esempio di un file `/vendor/composer/installed.json`.

```
{
"packages": [
    {
        "name": "nesbot/carbon",
        "version": "2.53.1",
        // TRUNCATED
    },
    {
        "name": "symfony/deprecation-contracts",
        "version": "v3.2.1",
        // TRUNCATED
    },
    {
        "name": "symfony/polyfill-mbstring",
        "version": "v1.27.0",
        // TRUNCATED
    }
]
// TRUNCATED
}
```

> **Note**
>
> Questo file produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Scansione delle dipendenze in Python

Linguaggio di programmazione	Programma di gestione dei pacchetti	Artefatti supportati	Supporto Toolchain	Dipendenze di sviluppo	Dipendenze transitive	Bandiera privata	Ricorsivamente
Python	pip	requirements.txt	N/D	N/D	N/D	N/D	Sì
	Poetry	Poetry.lock	N/D	N/D	N/D	N/D	Sì
	Pipenv	Pipfile.lock	N/D	N/D	N/D	N/D	Sì
	Egg/Wheel	.egg-info/PKG-INFO	N/D	N/D	N/D	N/D	Sì
		.dist-info/METADATA	N/D	N/D	N/D	N/D	Sì

requirements.txt

Il `requirements.txt` file è un formato ampiamente utilizzato nei Python progetti per specificare le dipendenze del progetto. Ogni riga di questo file include un pacchetto con i relativi vincoli di versione. Amazon Inspector SBOM Generator analizza questo file per identificare e catalogare accuratamente le dipendenze.

Funzionalità principali

- Supporta gli specificatori di versione (== e =)
- Supporta commenti e linee di dipendenza complesse

> **Note**
>
> Gli specificatori di versione <= e => non sono supportati.

Esempio di file **`requirements.txt`**

Di seguito è riportato un esempio di un file `requirements.txt`.

```
flask==1.1.2
requests==2.24.0
numpy==1.18.5
foo~=1.2.0
# Comment about a dependency
scipy. # invalid
```

> **Note**
>
> Questo file produce un output che contiene l'URL del pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

pipfile.lock

Pipenvè uno strumento che offre il meglio di tutti i mondi del packaging (impacchettato, bloccato e sbloccato). `Pipfile.lock`Blocca le versioni esatte delle dipendenze per facilitare le build deterministiche. Amazon Inspector SBOM Generator legge questo file per elencare le dipendenze e le relative versioni risolte.

Funzionalità principali

- Analizza il formato JSON per la risoluzione delle dipendenze
- Supporta le dipendenze predefinite e di sviluppo

Esempio di file **`Pipfile.lock`**

Di seguito è riportato un esempio di un file `Pipfile.lock`.

```
{
"default": {
    "requests": {
        "version": "==2.24.0",
        "hashes": [
            "sha256:cc718bb187e53b8d"
        ]
    }
},
"develop": {
    "blinker": {
        "hashes": [
            "sha256:1779309f71bf239144b9399d06ae925637cf6634cf6bd131104184531bf67c01",
            "sha256:8f77b09d3bf7c795e969e9486f39c2c5e9c39d4ee07424be2bc594ece9642d83"
        ],
        "markers": "python_version >= '3.8'",
        "version": "==1.8.2"
    }
}
}
```

> **Note**
>
> Questo file produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Poetry.lock

Poetryè uno strumento di gestione e pacchettizzazione delle dipendenze per Python. Il `Poetry.lock` file blocca le versioni esatte delle dipendenze per facilitare ambienti coerenti. Amazon Inspector SBOM Generator estrae informazioni dettagliate sulle dipendenze da questo file.

Funzionalità principali

- Analizza il formato TOML per i dati strutturati
- Estrae i nomi e le versioni delle dipendenze

Esempio di file **`Poetry.lock`**

Di seguito è riportato un esempio di un file `Poetry.lock`.

```
[[package]]
name = "flask"
version = "1.1.2"
description = "A simple framework for building complex web applications."
category = "main"
optional = false
python-versions = ">=3.5"
[[package]]
name = "requests"
version = "2.24.0"
description = "Python HTTP for Humans."
category = "main"
optional = false
python-versions = ">=3.5"
```

> **Note**
>
> Questo file produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Uovo/Ruota

Per i pacchetti Python installati a livello globale, Amazon Inspector SBOM Generator supporta l'analisi dei file di metadati presenti nelle directory and. `.egg-info/PKG-INFO` `.dist-info/METADATA` Questi file forniscono metadati dettagliati sui pacchetti installati.

Funzionalità principali

- Estrae il nome e la versione del pacchetto
- Supporta sia i formati a uovo che a forma di ruota

Esempio di file **PKG-INFO/METADATA**

Di seguito è riportato un esempio di un file `PKG-INFO/METADATA`.

```
Metadata-Version: 1.2
Name: Flask
Version: 1.1.2
Summary: A simple framework for building complex web applications.
Home-page: https://palletsprojects.com/p/flask/
```

> **Note**
>
> Questo file produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Scansione delle dipendenze con Ruby

Linguaggio di programmazione	Programma di gestione dei pacchetti	Artefatti supportati	Supporto per il toolchain	Dipendenze di sviluppo	Dipendenze transitive	Bandiera privata	Ricorsivamente
`Ruby`	`Bundler`	`Gemfile.lock`	N/D	N/D	Sì	N/D	Sì
			N/D	N/D	N/D	N/D	Sì
		`.gemspec`	N/D	N/D	N/D	N/D	Sì

Linguaggio di programmazione	Programma di gestione dei pacchetti	Artefatti supportati	Supporto per il toolchain	Dipendenze di sviluppo	Dipendenze transitive	Bandiera privata	Ricorsivamente
		`globall installed Gems`					

GemFile.lock

Il `Gemfile.lock` file blocca le versioni esatte di tutte le dipendenze per garantire che le stesse versioni vengano utilizzate in ogni ambiente.

Funzionalità principali

- Analizza il `Gemfile.lock` file in base alle dipendenze e alle versioni delle dipendenze
- Estrae i nomi dettagliati dei pacchetti e le versioni dei pacchetti

Esempio di file **`Gemfile.lock`**

Di seguito è riportato un esempio di un file `Gemfile.lock`.

```
GEM
remote: https://rubygems.org/
specs:
ast (2.4.2)
awesome_print (1.9.2)
diff-lcs (1.5.0)
json (2.6.3)
parallel (1.22.1)
parser (3.2.2.0)
nokogiri (1.16.6-aarch64-linux)
```

> **Note**
>
> Questo file produce un output che contiene l'URL del pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

.gemspec

Il `.gemspec` file è un RubyGem file contenente metadati su una gemma. Amazon Inspector SBOM Generator analizza questo file per raccogliere informazioni dettagliate su una gemma.

Funzionalità principali

- Analizza ed estrae il nome e la versione della gemma

> **Note**
>
> La specifica di riferimento non è supportata.

Esempio di file `.gemspec`

Di seguito è riportato un esempio di un file `.gemspec`.

```
Gem::Specification.new do |s|
s.name        = "generategem"
s.version     = "2.0.0"
s.date        = "2020-06-12"
s.summary     = "generategem"
s.description = "A Gemspec Builder"
s.email       = "edersondeveloper@gmail.com"
s.files       = ["lib/generategem.rb"]
s.homepage    = "https://github.com/edersonferreira/generategem"
s.license     = "MIT"
s.executables = ["generategem"]
s.add_dependency('colorize', '~> 0.8.1')
end
```

```
# Not supported

Gem::Specification.new do |s|
s.name        = &class1
s.version     = &foo.bar.version
```

> **Note**
>
> Questo file produce un output che contiene l'URL del pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Gemme installate a livello globale

Amazon Inspector SBOM Generator supporta la scansione di gem installate a livello globale, che si trovano in directory standard, ad esempio in `/usr/local/lib/ruby/gems/<ruby_version>/gems/` EC2 Amazon/Amazon ECR e in Lambda. `ruby/gems/<ruby_version>/gems/` Questo assicura che tutte le dipendenze installate a livello globale siano identificate e catalogate.

Funzionalità principali

- Identifica e analizza tutte le gem installate a livello globale in directory standard
- Estrae i metadati e le informazioni sulla versione per ogni gem installata a livello globale

Esempio di struttura di directory

Di seguito è riportato un esempio di struttura di directory.

```
.
### /usr/local/lib/ruby/3.5.0/gems/
### actrivesupport-6.1.4
### concurrent-ruby-1.1.9
```

```
### i18n-1.8.10
```

> **Note**
>
> Questa struttura produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Scansione delle dipendenze da Rust

Linguaggio di programmazione	Programma di gestione dei pacchetti	Artefatti supportati	Supporto Toolchain	Dipendenze di sviluppo	Dipendenze transitive	Bandiera privata	Ricorsivamente

`Rust`	`Cargo.toml`	`Cargo.toml`
		`Cargo.lock`
		`Rust binary (built with cargo-auditable)`
			N/D
			N/D
			Sì
				N/D
				N/D
				N/D
					N/D
					Sì
					N/D
						N/D
						N/D
						N/D
							Sì
							Sì
							Sì

Cargo.toml

Il `Cargo.toml` file è il file manifesto dei progetti. Rust

Funzionalità principali

- Analizza ed estrae il `Cargo.toml` file per identificare il nome e la versione del pacchetto del progetto.

Esempio di file **`Cargo.toml`**

Di seguito è riportato un esempio di un file `Cargo.toml`.

```
[package]
name = "wait-timeout"
version = "0.2.0"
description = "A crate to wait on a child process with a timeout specified across Unix
 and\nWindows platforms.\n"
homepage = "https://github.com/alexcrichton/wait-timeout"
documentation = "https://docs.rs/wait-timeout"
readme = "README.md"
categories = ["os"]
license = "MIT/Apache-2.0"
repository = "https://github.com/alexcrichton/wait-timeout"
[target."cfg(unix)".dependencies.libc]
version = "0.2"
[badges.appveyor]
repository = "alexcrichton/wait-timeout"
```

> **Note**
>
> Questo file produce un output che contiene l'URL del pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Cargo.lock

Il `Cargo.lock` file blocca le versioni dipendenti per garantire che vengano utilizzate le stesse versioni ogni volta che viene creato un progetto.

Funzionalità principali

- Analizza il `Cargo.lock` file per identificare tutte le dipendenze e le versioni delle dipendenze.

Esempio di file **`Cargo.lock`**

Di seguito è riportato un esempio di un file `Cargo.lock`.

```
# This file is automatically @generated by Cargo.
# It is not intended for manual editing.
[[package]]
name = "adler32"
version = "1.0.3"
source = "registry+https://github.com/rust-lang/crates.io-index"

[[package]]
name = "aho-corasick"
version = "0.7.4"
source = "registry+https://github.com/rust-lang/crates.io-index"
```

> **Note**
>
> Questo file produce un output che contiene l'URL del pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

File binari Rust con cargo-auditable

Amazon Inspector SBOM Generator raccoglie le dipendenze dai Rust file binari creati con la libreria. `cargo-auditable` Ciò fornisce informazioni aggiuntive sulle dipendenze abilitando l'estrazione delle dipendenze dai binari compilati.

Funzionalità principali

- Estrae le informazioni sulle dipendenze direttamente dai Rust file binari creati con la libreria `cargo-auditable`

- Recupera i metadati e le informazioni sulla versione per le dipendenze incluse nei file binari

> **Note**
>
> Questo file produce un output che contiene l'URL di un pacchetto. Questo URL può essere utilizzato per specificare informazioni sui pacchetti software durante la generazione di una distinta base del software e può essere incluso nell'ScanSbomAPI. Per ulteriori informazioni, vedere package-url sul sito Web. GitHub

Artefatti non supportati

Questa sezione descrive gli artefatti non supportati.

Java

Il generatore Amazon Inspector SBOM Generator supporta solo il rilevamento delle vulnerabilità per le dipendenze provenienti dal repository principale. Maven Gli Maven archivi privati o personalizzati, come e, non sono supportati. Red Hat Maven Jenkins Per un rilevamento accurato delle vulnerabilità, assicurati che Java le dipendenze vengano estratte dal repository principale. Maven Le dipendenze da altri repository non verranno coperte nelle scansioni di vulnerabilità.

JavaScript

pacchetti esbuild

Per i esbuild pacchetti ridotti, Amazon Inspector SBOM Generator non supporta la scansione delle dipendenze per i progetti in uso. esbuild Le mappe di origine generate da esbuild non includono metadati sufficienti (nomi e versioni delle dipendenze) necessari per una generazione accurata. Sbomgen Per risultati affidabili, scansiona i file di progetto originali, come `node_modules/directory` `epackage-lock.json`, prima del processo di raggruppamento.

pacchetto.json

Amazon Inspector SBOM Generator non supporta la scansione del file package.json a livello di root per informazioni sulle dipendenze. Questo file specifica solo i nomi dei pacchetti e gli intervalli di versioni, ma non include le versioni dei pacchetti completamente risolte. Per risultati di scansione accurati, utilizzate `package.json` o altri file di blocco, come `yarn.lock` `epnpm.lock`, che includono versioni risolte.

Dotnet

Quando si utilizzano versioni mobili o intervalli di versioni`PackageReference`, diventa più difficile determinare l'esatta versione del pacchetto utilizzata in un progetto senza eseguire la risoluzione del pacchetto. Le versioni e gli intervalli di versioni fluttuanti consentono agli sviluppatori di specificare un intervallo di versioni del pacchetto accettabili anziché una versione fissa.

Binari Go

Amazon Inspector SBOM Generator non esegue la scansione di Go file binari creati con flag di build configurati per escludere l'ID di build. Questi flag di build Bomerman impediscono di mappare accuratamente il file binario alla sua fonte originale. GoI file binari non chiari non sono supportati a causa dell'impossibilità di estrarre le informazioni sui pacchetti. Per una scansione accurata delle dipendenze, assicurati che i Go file binari siano compilati con le impostazioni predefinite, incluso l'ID di build.

Binari Rust

Amazon Inspector SBOM Generator analizza i Rust file binari solo se questi sono stati creati utilizzando la libreria cargo-auditable. Rusti file binari che non utilizzano questa libreria non dispongono dei metadati necessari per un'estrazione accurata delle dipendenze. Amazon Inspector SBOM Generator estrae la versione compilata della Rust toolchain a partire dalla Rust 1.7.3, ma solo per i file binari in un ambiente. Linux Per una scansione completa, crea file binari utilizzando cargo-auditable. Rust Linux

> **Note**
>
> Il rilevamento delle vulnerabilità per la Rust toolchain stessa non è supportato, anche se la versione della toolchain viene estratta.

Raccolta completa di ecosistemi Amazon Inspector SBOM Generator

Amazon Inspector SBOM Generator è uno strumento per creare una distinta base del software (SBOM) ed eseguire la scansione delle vulnerabilità per i pacchetti supportati dai sistemi operativi e dai linguaggi di programmazione. Supporta inoltre la scansione di vari ecosistemi oltre ai sistemi operativi principali, garantendo un'analisi solida e dettagliata dei componenti dell'infrastruttura.

Generando una SBOM, gli utenti possono comprendere la composizione dei loro moderni stack tecnologici, identificare le vulnerabilità nei componenti dell'ecosistema e ottenere visibilità sul software di terze parti.

Ecosistemi supportati

La raccolta di ecosistemi estende la generazione di SBOM oltre ai pacchetti installati tramite gestori di pacchetti del sistema operativo. Ciò avviene attraverso la raccolta di applicazioni distribuite con metodi alternativi, come l'installazione manuale. Il generatore SBOM di Amazon Inspector supporta la scansione per i seguenti ecosistemi:

Ecosistemi	Applicazioni
Oracle Java	JDK JRE Amazon Corretto
Apache	httpd gatto
WordPress	core plugin tema
Google	Chrome
Node.JS	nodo

Apachecollezione ecosistemica

Amazon Inspector SBOM Generator analizza le Apache installazioni che si trovano in percorsi di installazione comuni su più piattaforme:

- macOS: `/Library/`
- Linux: `/etc/`, `/usr/share`, `/usr/lib`, `/usr/local`, `/var`, `/opt`

Applicazioni supportate

- httpd
- tomcat

Funzionalità principali

- Apache httpd— Analizza il `/include/ap_release.h` file per estrarre le macro di installazione, che contengono le stringhe di identificazione principali, le stringhe di identificazione minori e le stringhe di identificazione delle patch.
- Apache tomcat— Decomprime il `catalina.jar` file per estrarre le macro di installazione all'interno del file (), che contiene la stringa della versione. `META-INF/MANIFEST.MF`

Esempio di file **`ap_release.h`**

Di seguito è riportato un esempio del contenuto all'interno del `ap_release.h` file.

```
//truncated

#define AP_SERVER_BASEVENDOR "Apache Software Foundation"
#define AP_SERVER_BASEPROJECT "Apache HTTP Server"
#define AP_SERVER_BASEPRODUCT "Apache"

#define AP_SERVER_MAJORVERSION_NUMBER 2
#define AP_SERVER_MINORVERSION_NUMBER 4
#define AP_SERVER_PATCHLEVEL_NUMBER   1
#define AP_SERVER_DEVBUILD_BOOLEAN    0

//truncated
```

Esempio: PURL

Di seguito è riportato un esempio di URL di pacchetto per un'`Apache httpd`applicazione.

```
Sample PURL: pkg:generic/apache/httpd@2.4.1
```

Esempio di file **`catalina.jar/META-INF/MANIFEST.MF`**

Di seguito è riportato un esempio del contenuto all'interno del `catalina.jar/META-INF/MANIFEST.MF` file.

```
//truncated

Implementation-Title: Apache Tomcat
Implementation-Vendor: Apache Software Foundation
Implementation-Version: 10.1.31

//truncated
```

Esempio: PURL

Di seguito è riportato un esempio di URL di pacchetto per un'`Apache Tomcat`applicazione.

```
Sample PURL: pkg:generic/apache/tomcat@10.1.31
```

Javaraccolta di ecosistemi

Applicazioni supportate

- Oracle JDK
- Oracle JRE
- Amazon Corretto

Funzionalità principali

- Estrae la stringa dell'Javainstallazione.
- Identifica il percorso della directory che contiene il Java runtime.
- Identifica il fornitore comeOracle JDK, Oracle JRE e. Amazon Corretto

Amazon Inspector SBOM Generator esegue la scansione delle Java installazioni attraverso i seguenti percorsi e piattaforme di installazione:

- macOS: `/Library/Java/JavaVirtualMachines`
- Linux 32-bit: `/usr/lib/jvm`
- Linux 64-bit: `/usr/lib64/jvm`
- Linux (generic): `/usr/java and /opt/java`

JavaInformazioni sulla versione di esempio

Di seguito è riportato un esempio di release. Oracle Java

```
// Amazon Corretto
IMPLEMENTOR="Amazon.com Inc."
IMPLEMENTOR_VERSION="Corretto-17.0.11.9.1"
JAVA_RUNTIME_VERSION="17.0.11+9-LTS"
JAVA_VERSION="17.0.11"
JAVA_VERSION_DATE="2024-04-16"
LIBC="default"
MODULES="java.base java.compiler java.datatransfer java.xml java.prefs java.desktop
 java.instrument java.logging java.management java.security.sasl java.naming
 java.rmi java.management.rmi java.net.http java.scripting java.security.jgss
 java.transaction.xa java.sql java.sql.rowset java.xml.crypto java.se java.smartcardio
 jdk.accessibility jdk.internal.jvmstat jdk.attach jdk.charsets jdk.compiler
 jdk.crypto.ec jdk.crypto.cryptoki jdk.dynalink jdk.internal.ed jdk.editpad
 jdk.hotspot.agent jdk.httpserver jdk.incubator.foreign jdk.incubator.vector
 jdk.internal.le jdk.internal.opt jdk.internal.vm.ci jdk.internal.vm.compiler
 jdk.internal.vm.compiler.management jdk.jartool jdk.javadoc jdk.jcmd jdk.management
 jdk.management.agent jdk.jconsole jdk.jdeps jdk.jdwp.agent jdk.jdi jdk.jfr jdk.jlink
 jdk.jpackage jdk.jshell jdk.jsobject jdk.jstatd jdk.localedata jdk.management.jfr
 jdk.naming.dns jdk.naming.rmi jdk.net jdk.nio.mapmode jdk.random jdk.sctp
 jdk.security.auth jdk.security.jgss jdk.unsupported jdk.unsupported.desktop
 jdk.xml.dom jdk.zipfs"
OS_ARCH="x86_64"
OS_NAME="Darwin"
SOURCE=".:git:7917f11551e8+"

// JDK
IMPLEMENTOR="Oracle Corporation"
JAVA_VERSION="19"
JAVA_VERSION_DATE="2022-09-20"
LIBC="default"
MODULES="java.base java.compiler java.datatransfer java.xml java.prefs java.desktop
 java.instrument java.logging java.management java.security.sasl java.naming
```

```
 java.rmi java.management.rmi java.net.http java.scripting java.security.jgss
 java.transaction.xa java.sql java.sql.rowset java.xml.crypto java.se java.smartcardio
 jdk.accessibility jdk.internal.jvmstat jdk.attach jdk.charsets jdk.zipfs jdk.compiler
 jdk.crypto.ec jdk.crypto.cryptoki jdk.dynalink jdk.internal.ed jdk.editpad
 jdk.hotspot.agent jdk.httpserver jdk.incubator.concurrent jdk.incubator.vector
 jdk.internal.le jdk.internal.opt jdk.internal.vm.ci jdk.internal.vm.compiler
 jdk.internal.vm.compiler.management jdk.jartool jdk.javadoc jdk.jcmd jdk.management
 jdk.management.agent jdk.jconsole jdk.jdeps jdk.jdwp.agent jdk.jdi jdk.jfr jdk.jlink
 jdk.jpackage jdk.jshell jdk.jsobject jdk.jstatd jdk.localedata jdk.management.jfr
 jdk.naming.dns jdk.naming.rmi jdk.net jdk.nio.mapmode jdk.random jdk.sctp
 jdk.security.auth jdk.security.jgss jdk.unsupported jdk.unsupported.desktop
 jdk.xml.dom"
OS_ARCH="x86_64"
OS_NAME="Darwin"
SOURCE=".:git:53b4a11304b0 open:git:967a28c3d85f"
```

Esempio: PURL

Di seguito è riportato un esempio di URL del pacchetto per una Oracle Java versione.

```
Sample PURL:
# Amazon Corretto
pkg:generic/amazon/amazon-corretto@21.0.3
# Oracle JDK
pkg:generic/oracle/jdk@11.0.16
# Oracle JRE
pkg:generic/oracle/jre@20
```

Googleraccolta di ecosistemi

Applicazione supportata

- Google Chrome

Artefatti supportati

Amazon Inspector raccoglie Google Chrome informazioni da quanto segue:

- Il `chrome/VERSION` file (sorgente della build)

- Il `puppeteer` file (installazione)

Amazon Inspector SBOM Generator analizza e raccoglie le versioni corrispondenti di ciascuno degli elementi supportati.

`chrome/VERSION`File di versione di esempio

Di seguito è riportato un esempio del file di `chrome/VERSION` versione.

```
MAJOR=130
MINOR=0
BUILD=6723
PATCH=58
```

Esempio: PURL

Di seguito è riportato un esempio di URL del pacchetto per un file di `chrome/VERSION` versione.

```
Sample PURL: pkg:generic/google/chrome@131.0.6778.87
```

File di **`puppeteer`** versione di esempio

Di seguito è riportato un esempio del file di `puppeteer` versione.

```
{
"name": "puppeteer",
"version": "23.9.0",
"description": "A high-level API to control headless Chrome over the DevTools
 Protocol",
"keywords": [
  "puppeteer",
  "chrome",
  "headless",
  "automation"
]
}
```

Esempio: PURL

Di seguito è riportato un esempio di URL del pacchetto per un file di `puppeteer` versione.

```
Sample PURL: pkg:generic/google/puppeteer@23.9.0
```

WordPressraccolta ecosistemica

Componenti supportati

- WordPress core
- WordPressplugin
- WordPresstemi

Funzionalità principali

- WordPresscore — analizza il `/wp-includes/version.`php file per estrarre il valore della versione dalla variabile $wp_version.
- WordPressplugins: analizza il `/wp-content/plugins/<WordPress Plugin>/readme.txt` file o il `/wp-content/plugins/<WordPress Plugin>/readme.`md file per estrarre il tag come stringa della versione. `Stable`
- WordPressthemes: analizza il `/wp-content/themes/<WordPress Theme>/style.css` file per estrarre la versione dai metadati della versione.

Esempio di file **`version.php`**

Di seguito è riportato un esempio di file WordPress principale`version.`php.

```
// truncated

/**
* The WordPress version string.
*
* Holds the current version number for WordPress core. Used to bust caches
* and to enable development mode for scripts when running from the /src directory.
```

```
*
* @global string $wp_version
*/
$wp_version = '6.5.5';

// truncated
```

Esempio: PURL

Di seguito è riportato un esempio di URL del pacchetto per WordPress core.

```
Sample PURL: pkg:generic/wordpress/core/wordpress@6.5.5
```

Esempio di file **`readme.txt`**

Di seguito è riportato un esempio di `readme.txt` file di WordPress plugin.

```
=== Plugin Name ===
Contributors: (this should be a list of wordpress.org userid's)
Donate link: https://example.com/
Tags: tag1, tag2
Requires at least: 4.7
Tested up to: 5.4
Stable tag: 4.3
Requires PHP: 7.0
License: GPLv2 or later
License URI: https://www.gnu.org/licenses/gpl-2.0.html

// truncated
```

Esempio: PURL

Quello che segue è un esempio di URL di pacchetto per un WordPress plugin.

```
Sample PURL: pkg:generic/wordpress/plugin/exclusive-addons-for-elementor@1.0.0
```

Esempio di file **`style.css`**

Di seguito è riportato un esempio di `style.css` file WordPress tematico.

```
/*
Author: the WordPress team
Author URI: https://wordpress.org
Description: Twenty Twenty-Four is designed to be flexible, versatile and applicable
 to any website. Its collection of templates and patterns tailor to different needs,
 such as presenting a business, blogging and writing or showcasing work. A multitude
 of possibilities open up with just a few adjustments to color and typography. Twenty
 Twenty-Four comes with style variations and full page designs to help speed up the
 site building process, is fully compatible with the site editor, and takes advantage
 of new design tools introduced in WordPress 6.4.
Requires at least: 6.4
Tested up to: 6.5
Requires PHP: 7.0
Version: 1.2
License: GNU General Public License v2 or later
License URI: http://www.gnu.org/licenses/gpl-2.0.html
Text Domain: twentytwentyfour
Tags: one-column, custom-colors, custom-menu, custom-logo, editor-style, featured-
images, full-site-editing, block-patterns, rtl-language-support, sticky-post,
 threaded-comments, translation-ready, wide-blocks, block-styles, style-variations,
 accessibility-ready, blog, portfolio, news
*/
```

Esempio: PURL

Di seguito è riportato un esempio di URL del pacchetto per un WordPress tema.

```
Sample PURL: pkg:generic/wordpress/theme/avada@1.0.0
```

Node.JSraccolta runtime

Applicazioni supportate

- node runtime binario per Node.JS

Artefatti supportati

- MacOSe Linux — rilevamento `node` binario tramite dettagli binari installati con`asdf`,`fnm`, `nvm``volta`, o contenitori ufficialiNode.JS.

Esempi MacOS e Linux percorsi

Di seguito è riportato un esempio di percorsi per MacOS eLinux.

```
NVM:   ~/.nvm/, /usr/local/nvm
FNM:   ~/.local/share/fnm/
ASDF:  ~/.asdf/
MISE:  ~/.local/share/mise/
VOLTA: ~/.volta/
```

Esempio: PURL

Di seguito è riportato un esempio di URL del pacchetto perNode.JS.

```
Sample PURL: pkg:generic/nodejs/node@20.18.0
```

Collezione di ecosistemi OpenSSL

Applicazioni supportate

Il supporto per le librerie e i pacchetti di sviluppo OpenSSL è limitato al software creato con OpenSSL ufficiale per le versioni 3.0.0 e successive. Il software deve inoltre seguire il controllo delle versioni semantiche. Le varianti e le versioni OpenSSL personalizzate o biforcate precedenti alla 3.0.0 non sono supportate.

Amazon Inspector SBOM Generator estrae le informazioni chiave sui pacchetti per ogni istanza OpenSSL installata.

Funzionalità principali

- Estrae la stringa della versione SEMVER di base dal file di intestazione OpenSSL
- Identifica il percorso della directory contenente l'installazione di OpenSSL

Amazon Inspector SBOM Generator cerca le installazioni OpenSSL eseguendo la scansione del file in percorsi di installazione comuni su più `openssl v.h` piattaforme.

Esempio di percorso di installazione per Linux/Unix

Quello che segue è un esempio di percorso di installazione per Linux/Unix.

```
/usr/local/include/openssl/opensslv.h
/usr/local/ssl/include/openssl/opensslv.h
/usr/local/openssl/include/openssl/opensslv.h
/usr/local/opt/openssl/include/openssl/opensslv.h
/usr/include/openssl/opensslv.h
```

Amazon Inspector SBOM Generator estrae le informazioni sulla versione analizzando il `openssl v.h` file e cercando le definizioni delle versioni.

```
# define OPENSSL_VERSION_MAJOR  3
# define OPENSSL_VERSION_MINOR  4
# define OPENSSL_VERSION_PATCH  0
```

Esempio: PURL

Di seguito è riportato un esempio di URL del pacchetto per la versione OpenSSL.

```
Sample PURL: pkg:generic/openssl/openssl@3.4.0
```

Raccolta di licenze Amazon Inspector SBOM Generator

Amazon Inspector SBOM Generator aiuta a tenere traccia delle informazioni sulle licenze in una distinta base del software (SBOM). Raccoglie informazioni sulle licenze dai pacchetti supportati nei sistemi operativi e nei linguaggi di programmazione. Con espressioni di licenza standardizzate nella SBOM generata, potete comprendere i vostri obblighi di licenza.

Raccogli informazioni sulla licenza

Comando della di esempio

L'esempio seguente mostra come raccogliere informazioni sulla licenza da una directory.

```
./inspector-sbomgen directory --path /path/to/your/directory/ --collect-licenses
```

Esempio di componente SBOM

L'esempio seguente mostra una voce di componente nella SBOM generata.

```
"components": [
    {
      "bom-ref": "comp-2",
      "type": "application",
      "name": "sample-js-pkg",
      "version": "1.2.3",
      "licenses": [
        {
          "expression": "Apache-2.0 AND (MIT OR GPL-2.0-only)"
        }
      ],
      "purl": "pkg:npm/sample-js-pkg@1.2.3",
    }
  ]
```

Pacchetti supportati

I seguenti linguaggi di programmazione e pacchetti del sistema operativo sono supportati per la raccolta delle licenze.

Target	Programma di gestione dei pacchetti	Fonte di informazioni sulla licenza	Tipo
Alma Linux	RPM	• /usr/lib/sysimage/rpm/rpmdb.sqlite • /usr/lib/sysimage/rpm/Packages • /.db usr/lib/sysimage/rpm/Packages • /.sqlite var/lib/rpm/rpmdb	Sistema operativo

Target	Programma di gestione dei pacchetti	Fonte di informazioni sulla licenza	Tipo
		• /var/lib/rpm/Packages • /.db var/lib/rpm/Packages	
Amazon Linux	RPM	• /.sqlite usr/lib/sysimage/rpm/rpmdb • /usr/lib/sysimage/rpm/Packages • /.db usr/lib/sysimage/rpm/Packages • /.sqlite var/lib/rpm/rpmdb • /var/lib/rpm/Packages • /.db var/lib/rpm/Packages	Sistema operativo
CentOS	RPM	• /.sqlite usr/lib/sysimage/rpm/rpmdb • /usr/lib/sysimage/rpm/Packages • /.db usr/lib/sysimage/rpm/Packages • /.sqlite var/lib/rpm/rpmdb • /var/lib/rpm/Packages • /.db var/lib/rpm/Packages	Sistema operativo

Target	Programma di gestione dei pacchetti	Fonte di informazioni sulla licenza	Tipo
Fedora	RPM	• /.sqlite usr/lib/sysimage/rpm/rpmdb • /usr/lib/sysimage/rpm/Packages • /.db usr/lib/sysimage/rpm/Packages • /.sqlite var/lib/rpm/rpmdb • /var/lib/rpm/Packages • /.db var/lib/rpm/Packages	Sistema operativo
OpenSUSE	RPM	• /.sqlite usr/lib/sysimage/rpm/rpmdb • /usr/lib/sysimage/rpm/Packages • /.db usr/lib/sysimage/rpm/Packages • /.sqlite var/lib/rpm/rpmdb • /var/lib/rpm/Packages • /.db var/lib/rpm/Packages	Sistema operativo

Target	Programma di gestione dei pacchetti	Fonte di informazioni sulla licenza	Tipo
Oracle Linux	RPM	• /.sqlite usr/lib/sysimage/rpm/rpmdb • /usr/lib/sysimage/rpm/Packages • /.db usr/lib/sysimage/rpm/Packages • /.sqlite var/lib/rpm/rpmdb • /var/lib/rpm/Packages • /.db var/lib/rpm/Packages	Sistema operativo
Photon OS	RPM	• /.sqlite usr/lib/sysimage/rpm/rpmdb • /usr/lib/sysimage/rpm/Packages • /.db usr/lib/sysimage/rpm/Packages • /.sqlite var/lib/rpm/rpmdb • /var/lib/rpm/Packages • /.db var/lib/rpm/Packages	Sistema operativo

Target	Programma di gestione dei pacchetti	Fonte di informazioni sulla licenza	Tipo
RHEL	RPM	• /.sqlite usr/lib/sysimage/rpm/rpmdb • /usr/lib/sysimage/rpm/Packages • /.db usr/lib/sysimage/rpm/Packages • /.sqlite var/lib/rpm/rpmdb • /var/lib/rpm/Packages • /.db var/lib/rpm/Packages	Sistema operativo
Rocky Linux	RPM	• /.sqlite usr/lib/sysimage/rpm/rpmdb • /usr/lib/sysimage/rpm/Packages • /.db usr/lib/sysimage/rpm/Packages • /.sqlite var/lib/rpm/rpmdb • /var/lib/rpm/Packages • /.db var/lib/rpm/Packages	Sistema operativo

Target	Programma di gestione dei pacchetti	Fonte di informazioni sulla licenza	Tipo
SLES	RPM	• /.sqlite usr/lib/sysimage/rpm/rpmdb • /usr/lib/sysimage/rpm/Packages • /.db usr/lib/sysimage/rpm/Packages • /.sqlite var/lib/rpm/rpmdb • /var/lib/rpm/Packages • /.db var/lib/rpm/Packages	Sistema operativo
Alpine Linux	APK	`/lib/apk/db/installed`	Sistema operativo
Chainguard	APK	`/lib/apk/db/installed`	Sistema operativo
Debian	DPKG	`/usr/share/doc/*/copyright`	Sistema operativo
Ubuntu	DPKG	`/usr/share/doc/*/copyright`	Sistema operativo
Node.js	Javascript	`node_modules/*/package.json`	Linguaggio di programmazione
PHP	Pacchetto Composer	• `composer.lock` • `/vendor/composer/installed.json`	Linguaggio di programmazione

Target	Programma di gestione dei pacchetti	Fonte di informazioni sulla licenza	Tipo
Go	Go	`LICENSE`	Linguaggio di programmazione
Python	Python/Egg/Wheel	• `.dist-info/METADATA` • `.egg-info` • `.egg-info/PKG-INFO`	Linguaggio di programmazione
Ruby	RubyGem	`*.gemspec`	Linguaggio di programmazione
Rust	crate	`Cargo.toml`	Linguaggio di programmazione

Standardizzazione delle espressioni di licenza

Il formato delle espressioni di licenza SPDX fornisce una rappresentazione accurata dei termini di licenza presenti nel software open source. Amazon Inspector SBOM Generator standardizza tutte le informazioni sulla licenza in espressioni di licenza SPDX attraverso le regole descritte in questa sezione. Le regole garantiscono coerenza e compatibilità tra le informazioni sulle licenze.

Mappatura degli identificatori in formato abbreviato SPDX

Tutti i nomi di licenza sono mappati su identificatori in formato breve SPDX. Ad esempio, `MIT License` è abbreviata in `MIT`.

Combinazione multipla di licenze

È possibile combinare più di una licenza con l'`AND`operatore. Di seguito è riportato un comando di esempio che mostra come formattare il comando.

```
MIT AND Apache-2.0
```

Prefisso di licenza personalizzato

Le licenze personalizzate hanno il prefisso`LicenseRef`, ad esempio. `LicenseRef-CompanyPrivate`

Prefisso di eccezione personalizzato

Le eccezioni personalizzate hanno il prefisso`AdditionRef-`, ad esempio. `AdditionRef-CustomException`

Cos'è l'URL di un pacchetto?

L'URL di un pacchetto o PURL è un formato standardizzato utilizzato per identificare pacchetti software, componenti e librerie in diversi sistemi di gestione dei pacchetti. Il formato semplifica il monitoraggio, l'analisi e la gestione delle dipendenze nei progetti software, in particolare durante la generazione di una distinta base del software (). SBOMs

Struttura PURL

La struttura PURL è simile a un URL ed è composta da più componenti:

- `pkg`— Il prefisso letterale
- `type`— Il tipo di pacchetto
- `namespace`— Il raggruppamento
- `name`— Il nome del pacchetto
- `version`— La versione del pacchetto
- `qualifiers`— Coppie chiave-valore aggiuntive
- `subpath`— Il percorso del file nel pacchetto

Esempio: PURL

Di seguito è riportato un esempio di come potrebbe apparire un PURL.

```
pkg:<type>/<namespace>/<name>@<version>?<qualifiers>#<subpath>
```

Il PURL generico

Un PURL generico viene utilizzato per rappresentare pacchetti e componenti software che non rientrano negli ecosistemi di pacchetti consolidati, ad npm esempio, o. pypi maven Identifica i componenti software e acquisisce metadati che potrebbero non essere in linea con sistemi di gestione dei pacchetti specifici. Un PURL generico è utile per una varietà di progetti software, dai file binari compilati alle piattaforme, come e. Apache WordPress Ne consente l'applicazione in un'ampia gamma di casi d'uso, inclusi file binari compilati, piattaforme web e distribuzioni software personalizzate.

Casi d'uso principali

- Supporta i file binari compilati ed è utile per Go e Rust
- Supporta piattaforme web, come Apache andWordPress, in cui un pacchetto potrebbe non essere associato ai gestori di pacchetti tradizionali.
- Supporta software legacy personalizzato consentendo alle organizzazioni di fare riferimento a software o sistemi sviluppati internamente privi di pacchetti formali.

Formato di esempio

Di seguito è riportato un esempio del formato PURL generico.

```
pkg:generic/<namespace>/<name>@<version>?<qualifiers>
```

Esempi aggiuntivi del formato PURL generico

Di seguito sono riportati altri esempi del formato PURL generico.

Binario compilato Go

Quanto segue rappresenta il `inspector-sbomgen binary` compilato con aGo.

```
pkg:generic/inspector-sbomgen?go_toolchain=1.22.5
```

RustBinario compilato

Quanto segue rappresenta il `myrustapp` file binario compilato conRust.

```
pkg:generic/myrustapp?rust_toolchain=1.71.0
```

Progetto Apache

Quanto segue si riferisce a un progetto http nel Apache namespace.

```
pkg:generic/apache/httpd@1.0.0
```

Software WordPress

Quanto segue si riferisce a un software di baseWordPress.

```
pkg:generic/wordpress/core/wordpress@6.0.0
```

WordPresstema

Quanto segue si riferisce a un WordPress tema personalizzato.

```
pkg:generic/wordpress/theme/mytheme@1.0.0
```

WordPress Plugin

Quanto segue si riferisce a un WordPress plugin personalizzato.

```
pkg:generic/wordpress/plugin/myplugin@1.0.0
```

Gestione di riferimenti di versione non risolti o non standard in Amazon Inspector SBOM Generator

Amazon Inspector SBOM Generator individua e analizza gli artefatti supportati all'interno di un sistema identificando le dipendenze direttamente dai file di origine. Non è un gestore di pacchetti e non risolve intervalli di versioni, deduce versioni basate su riferimenti dinamici o gestisce le ricerche nel registro. Raccoglie le dipendenze solo così come sono definite negli artefatti sorgenti del progetto. In molti casi, le dipendenze nei manifesti dei pacchetti, ad esempio, o, vengono specificate utilizzando `package.json` versioni non `pom.xml` risolte o `requirements.txt` basate su intervalli. Questo argomento include esempi di come potrebbero apparire queste dipendenze.

Raccomandazioni

Amazon Inspector SBOM Generator estrae le dipendenze dagli artefatti di origine, ma non risolve o interpreta intervalli di versioni o riferimenti dinamici. Per una scansione più accurata delle vulnerabilità

SBOMs, consigliamo di utilizzare identificatori di versione semantici risolti nelle dipendenze del progetto.

Java

InfattiJava, i Maven progetti possono utilizzare intervalli di versioni per definire le dipendenze nel file. `pom.xml`

```
<dependency>
    <groupId>org.inspector</groupId>
    <artifactId>inspector-api</artifactId>
    <version>(,1.0]</version>
</dependency>
```

L'intervallo specifica che qualsiasi versione fino alla 1.0 inclusa è accettabile. Tuttavia, se una versione non è una versione risolta, Amazon Inspector SBOM Generator non la raccoglierà perché non può essere mappata a una versione specifica.

JavaScript

Il `package.json` file può JavaScript infatti includere intervalli di versioni simili ai seguenti:

```
"dependencies": {
    "ky": "^1.2.0",
    "registry-auth-token": "^5.0.2",
    "registry-url": "^6.0.1",
    "semver": "^7.6.0"
}
```

L'^operatore specifica che qualsiasi versione superiore o uguale alla versione specificata è accettabile. Tuttavia, se la versione specificata non è una versione risolta, Amazon Inspector SBOM Generator non la raccoglierà perché così facendo si possono generare falsi positivi durante il rilevamento delle vulnerabilità.

Python

InfattiPython, il `requirements.txt` file può includere voci con un'espressione booleana.

```
requests>=1.0.0
```

L'>=operatore specifica che qualsiasi versione maggiore o uguale a `1.0.0` è accettabile. Poiché questa particolare espressione non specifica una versione esatta, Amazon Inspector SBOM Generator non è in grado di raccogliere in modo affidabile una versione per l'analisi delle vulnerabilità.

Amazon Inspector SBOM Generator non supporta identificatori di versione non standard o ambigui, come beta, latest o snapshot.

```
pkg:maven/org.example.com/testmaven@1.0.2%20Beta-RC-1_Release
```

> **Note**
>
> L'uso di un suffisso non standard, ad esempio, non è conforme al controllo delle versioni semantiche standard e non può essere valutato per individuare le vulnerabilità all'interno del motore di rilevamento Amazon Inspector. Beta-RC-1_Release

Utilizzo CycloneDX namespace con Amazon Inspector

Amazon Inspector ti offre CycloneDX namespace e nomi di proprietà con cui puoi usare. SBOMs Questa sezione descrive tutte le proprietà chiave/valore personalizzate che possono essere aggiunte ai componenti in CycloneDX SBOMs. Per ulteriori informazioni, consulta la tassonomia delle proprietà CyclonedX su GitHub sito web.

`amazon:inspector:sbom_scanner`tassonomia dei namespace

L'API Amazon Inspector Scan utilizza lo spazio dei `amazon:inspector:sbom_scanner` nomi e ha le seguenti proprietà:

Proprietà	Descrizione
`amazon:inspector:sbom_scanner:cisa_kev_date_added`	Indica quando la vulnerabilità è stata aggiunta al catalogo CISA Known Exploited Vulnerabilities.

Proprietà	Descrizione
`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:critical_vulnerabilities`	Conteggio del numero totale di vulnerabilità di gravità critica rilevate nello SBOM.
`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:fixed_version:` *`component_bom_ref`*	Fornisce la versione fissa del componente indicato per la vulnerabilità specificata.
`amazon:inspector:sbom_scanner:high_vulnerabilities`	Conteggio del numero totale di vulnerabilità ad alta gravità rilevate nella 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:is_malicious`	Indica se OpenSSF identifica i componenti interessati come dannosi.
`amazon:inspector:sbom_scanner:low_vulnerabilities`	Conteggio del numero totale di vulnerabilità di bassa 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:path`	Il percorso del file che fornisce le informazioni sull'oggetto del pacchetto.

Proprietà	Descrizione
`amazon:inspector:sbom_scanner:priority`	La priorità consigliata per correggere una determinata vulnerabilità. I valori in ordine decrescente sono «IMMEDIATE», «URGENT», «MODERATE» e «STANDARD».
`amazon:inspector:sbom_scanner:priority_intelligence`	La qualità dell'intelligence utilizzata per determinare la priorità di una determinata vulnerabilità. I valori includono «VERIFIED» o «UNVERIFIED».
`amazon:inspector:sbom_scanner:warning`	Fornisce un contesto sul motivo per cui un determinato componente non è stato analizzato, ad esempio: «Componente ignorato: nessun purl fornito».

`amazon:inspector:sbom_generator`tassonomia dello spazio dei nomi

Il generatore SBOM di Amazon Inspector utilizza lo spazio dei `amazon:inspector:sbom_generator` nomi e presenta le seguenti proprietà:

Proprietà	Descrizione
`amazon:inspector:sbom_generator:cpu_architecture`	L'architettura della CPU del sistema da inventariare (x86_64).
`amazon:inspector:sbom_generator:ec2:instance_id`	L'ID dell' EC2 istanza Amazon.
`amazon:inspector:sbom_generator:live_patching_enabled`	Un valore booleano che indica se il live patching è abilitato su Amazon Amazon EC2 Linux.
`amazon:inspector:sbom_generator:live_patched_cves`	Un elenco di CVEs patch applicate tramite live patching su Amazon Amazon EC2 Linux.

Proprietà	Descrizione
`amazon:inspector:sbom_generator:dockerfile_finding: inspector_finding_id`	Indica che un risultato di Amazon Inspector in un componente è correlato a Dockerfile controlli .
`amazon:inspector:sbom_generator:image_id`	L'hash appartenente al file di configurazione dell'immagine del contenitore (noto anche come ID immagine).
`amazon:inspector:sbom_generator:image_arch`	L'architettura dell'immagine del contenitore.
`amazon:inspector:sbom_generator:image_author`	L'autore dell'immagine del contenitore.
`amazon:inspector:sbom_generator:image_docker_version`	La versione docker utilizzata per creare l'immagine del contenitore.
`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:duplicate_purl`	Indica il pacchetto duplicato PURL trovato da un altro scanner.
`amazon:inspector:sbom_generator:kernel_name`	Il nome del kernel del sistema da inventariare.
`amazon:inspector:sbom_generator:kernel_version`	La versione del kernel del sistema da inventari are.
`amazon:inspector:sbom_generator:kernel_component`	Un valore booleano che indica se un pacchetto oggetto è un componente del kernel
`amazon:inspector:sbom_generator:running_kernel`	Un valore booleano che indica se un pacchetto oggetto è il kernel in esecuzione
`amazon:inspector:sbom_generator:layer_diff_id`	L'hash del livello di immagine del contenitore non compresso.

Proprietà	Descrizione
`amazon:inspector:sbom_generator:replaced_by`	Il valore che sostituisce quello corrente Go modulo.
`amazon:inspector:sbom_generator:os_hostname`	Il nome host del sistema da inventariare.
`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:file_size_bytes`	Indica la dimensione del file di un determinato artefatto.
`amazon:inspector:sbom_generator:unresolved_version`	Indica una stringa di versione che non è stata risolta dal gestore di pacchetti.
`amazon:inspector:sbom_generator:experimental:transitive_dependency`	Indica le dipendenze indirette da un gestore di pacchetti.

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

L' CI/CD integrazione con Amazon Inspector utilizza 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 software (SBOM) per archivi, immagini di container, directory, sistemi locali, compilati e binari. Go Rust L'API Amazon Inspector Scan analizza lo SBOM per creare un report con dettagli sulle vulnerabilità rilevate. Puoi integrare le scansioni delle immagini dei container di Amazon Inspector con la tua CI/CD pipeline per individuare le vulnerabilità del software e produrre report sulle vulnerabilità, che consentono di indagare e correggere i rischi prima della distribuzione. Per configurare CI/CD l'integrazione, puoi utilizzare i plug-in o creare un' CI/CD integrazione personalizzata utilizzando Amazon Inspector SBOM Generator e l'API Amazon Inspector Scan.

Argomenti

- Integrazione con i plugin
- Integrazione personalizzata
- Configurazione di un AWS account per utilizzare l'integrazione con Amazon Inspector CI/CD
- Controlli dei file Dockerfile di Amazon Inspector
- Creazione di un'integrazione di CI/CD pipeline personalizzata con Amazon Inspector Scan
- Utilizzo del plug-in Amazon Inspector Jenkins
- Utilizzo del plug-in Amazon Inspector TeamCity
- Utilizzo di Amazon Inspector con azioni GitHub
- Utilizzo di Amazon Inspector con i componenti GitLab
- Utilizzo CodeCatalyst delle azioni con Amazon Inspector
- Utilizzo delle azioni di scansione di Amazon Inspector con CodePipeline

Integrazione con i plugin

Amazon Inspector fornisce plug-in per le soluzioni supportate. CI/CD 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' CI/CD integrazione con Amazon Inspector tramite i plugin:

1. Si configura un Account AWS per consentire l'accesso all'API Amazon Inspector Scan. Per istruzioni, consultare Configurazione di un AWS account per utilizzare l'integrazione con Amazon Inspector CI/CD .
2. Installa il plug-in Amazon Inspector dal marketplace.
3. Installa e configura il binario Amazon Inspector SBOM Generator. Per istruzioni, consultare Generatore SBOM Amazon Inspector.
4. Aggiungi Amazon Inspector Scans come fase di costruzione nella tua CI/CD pipeline 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 supportate CI/CD

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

- Plugin Jenkins
- TeamCity Plugin
- GitHub azioni

Integrazione personalizzata

Se Amazon Inspector non fornisce plug-in per la tua CI/CD soluzione, puoi creare un' CI/CD integrazione 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' CI/CD integrazione personalizzata con Amazon Inspector:

1. Si configura un Account AWS per consentire l'accesso all'API Amazon Inspector Scan. Per istruzioni, consultare Configurazione di un AWS account per utilizzare l'integrazione con Amazon Inspector CI/CD .
2. Installa e configura il binario Amazon Inspector SBOM Generator. Per istruzioni, consultare 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 un'integrazione di CI/CD pipeline personalizzata con Amazon Inspector Scan

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

Per utilizzare l' CI/CD integrazione con Amazon Inspector, devi registrarti a un. Account AWS Account AWS Deve avere un ruolo IAM che consenta alla tua CI/CD 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 a un Account AWS, puoi passare aConfigura un ruolo IAM per l'integrazione CI/CD.

Argomenti

- Iscriviti a un Account AWS
- Crea un utente con accesso amministrativo
- 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 https://portal.aws.amazon.com/billing/registrazione.
2. Segui le istruzioni online.

   Parte della procedura di registrazione prevede la ricezione di una telefonata o di un messaggio di testo e l'immissione di un codice di verifica sulla tastiera del telefono.

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

AWS ti invia un'email di conferma dopo il completamento della procedura di registrazione. In qualsiasi momento, puoi visualizzare l'attività corrente del tuo account e gestirlo accedendo a https://aws.amazon.com/e scegliendo Il mio account.

Crea un utente con accesso amministrativo

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

Proteggi i tuoi Utente root dell'account AWS

1. Accedi 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.

Crea un utente con accesso amministrativo

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.

   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.

Assegna l'accesso a ulteriori utenti

1. In IAM Identity Center, crea un set di autorizzazioni conforme alla best practice dell'applicazione di autorizzazioni con il privilegio minimo.

   Segui le istruzioni riportate nella pagina Creazione di un set di autorizzazioni nella Guida per l'utente di AWS IAM Identity Center .

2. Assegna al gruppo prima gli utenti e poi l'accesso con autenticazione unica (Single Sign-On).

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

Configura un ruolo IAM per l'integrazione CI/CD

Per integrare la scansione di Amazon Inspector nella tua CI/CD pipeline devi creare una policy IAM che consenta l'accesso all'API Amazon Inspector Scan che analizza la distinta base del software (). SBOMs 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, seleziona Policies, quindi scegli Crea 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. Scegli Next (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. Scegli Next (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`.

Controlli dei file Dockerfile di Amazon Inspector

Questa sezione descrive come utilizzare Amazon Inspector SBOM Generator per scansionare immagini Dockerfiles e Docker container alla ricerca di configurazioni errate che introducono vulnerabilità di sicurezza.

Argomenti

- Utilizzo dei controlli Dockerfile Sbomgen
- Controlli Dockerfile supportati

Utilizzo dei controlli Dockerfile Sbomgen

I controlli Dockerfile vengono eseguiti automaticamente quando viene scoperto un file denominato `Dockerfile` o e quando `*.Dockerfile` viene scansionata un'immagine Docker.

È possibile disabilitare i controlli Dockerfile utilizzando l'argomento. `--skip-scanners dockerfile` Puoi anche combinare i controlli Dockerfile con qualsiasi scanner disponibile, come sistemi operativi o pacchetti di terze parti.

Esempi di comandi Docker check

I seguenti comandi di esempio mostrano come generare immagini SBOMs per Dockerfiles e container Docker, nonché per sistemi operativi e pacchetti di terze parti.

```
# generate SBOM only containing Docker checks for Dockerfiles in a local directory
./inspector-sbomgen directory --path ./project/ --scanners dockerfile

# generate SBOM for container image will by default include Dockerfile checks
./inspector-sbomgen container --image image:tag
```

```
# generate SBOM only containing Docker checks for specific Dockerfiles and Alpine,
 Debian, and Rhel OS packages in a local directory
/inspector-sbomgen directory --path ./project/ --scanners dockerfile,dpkg,alpine-
apk,rhel-rpm

# generate SBOM only containing Docker checks for specific Dockerfiles in a local
 directory
./inspector-sbomgen directory --path ./project/ --skip-scanners dockerfile
```

Componente di file di esempio

Di seguito è riportato un esempio di ricerca di Dockerfile per un componente di file.

```
{
     "bom-ref": "comp-2",
      "name": "dockerfile:data/docker/Dockerfile",
      "properties": [
        {
          "name": "amazon:inspector:sbom_scanner:dockerfile_finding:IN-DOCKER-001",
          "value": "affected_lines:27-27"
        }
      ],
      "type": "file"
    },
```

Esempio di componente di risposta alla vulnerabilità

Di seguito è riportato un esempio di ricerca di Dockerfile per un componente di risposta alle vulnerabilità.

```
{
      "advisories": [
        {
          "url": "https://docs.docker.com/develop/develop-images/instructions/"
        }
      ],
      "affects": [
        {
          "ref": "comp-2"
        }
      ],
```

```
      "analysis": {
        "state": "in_triage"
      },
      "bom-ref": "vuln-13",
      "created": "2024-03-27T14:36:39Z",
      "description": "apt-get layer caching: Using apt-get update alone in a RUN
 statement causes caching issues and subsequent apt-get install instructions to fail.",
      "id": "IN-DOCKER-001",
      "ratings": [
        {
          "method": "other",
          "severity": "info",
          "source": {
            "name": "AMAZON_INSPECTOR",
            "url": "https://aws.amazon.com/inspector/"
          }
        }
      ],
      "source": {
        "name": "AMAZON_INSPECTOR",
        "url": "https://aws.amazon.com/inspector/"
      },
      "updated": "2024-03-27T14:36:39Z"
    },
```

> **Note**
>
> Se si richiama Sbomgen senza il `--scan-sbom` flag, è possibile visualizzare solo i risultati non elaborati di Dockerfile.

Controlli Dockerfile supportati

SbomgenI controlli Dockerfile sono supportati per quanto segue:

- Il pacchetto binario Sudo
- Utilità Debian APT
- Segreti codificati
- Contenitori per radici
- Flag di comando che indeboliscono il runtime

- Variabili di ambiente che indeboliscono il runtime

Ciascuno di questi controlli Dockerfile ha un indice di gravità corrispondente, riportato all'inizio dei seguenti argomenti.

> **Note**
>
> Le raccomandazioni descritte nei seguenti argomenti si basano sulle migliori pratiche del settore.

Il pacchetto binario Sudo

> **Note**
>
> Il grado di gravità di questo controllo è Info.

Si consiglia di non installare o utilizzare il pacchetto binario Sudo perché ha un comportamento TTY e di inoltro del segnale imprevedibile. Per ulteriori informazioni, consulta User nel sito Web Docker Docs. Se il tuo caso d'uso richiede funzionalità simili al pacchetto binario Sudo, ti consigliamo di utilizzare Gosu.

DebianUtilità APT

> **Note**
>
> Il grado di severità di questo controllo è Alto.

Di seguito sono riportate le migliori pratiche per l'utilizzo delle utilità Debian APT.

Combinare **`apt-get`** i comandi in un'unica **`Run`** istruzione per evitare problemi di memorizzazione nella cache

Ti consigliamo di combinare `apt-get` i comandi in un'unica istruzione RUN all'interno del contenitore Docker. L'utilizzo `apt-get update` da solo comporta problemi di memorizzazione nella cache e l'esito negativo delle `apt-get install` istruzioni successive. Per ulteriori informazioni, vedere apt-get nel sito Web di Docker Docs.

> **Note**
>
> Il comportamento di memorizzazione nella cache descritto può verificarsi anche all'interno del Docker contenitore se il software del contenitore Docker non è aggiornato.

Utilizzo dell'utilità da riga di comando APT in modo non interattivo

Si consiglia di utilizzare l'utilità da riga di comando APT in modo interattivo. L'utilità da riga di comando APT è progettata come strumento per l'utente finale e il suo comportamento cambia tra le versioni. Per maggiori informazioni, vedere Utilizzo degli script e differenze rispetto agli altri strumenti APT nel sito web di Debian.

Segreti codificati

> **Note**
>
> Il grado di severità di questo controllo è Critico.

Le informazioni riservate nel tuo Dockerfile sono considerate un segreto codificato. I seguenti segreti codificati possono essere identificati tramite i controlli dei file Docker: Sbomgen

- AWS IDs chiave di accesso — `AKIAIOSFODNN7EXAMPLE`
- AWS chiavi segrete — `wJalrXUtnFEMI/K7MDENG/bPxRfiCYEXAMPLEKEY`
- DockerHub token di accesso personali — `dckr_pat_thisisa27charexample1234567`
- GitHub token di accesso personali — `ghp_examplev61wY7Pj1YnotrealUoY123456789`
- GitLab token di accesso personali — `glpat-12345example12345678`

contenitori root

> **Note**
>
> L'indicatore di gravità per questo controllo è Info.

Consigliamo di eseguire contenitori Docker senza privilegi di root. Per i carichi di lavoro containerizzati che non possono essere eseguiti senza i privilegi di root, consigliamo di creare le

applicazioni utilizzando un principio con il minor numero di privilegi. Per ulteriori informazioni, consulta User nel sito Web Docker Docs.

Variabili di ambiente che indeboliscono il runtime

> **Note**
>
> Il grado di severità per questo controllo è Alto.

Diverse utilità da riga di comando o runtime dei linguaggi di programmazione supportano l'aggiramento delle impostazioni predefinite sicure, il che consente l'esecuzione con metodi non sicuri.

NODE_TLS_REJECT_UNAUTHORIZED=0

Quando i processi vengono eseguiti con set to, la convalida del certificato TLS è disabilitata. Node.js `NODE_TLS_REJECT_UNAUTHORIZED 0` Per ulteriori informazioni, consulta NODE_TLS_REJECT_UNAUTHORIZED=0 nel sito Web Node.js.

GIT_SSL_NO_VERIFY=*

Quando i processi della riga di comando git vengono eseguiti con `GIT_SSL_NO_VERIFY` set, Git salta la verifica dei certificati TLS. Per ulteriori informazioni, consulta Variabili di ambiente nel sito Web Git.

PIP_TRUSTED_HOST=*

Quando i processi della riga di comando Python pip vengono eseguiti con `PIP_TRUSTED_HOST` set, Pip salta la verifica dei certificati TLS sul dominio specificato. Per ulteriori informazioni, consulta --trusted-host nel sito Web di Pip.

NPM_CONFIG_STRICT_SSL=false

Quando i processi della riga di comando Node.js npm vengono eseguiti con `NPM_CONFIG_STRICT_SSL` set to false, l'utilità Node Package Manager (npm) si connetterà al registro NPM senza convalidare i certificati TLS. Per ulteriori informazioni, vedere strict-ssl nel sito Web di npm Docs.

Flag di comando che indeboliscono il runtime

> **Note**
>
> Il grado di severità di questo controllo è Alto.

Analogamente alle variabili di ambiente che indeboliscono il runtime, diverse utilità della riga di comando o runtime dei linguaggi di programmazione supportano l'aggiramento delle impostazioni predefinite sicure, il che consente l'esecuzione con metodi non sicuri.

`npm --strict-ssl=false`

Quando i processi della riga di comando npm di Node.js vengono eseguiti con il `--strict-ssl=false` flag, l'utilità Node Package Manager (npm) si connette al registro NPM senza convalidare i certificati TLS. Per ulteriori informazioni, vedere strict-ssl nel sito Web di npm Docs.

`apk --allow-untrusted`

Quando l'Alpine Package Keeperutilità viene eseguita con il `--allow-untrusted` flag, `apk` installerà i pacchetti senza firme o non attendibili. Per ulteriori informazioni, consulta il seguente repository nel sito Web di Apline.

`apt-get --allow-unauthenticated`

Quando l'utilità dei `apt-get` pacchetti Debian viene eseguita con il `--allow-unauthenticated` flag, `apt-get` non controlla la validità del pacchetto. Per maggiori informazioni, vedere apt-Get (8) nel sito web di Debian.

`pip --trusted-host`

Quando l'utilità Python pip viene eseguita con il `--trusted-host` flag, il nome host specificato ignorerà la convalida del certificato TLS. Per ulteriori informazioni, consulta --trusted-host nel sito Web di Pip.

`rpm --nodigest, --nosignature, --noverify, --nofiledigest`

Quando il gestore di pacchetti basato su RPM `rpm` viene eseguito con i `--nofiledigest` flag,, e`--nodigest`, `--nosignature--noverify`, il gestore di pacchetti RPM non convalida le intestazioni,

le firme o i file dei pacchetti durante l'installazione di un pacchetto. Per ulteriori informazioni, consultate la seguente pagina di manuale RPM nel sito Web di RPM.

`yum-config-manager --setopt=sslverify false`

Quando il gestore di pacchetti basato su RPM `yum-config-manager` viene eseguito con il `--setopt=sslverify` flag impostato su false, il gestore di pacchetti YUM non convalida i certificati TLS. Per ulteriori informazioni, consulta la seguente pagina di manuale YUM nel sito Web di Man7.

`yum --nogpgcheck`

Quando il gestore di pacchetti basato su RPM `yum` viene eseguito con il `--nogpgcheck` flag, il gestore di pacchetti YUM salta il controllo delle firme GPG sui pacchetti. Per maggiori informazioni, vedete yum (8) nel sito web di Man7.

`curl --insecure, curl -k`

Quando `curl` viene eseguito con il `-k` flag `--insecure` o, la convalida del certificato TLS è disabilitata. Per impostazione predefinita, ogni connessione sicura `curl` effettuata viene verificata prima che il trasferimento abbia luogo. Questa opzione consente di `curl` saltare la fase di verifica e di procedere senza controllare. Per ulteriori informazioni, consulta la seguente pagina di manuale di Curl nel sito web di Curl.

`wget --no-check-certificate`

Quando `wget` viene eseguito con il `--no-check-certificate` flag, la convalida del certificato TLS è disabilitata. Per ulteriori informazioni, consultate la seguente pagina di manuale di Wget nel sito web GNU.

Controlli di rimozione per i database dei pacchetti del sistema operativo all'interno dei contenitori

> **Note**
>
> Il grado di gravità di questo controllo è Info.

La rimozione di un database dei pacchetti del sistema operativo riduce la capacità di scansionare l'inventario completo del software dell'immagine di un contenitore. Questi database devono essere lasciati intatti durante le fasi di creazione del contenitore.

I controlli di rimozione per un database di pacchetti del sistema operativo sono supportati per i seguenti gestori di pacchetti:

Alpine Package Keeper (APK)

Le immagini dei container che utilizzano il gestore di pacchetti APK per il software installato devono garantire che i file di sistema APK non vengano rimossi durante la compilazione. Per ulteriori informazioni, consulta la documentazione dei file di sistema APK manpages sul Arch Linux sito Web.

Gestore di pacchetti Debian (DPKG)

I contenitori che utilizzano il gestore di pacchetti DPKG, come le immagini basate su Debian, Ubuntu o Distroless, devono assicurarsi che il database DPKG non venga rimosso durante la creazione di un contenitore. Per ulteriori informazioni, consultate la documentazione dei file di sistema delle pagine di sistema di DPKG sul sito web. Ubuntu

Gestore di pacchetti RPM (RPM)

I contenitori che utilizzano RPM Package Manager (yum/dnf), come Amazon Linux o Red Hat Enterprise Linux, devono assicurarsi che il database RPM non venga rimosso durante la creazione di un contenitore. Per ulteriori informazioni, consulta la documentazione relativa ai file di sistema di RPM manpages sul sito Web RPM.

Creazione di un'integrazione di CI/CD pipeline personalizzata con Amazon Inspector Scan

Ti consigliamo di utilizzare i plug-in Amazon Inspector se CI/CD i plug-in Amazon Inspector sono disponibili per la tua CI/CD soluzione. CI/CD Se i CI/CD plugin Amazon Inspector non sono disponibili per la tua CI/CD soluzione, puoi utilizzare una combinazione di Amazon Inspector SBOM Generator e Amazon Inspector Scan API per creare un'integrazione personalizzata. CI/CD I passaggi seguenti descrivono come creare un'integrazione di CI/CD pipeline personalizzata con Amazon Inspector Scan.

> **Tip**
>
> Puoi utilizzare Amazon Inspector SBOM Generator (Sbomgen) per saltare i passaggi 3 e 4 se desideri generare e scansionare il tuo SBOM con un solo comando.

Fase 1: Configurazione Account AWS

Configura un Account AWS dispositivo che fornisca l'accesso all'API Amazon Inspector Scan. Per ulteriori informazioni, consulta Configurazione di un AWS account per utilizzare l'integrazione con Amazon Inspector CI/CD .

Fase 2: Installazione Sbomgen del binario

Installa e configura il Sbomgen file binario. Per ulteriori informazioni, consulta l'argomento relativo all'installazione di Sbomgen.

Fase 3. Uso di Sbomgen

Utilizzate il Sbomgen per creare un file SBOM per l'immagine di un contenitore che desiderate scansionare.

È possibile utilizzare l'esempio seguente. Sostituire *`image:id`* con il nome dell'immagine da scansionare. Sostituire *`sbom_path.json`* con la posizione in cui si desidera salvare l'output SBOM.

Esempio

```
./inspector-sbomgen container --image image:id -o sbom_path.json
```

Fase 4. Chiamata dell'API Amazon Inspector Scan

Chiama l'`inspector-scan`API per scansionare la SBOM generata e fornire un report di vulnerabilità.

È possibile utilizzare l'esempio seguente. Sostituire *`sbom_path.json`* con la posizione di un file SBOM compatibile con CyclonedX valido. *`ENDPOINT`*Sostituiscilo con l'endpoint API relativo al luogo in cui sei attualmente autenticato Regione AWS . Sostituisci *`REGION`* con la regione corrispondente.

Esempio

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

Per un elenco completo degli Regioni AWS endpoint, consulta Regioni ed endpoint.

(Facoltativo) Fase 5. Genera e scansiona SBOM con un solo comando

> **Note**
>
> Completa questo passaggio solo se hai saltato i passaggi 3 e 4.

Genera e scansiona il tuo SBOM con un unico comando usando il flag. `--scan-bom`

È possibile utilizzare l'esempio seguente. Sostituisci *`image:id`* con il nome dell'immagine che desideri scansionare. Sostituire *`profile`* con il profilo corrispondente. Sostituisci *`REGION`* con la regione corrispondente. Sostituire *`/tmp/scan.json`* con la posizione del file scan.json nella directory tmp.

Esempio

```
./inspector-sbomgen container --image image:id --scan-sbom --aws-profile
profile --aws-region REGION -o /tmp/scan.json
```

Per un elenco completo degli endpoint, consulta Regioni AWS Regioni ed endpoint.

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. Con il Jenkins plug-in Amazon Inspector, puoi aggiungere scansioni di vulnerabilità di Amazon Inspector alla tua pipeline. Jenkins 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, consultare Configurazione di un AWS account per utilizzare l'integrazione con Amazon Inspector CI/CD .

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 Jenkins 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. L'opzione automatica consente al plugin di scaricare la versione più recente. Inoltre, ti assicura di avere sempre le funzionalità più recenti, gli aggiornamenti di sicurezza e le correzioni di bug.

   a. (Opzione 1) Scegli Automatico per scaricare l'ultima versione di inspector-sbomgen. Questa opzione rileva automaticamente il sistema operativo e l'architettura della CPU attualmente in uso.

   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 Report Artifact Name, inserite un nome personalizzato per gli artefatti generati durante il processo di creazione. Questo aiuta a identificarli e gestirli in modo univoco.

   d. (Facoltativo) Per Skip files, specificate una o più directory da escludere dalla scansione. Considerate questa opzione per le cartelle che non devono essere scansionate a causa delle loro dimensioni.

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

   f. (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/). *AccountNumber RoleName*

ii. (Facoltativo) Per le credenziali AWS, specifica AWS le credenziali 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.

g. (Facoltativo) Seleziona Abilita le soglie di vulnerabilità. Con questa opzione, puoi determinare se la compilazione fallisce se una vulnerabilità analizzata supera un valore. Se tutti i valori sono uguali`0`, la compilazione ha esito positivo, indipendentemente dal numero di vulnerabilità analizzate. Per il punteggio EPSS, il valore può essere compreso tra 0 e 1. Se una vulnerabilità analizzata supera un valore, la compilazione fallisce e tutte le vulnerabilità CVEs con un punteggio EPSS superiore al valore vengono visualizzate nella console.

4. Scegli Save (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, sostituiscilo *`SBOMGEN_SOURCE`* con LinuxAMD64 o LinuxARM64. Sostituisci *`IMAGE_PATH`* con il percorso dell'immagine (ad esempio*`alpine:latest`*), *`IAM_ROLE`* con l'ARN del ruolo IAM che hai configurato nella fase 1 e *`ID`* con il tuo ID di Docker credenziale se utilizzi 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 del generatore SBOM di Amazon Inspector installato nella fase 3, *IMAGE_PATH* con il percorso dell'immagine (ad esempio*alpine:latest*), con *IAM_ROLE* l'ARN del ruolo IAM configurato nella fase 1 e *ID* con il tuo ID Docker credenziale se utilizzi un repository privato. Facoltativamente, puoi abilitare le soglie di vulnerabilità e specificare i valori per ogni gravità.

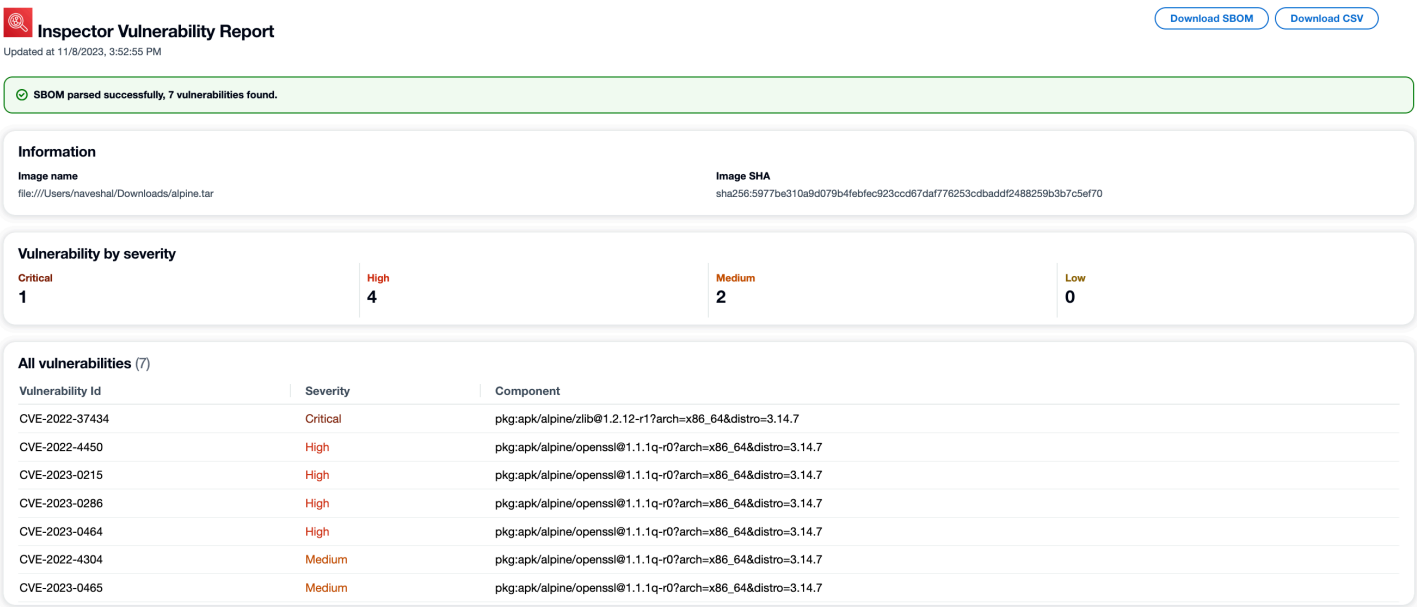
> **Note**
>
> SbomgenInseriscilo nella directory Jenkins e fornisci il percorso della directory Jenkins nel plugin (ad esempio). */opt/folder/arm64/inspector-sbomgen*

```
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:



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`.

Impossibile caricare l'immagine da fonti tarball, locali o remote

Errore:

```
2024/10/16 02:25:17 [ImageDownloadFailed]: failed to load image from
tarball, local, or remote sources.
```

> **Note**
>
> Questo errore può verificarsi se il plug-in Jenkins non è in grado di leggere l'immagine del contenitore, l'immagine del contenitore non viene trovata nel Docker motore e l'immagine del contenitore non viene trovata nel registro del contenitore remoto.

Risoluzione:

Verifica quanto segue;

- L'utente del plugin Jenkins dispone dei permessi di lettura per l'immagine che desideri scansionare.
- L'immagine che desideri scansionare è presente nel Docker motore.
- L'URL dell'immagine remota è corretto.
- Sei autenticato nel registro remoto (se applicabile).

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 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 esaminare e correggere i rischi prima della distribuzione. Con il TeamCity plug-in Amazon Inspector, puoi aggiungere scansioni di vulnerabilità di Amazon Inspector alla tua pipeline. TeamCity 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 TeamCity plug-in Amazon Inspector nel TeamCity marketplace all'indirizzo https://plugins.jetbrains.com/plugin/23236 -. amazon-inspector-scanner Per informazioni su come integrare Amazon Inspector Scan nella tua CI/CD pipeline, consulta Integrazione delle scansioni di Amazon Inspector nella tua pipeline. CI/CD Per un elenco dei sistemi operativi e dei linguaggi di programmazione supportati da Amazon Inspector, consulta Sistemi operativi e linguaggi di programmazione supportati. I passaggi seguenti descrivono come 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, consultare Configurazione di un AWS account per utilizzare l'integrazione con Amazon Inspector CI/CD .
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, consultare Installazione di 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.

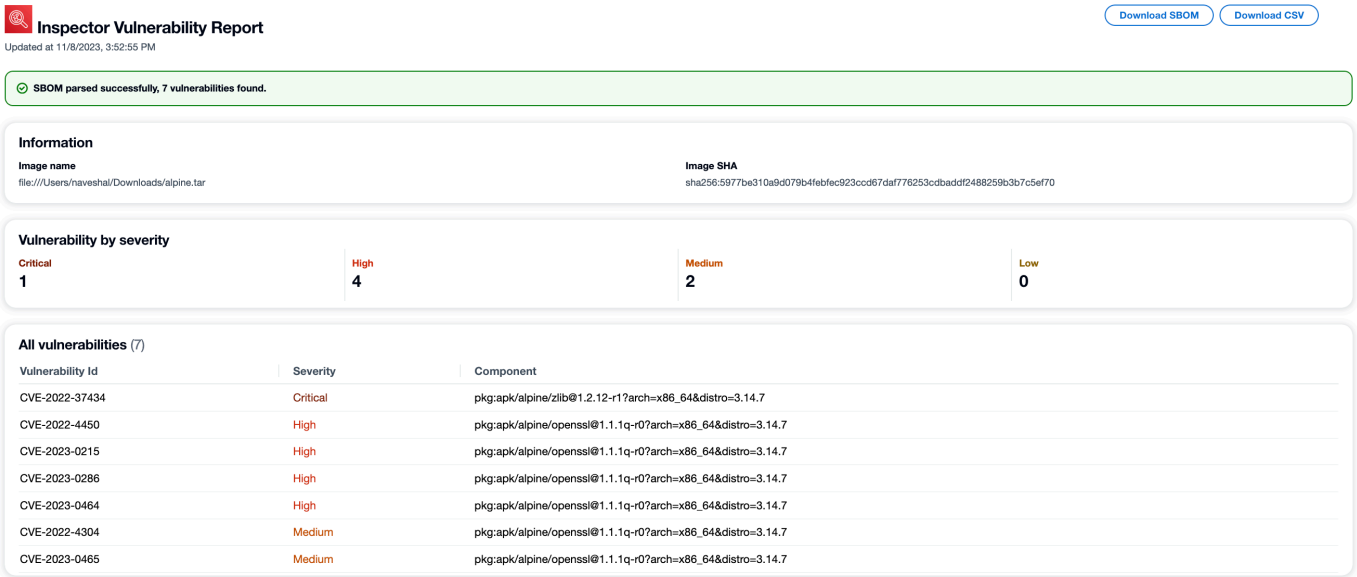
  Per ulteriori informazioni, consulta Installazione di Amazon Inspector SBOM Generator (Sbomgen) in Amazon Inspector SBOM Generator.
- Inserisci il tuo ID immagine. L'immagine può essere locale, remota o archiviata. I nomi delle immagini devono seguire la convenzione di Docker denominazione. Se state 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 successo 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:



Utilizzo di Amazon Inspector con azioni GitHub

Puoi usare Amazon Inspector con GitHub actionsper aggiungere scansioni di vulnerabilità di Amazon Inspector ai tuoi flussi di lavoro. GitHub Questo sfrutta 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 delle vulnerabilità di Amazon Inspector possono essere configurate per superare o fallire i flussi di lavoro in base al numero e alla gravità delle vulnerabilità rilevate. È possibile visualizzare la versione più recente dell'azione Amazon Inspector sul GitHub sito Web. Per informazioni su come integrare Amazon Inspector Scan nella tua CI/CD pipeline, consulta Integrazione delle scansioni di Amazon Inspector nella tua pipeline. CI/CD Per un elenco dei sistemi operativi e dei linguaggi di programmazione supportati da Amazon Inspector, consulta Sistemi operativi e linguaggi di programmazione supportati.

Utilizzo di Amazon Inspector con i componenti GitLab

Puoi usare Amazon Inspector con componenti GitLab CI/CD per aggiungere scansioni di vulnerabilità di Amazon Inspector ai tuoi progetti. GitLab Questo sfrutta 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 delle vulnerabilità di Amazon Inspector possono essere configurate per superare o fallire i flussi di lavoro in base al numero e alla gravità delle vulnerabilità rilevate. Puoi visualizzare la versione più recente del componente Amazon

Inspector sul GitLab sito Web. Per informazioni su come integrare Amazon Inspector Scan nella tua CI/CD pipeline, consulta Integrazione delle scansioni di Amazon Inspector nella tua pipeline. CI/CD Per un elenco dei sistemi operativi e dei linguaggi di programmazione supportati da Amazon Inspector, consulta Sistemi operativi e linguaggi di programmazione supportati.

Utilizzo CodeCatalyst delle azioni con Amazon Inspector

Puoi usare Amazon Inspector con Amazon CodeCatalyst per aggiungere scansioni di vulnerabilità di Amazon Inspector ai tuoi flussi di lavoro. CodeCatalyst Questo sfrutta 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 delle vulnerabilità di Amazon Inspector possono essere configurate per superare o fallire i flussi di lavoro in base al numero e alla gravità delle vulnerabilità rilevate. Per informazioni su come integrare Amazon Inspector Scan nella tua CI/CD pipeline, consulta Integrazione delle scansioni di Amazon Inspector nella tua pipeline. CI/CD Per un elenco dei sistemi operativi e dei linguaggi di programmazione supportati da Amazon Inspector, consulta Sistemi operativi e linguaggi di programmazione supportati.

Utilizzo delle azioni di scansione di Amazon Inspector con CodePipeline

Puoi usare Amazon Inspector AWS CodePipeline aggiungendo scansioni di vulnerabilità ai tuoi flussi di lavoro. Questa integrazione sfrutta Amazon Inspector SBOM Generator e Amazon Inspector Scan API per produrre report dettagliati alla fine della build. L'integrazione consente di analizzare e correggere i rischi prima della distribuzione. L'`InspectorScan`azione è un'azione di elaborazione gestita CodePipeline che automatizza il rilevamento e la correzione delle vulnerabilità di sicurezza nel codice open source. Puoi utilizzare questa azione con il codice sorgente dell'applicazione nel tuo repository di terze parti, ad esempio Bitbucket Cloud, GitHub o con immagini per applicazioni container. Per ulteriori informazioni, consulta il riferimento all'azione InspectorScan invoke nella Guida per l'utente.AWS CodePipeline

Valutazione della copertura di Amazon Inspector del tuo ambiente AWS

Puoi valutare la copertura di Amazon Inspector del tuo AWS ambiente dalla schermata di gestione dell'account nella console Amazon Inspector, che mostra dettagli e statistiche sullo stato delle scansioni di Amazon Inspector per i tuoi account e le tue risorse.

> **Note**
>
> Se sei l'amministratore delegato di un'organizzazione, puoi visualizzare dettagli e statistiche per tutti gli account dell'organizzazione.

La procedura seguente descrive come valutare la copertura del tuo ambiente Amazon Inspector.

Per valutare la copertura di Amazon Inspector del tuo ambiente AWS

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Dal pannello di navigazione, scegli Gestione dell'account.
3. Per rivedere la copertura, scegli una delle seguenti schede:
   - Scegli Account per esaminare la copertura a livello di account.
   - Scegli Istanze per esaminare la copertura delle istanze Amazon Elastic Compute Cloud EC2 (Amazon).
   - Scegli i repository Container per esaminare la copertura dei repository Amazon Elastic Container Registry (Amazon ECR).
   - Scegli le immagini dei container per esaminare la copertura delle immagini dei container Amazon ECR.
   - Scegli le funzioni Lambda per esaminare la copertura delle funzioni Lambda.

I seguenti argomenti descrivono le informazioni fornite da ciascuna di queste schede.

Argomenti

- Valutazione della copertura a livello di account

- Valutazione della copertura delle istanze Amazon EC2
- Valutazione della copertura dei repository Amazon ECR
- Valutazione della copertura delle immagini dei container Amazon ECR
- Valutazione della copertura delle funzioni AWS Lambda

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 Tipi di scansione automatizzati in 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 EC2 istanze Amazon presenti nel tuo AWS ambiente. 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' EC2 istanza 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 alla ricerca EC2 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 EC2 istanze Amazon.

In ogni scheda, la colonna Account specifica chi possiede un' Account AWS istanza.

EC2 tag di istanza: 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`.

Utilizzo monitorato: 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 scansionare l'istanza.

Per visualizzare ulteriori dettagli su un' EC2 istanza, scegli il link nella colonna dell'EC2 istanza. 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, consultaVisualizzazione dei dettagli relativi ai risultati di Amazon Inspector.

Valori dello stato di scansione per le EC2 istanze Amazon

Per un'istanza Amazon Elastic Compute Cloud (Amazon EC2), i possibili valori Status sono:

- Monitoraggio attivo: Amazon Inspector monitora e analizza continuamente l'istanza.
- Limite di storage dell'istanza senza agente superato: Amazon Inspector utilizza questo stato quando la dimensione combinata di tutti i volumi collegati a un'istanza è superiore a 1200 GB o un'istanza ha più di 8 volumi collegati.
- Limite di tempo di raccolta delle istanze senza agente superato: Amazon Inspector si verifica un timeout durante il tentativo di eseguire una scansione senza agente su un'istanza.

- EC2 istanza 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.
- EC2 Istanza 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. Valori di stato EC2 delle istanze Amazon

- Monitoraggio attivo con errori parziali: questo stato indica che EC2 la scansione è attiva, ma sono presenti errori associatiIspezione approfondita di Amazon Inspector per istanze Amazon basate su Linux EC2 . I possibili errori di ispezione approfondita 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' EC2 istanza, consulta. Scansione delle EC2 istanze Amazon

Valutazione della copertura dei repository Amazon ECR

La scheda Repositories mostra i repository Amazon ECR presenti 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 nuova scansione di Amazon 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 contenitori 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 di Amazon 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 l'ultima volta che Amazon Inspector ha verificato la presenza

di vulnerabilità in quella risorsa. 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, consultaVisualizzazione dei dettagli relativi ai risultati 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: scansione Amazon ECR con Amazon Inspector Per un elenco dei tipi di file multimediali supportati da Amazon Inspector, consulta Tipi di file multimediali supportati.

Per informazioni dettagliate sulla configurazione delle impostazioni di scansione per archivi e immagini, consulta. Scansione delle immagini dei contenitori 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 Funzione di scansione 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 l'ultima volta che Amazon Inspector ha verificato la presenza di vulnerabilità in quella risorsa. 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 (). CVEs
- 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 con AWS Organizations

Puoi utilizzare Amazon Inspector per gestire più account in un'organizzazione. A tale scopo, è necessario attivare Amazon Inspector con l'account di AWS Organizations gestione e specificare un amministratore delegato. L'amministratore delegato gestisce Amazon Inspector per un'organizzazione e può eseguire attività per conto dell'organizzazione. I seguenti argomenti descrivono la differenza tra un account amministratore delegato e un account membro, come designare e rimuovere un amministratore delegato e come gestire gli account dei membri.

Argomenti

- Informazioni sull'account amministratore delegato e sull'account membro in Amazon Inspector
- Designazione di un account amministratore delegato per Amazon Inspector

Informazioni sull'account amministratore delegato e sull'account membro in Amazon Inspector

Quando si utilizza Amazon Inspector in un ambiente con più account, l'account amministratore delegato ha accesso a metadati specifici. I metadati includono la scansione standard per Amazon EC2, Amazon ECR e Lambda e la scansione del codice Lambda. Include anche i risultati dei risultati di ricerca sulla sicurezza per gli account dei membri. Questa sezione fornisce informazioni sulle azioni che l'account amministratore delegato può eseguire e sugli account membro.

Azioni dell'amministratore delegato

In genere, quando l'amministratore delegato applica le 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:

- Solo l'account AWS Organizations di gestione può designare e rimuovere un amministratore delegato.
- Quando si designa un amministratore delegato, è necessario appartenere alla stessa organizzazione degli account dei membri che si desidera gestire.

- 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 SBOMs per tutti gli account dei membri dell'organizzazione.
- Imposta la modalità di EC2 scansione Amazon per tutti gli account dei 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 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 tutte SBOMs 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 account amministratore delegato per Amazon Inspector

L'amministratore delegato è un account che gestisce un servizio per un'organizzazione. Questo argomento descrive come designare un amministratore delegato per Amazon Inspector.

Considerazioni

Prima di designare un amministratore delegato, tieni presente quanto segue:

L'amministratore delegato può gestire un massimo di 10.000 membri.

> Se superi i 10.000 account membri, ricevi una notifica tramite Amazon CloudWatch Personal Health Dashboard e un'e-mail all'account amministratore delegato.

L'amministratore delegato è regionale.

> Amazon Inspector è un servizio regionale. È necessario ripetere i passaggi della procedura in ogni Regione AWS luogo in cui si prevede di utilizzare Amazon Inspector.

Un'organizzazione può avere un solo amministratore delegato.

> Se si designa un account come amministratore delegato in uno di essi Regione AWS, tale account deve essere l'amministratore delegato di tutti gli altri. Regioni AWS

La modifica di un amministratore delegato non disattiva Amazon Inspector per gli account dei membri.

> Se rimuovi un amministratore delegato, gli account dei membri diventano account autonomi e le impostazioni di scansione non ne risentono.

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 della tua

policy IAM per concedere queste autorizzazioni. Per ulteriori informazioni, consulta Gestione delle politiche IAM.

```
{
    "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 descrive come designare un amministratore delegato per l'organizzazione. Prima di completare la procedura, assicurati di far parte della stessa organizzazione degli account dei membri che desideri vengano gestiti dall'amministratore delegato.

> **Note**
>
> È necessario utilizzare l'account AWS Organizations di gestione per completare questa procedura. Solo l'account AWS Organizations di gestione può designare un amministratore delegato. Potrebbero essere necessarie autorizzazioni per designare un amministratore delegato. Per ulteriori informazioni, consulta Autorizzazioni necessarie per designare un amministratore delegato.

Quando attivi Amazon Inspector per la prima volta, Amazon Inspector crea il `AWSServiceRoleForAmazonInspector` ruolo collegato al servizio per l'account. Per informazioni su come Amazon Inspector utilizza i ruoli collegati ai servizi, consulta. Utilizzo di ruoli collegati ai servizi per Amazon Inspector

Console

Per designare un amministratore delegato per Amazon Inspector

1. Accedi all'account di AWS Organizations gestione, quindi apri la console Amazon Inspector su https://console.aws.amazon.com/inspector/ v2/home.
2. Usa il Regione AWS selettore per specificare Regione AWS dove vuoi designare l'amministratore delegato.
3. Dal riquadro di navigazione, scegli Impostazioni generali.
4. In Amministratore delegato, inserisci l'ID a 12 cifre della persona Account AWS che desideri designare come amministratore delegato.
5. Scegli Delegato, quindi scegli nuovamente Delegato.

Quando si designa un amministratore delegato, per impostazione predefinita vengono attivati tutti i tipi di scansione per l'account. Se desideri attivare Amazon Inspector per l'account di AWS Organizations gestione, completa la seguente procedura.

Per attivare Amazon Inspector per l'account di gestione AWS Organizations

1. Accedi all'account amministratore delegato, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Dal pannello di navigazione, scegli Gestione dell'account.
3. In Account, seleziona l'account di AWS Organizations gestione, quindi scegli Attiva.
4. Seleziona i tipi di scansione che desideri attivare per l'account di AWS Organizations gestione, quindi scegli Invia.

API

Designate 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.

Attivazione delle scansioni Amazon Inspector per gli account dei membri

Se sei l'amministratore delegato di un'organizzazione, puoi attivare la scansione di Amazon e EC2 Amazon ECR per gli account dei membri dell'organizzazione. Una volta attivata la scansione per un account membro, Amazon Inspector viene attivato automaticamente per quell'account e l'account viene associato all'account amministratore delegato. Per informazioni sui tipi di scansione di Amazon Inspector, consulta. Tipi di scansione automatizzati in Amazon Inspector Questa sezione descrive come attivare la scansione degli account dei membri.

Attiva la scansione degli account dei membri

È possibile attivare la scansione degli account dei membri in diversi modi. Le seguenti procedure descrivono come attivare la scansione per tutti gli account membro e account membro specifici come amministratore delegato, nonché come attivare la scansione come account membro.

Per attivare automaticamente la scansione per tutti gli account dei membri

1. Accedi utilizzando le credenziali dell'account amministratore delegato, quindi apri la console Amazon Inspector su v2/home. https://console.aws.amazon.com/inspector/
2. Usa il selettore di regione per scegliere Regione AWS dove vuoi attivare la scansione per tutti gli account dei membri.
3. Dal pannello di navigazione, scegli Gestione account. La scheda Account mostra tutti gli account dei membri associati all'account AWS Organizations di gestione.
4. In Organizzazione, seleziona la casella accanto a Numero di account. Quindi scegli Attiva per selezionare le opzioni di scansione che desideri applicare agli account dei membri. È possibile selezionare i seguenti tipi di scansione:

   - EC2 Scansione Amazon
   - Scansione Amazon ECR
   - Scansione standard Lambda
   - Scansione del codice Lambda

- Dopo aver selezionato i tipi di scansione preferiti, scegli Salva.

> **Note**
>
> Se disponi di più pagine di account, devi ripetere questo passaggio su ogni pagina. Puoi scegliere l'icona a forma di ingranaggio per modificare il numero di account visualizzati su ogni pagina.

5. Attiva l'impostazione Attiva automaticamente Inspector per gli account dei nuovi membri e seleziona le opzioni di scansione che desideri applicare ai nuovi account membro aggiunti alla tua organizzazione. È possibile selezionare i seguenti tipi di scansione:

   - EC2 Scansione Amazon
   - Scansione Amazon ECR
   - Scansione standard Lambda
   - Scansione del codice Lambda

   - Dopo aver selezionato i tipi di scansione preferiti, scegli Attiva.

   > **Note**
   >
   > L'impostazione Attiva automaticamente Inspector per gli account dei nuovi membri attiva Amazon Inspector per tutti i futuri membri della tua organizzazione.
   > Se il numero di account membri è superiore a 5.000, questa impostazione viene disattivata automaticamente. Se il numero totale di account membri scende a meno di 5.000, l'impostazione viene riattivata automaticamente.

6. (Consigliato) Ripeti ciascuno di questi passaggi in ogni Regione AWS punto in cui desideri attivare la scansione degli account dei membri.

Per attivare la scansione di account membri specifici

1. Accedi utilizzando le credenziali dell'account amministratore delegato, quindi apri la console Amazon Inspector su v2/home. https://console.aws.amazon.com/inspector/

2. Usa il selettore di regione per scegliere Regione AWS dove vuoi attivare la scansione per tutti gli account dei membri.
3. Dal pannello di navigazione, scegli Gestione account. La scheda Account mostra tutti gli account dei membri associati all'account AWS Organizations di gestione.
4. In Organizzazione, seleziona la casella accanto al numero di account di ciascun membro per cui desideri attivare la scansione. Quindi scegli Attiva per selezionare le opzioni di scansione che desideri applicare agli account dei membri. È possibile selezionare i seguenti tipi di scansione:

   - EC2 Scansione Amazon
   - Scansione Amazon ECR
   - Scansione standard Lambda
   - Scansione del codice Lambda

   - Dopo aver selezionato i tipi di scansione preferiti, scegli Salva.

   > **Note**
   >
   > Se disponi di più pagine di account, devi ripetere questo passaggio su ogni pagina. Puoi scegliere l'icona a forma di ingranaggio per modificare il numero di account visualizzati su ogni pagina.

5. (Consigliato) Ripeti ciascuno di questi passaggi in ogni Regione AWS punto in cui desideri attivare la scansione per membri specifici.

Per attivare la scansione come account membro

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su v2/home.
2. Usa il selettore di regione per scegliere Regione AWS dove vuoi attivare la scansione per tutti gli account dei membri.
3. Dal pannello di navigazione, scegli Gestione account. La scheda Account mostra tutti gli account dei membri associati all'account AWS Organizations di gestione.
4. In Organizzazione, seleziona la casella accanto al numero del tuo account. Quindi scegli Attiva per selezionare le opzioni di scansione che desideri applicare. È possibile selezionare i seguenti tipi di scansione:

- EC2 Scansione Amazon
- Scansione Amazon ECR
- Scansione standard Lambda
- Scansione del codice Lambda

- Dopo aver selezionato i tipi di scansione preferiti, scegli Salva.

5. (Consigliato) Ripeti questi passaggi in ogni regione in cui desideri attivare la scansione per il tuo account membro.

> **Note**
>
> Se il tuo account di AWS Organizations gestione dispone di un account amministratore delegato per Amazon Inspector, puoi attivarlo come account membro per visualizzare i dettagli della scansione.

Dissociazione degli account dei membri in Amazon Inspector

In qualità di amministratore delegato, potresti dover dissociare un account membro dal tuo account. Quando si annulla l'associazione di un account membro, Amazon Inspector rimane attivo nell'account e l'account diventa un account autonomo. Inoltre, non sei più autorizzato a gestire Amazon Inspector per l'account. Tuttavia, puoi associare account membri precedentemente dissociati al tuo account in qualsiasi momento. Questa sezione descrive come dissociare gli account dei membri dalla funzione di amministratore delegato.

Console

Per dissociare gli account dei membri utilizzando la console

1. Accedi utilizzando le credenziali dell'account amministratore delegato, quindi apri la console Amazon Inspector su v2/home https://console.aws.amazon.com/inspector/
2. Usa il selettore di regione per scegliere Regione AWS dove vuoi dissociare gli account dei membri.
3. Dal pannello di navigazione, scegli Gestione account.
4. In Organizzazione, seleziona la casella accanto a ciascun numero di account da dissociare.

5. Scegli il menu Azioni, quindi scegli Dissocia account.

API

Per dissociare gli account dei membri utilizzando l'API

Esegui l'operazione DisassociateMemberAPI. Nella richiesta, fornisci l'account da IDs cui stai dissociando.

Rimozione dell'amministratore delegato in Amazon Inspector

Potrebbe essere necessario rimuovere l'account amministratore delegato di Amazon Inspector. Puoi farlo dall'account di AWS Organizations gestione. Quando rimuovi l'account amministratore delegato di Amazon Inspector, Amazon Inspector rimane attivo nell'account e in tutti gli account dei membri. L'account amministratore delegato e tutti i relativi account membri diventano account autonomi e mantengono le impostazioni di scansione originali. Questa sezione descrive come rimuovere l'account amministratore delegato.

Rimuovere l'amministratore delegato di Amazon Inspector

Le seguenti procedure descrivono come rimuovere l'amministratore delegato di Amazon Inspector e come associare gli account membro dall'account amministratore delegato.

Per informazioni su come assegnare un amministratore delegato di Amazon Inspector, consulta Designazione di un account amministratore delegato per Amazon Inspector.

> **Note**
>
> Dopo aver assegnato un amministratore delegato di Amazon Inspector, l'amministratore delegato di Amazon Inspector deve associare gli account dei membri manualmente.

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 su v2/home. https://console.aws.amazon.com/inspector/
3. Usa il selettore di regione per scegliere Regione AWS dove vuoi rimuovere l'amministratore delegato.

4. Dal riquadro di navigazione, scegli Impostazioni generali.
5. In Amministratore delegato, scegli Rimuovi, quindi conferma l'azione.

Per associare i membri a un nuovo amministratore delegato

1. Accedi utilizzando le credenziali dell'account amministratore delegato, quindi apri la console Amazon Inspector su v2/home. https://console.aws.amazon.com/inspector/
2. Usa il selettore della regione per scegliere Regione AWS dove vuoi associare i membri.
3. Dal riquadro di navigazione, scegli Gestione account.
4. In Organizzazione, seleziona la casella accanto a Numero di account.
5. Scegli Azioni, quindi scegli Aggiungi membro.

Etichettare le risorse di Amazon Inspector

Un tag è un'etichetta che aggiungi a una AWS risorsa. I tag consentono di classificare AWS le risorse in base a criteri specifici. I tag sono costituiti da una coppia chiave-valore. La chiave tag è un'etichetta generica. Il valore del tag è una descrizione della chiave del tag. Con Amazon Inspector, puoi impostare regole di soppressione dei tag e configurazioni di scansione CIS. Puoi aggiungere fino a 50 tag a ciascuna delle tue risorse Amazon Inspector.

Nozioni fondamentali sull'etichettatura

Ciascun tag è costituito da una coppia chiave-valore. La chiave tag è un'etichetta generica. Il valore del tag è una descrizione della chiave del tag. Questo argomento descrive i fondamenti dell'etichettatura delle risorse di Amazon Inspector. Quando tagghi le risorse di Amazon Inspector, considera quanto segue:

- Puoi etichettare le regole di soppressione e le configurazioni di scansione CIS.
- Puoi aggiungere fino a 50 tag a ciascuna delle tue risorse Amazon Inspector.
- Le chiavi dei tag devono essere uniche.
- Una chiave tag può avere un solo valore di tag.
- Le chiavi e i valori dei tag possono avere un massimo di 128 caratteri UTF-8. I caratteri possono essere lettere, numeri, spazi o i seguenti simboli:. `_ . : / = + - @`
- Non puoi utilizzare il `aws` prefisso in nessuno dei tuoi tag o modificare i tag con questo prefisso. I tag con il `aws` prefisso possono essere utilizzati solo da. AWS
- I tag assegnati a una risorsa Amazon Inspector sono disponibili solo nel tuo AWS account e nel luogo in Regione AWS cui li hai creati.
- Quando elimini una risorsa, vengono eliminati anche tutti i tag ad essa associati.

Per ulteriori informazioni sui tag, consulta le migliori pratiche e strategie nella Guida per l'utente di Tagging AWS Resources and Tag Editor.

> **Note**
>
> I tag non sono destinati a memorizzare informazioni riservate o sensibili. Non utilizzare mai i tag per archiviare questo tipo di dati. I tag possono essere accessibili da altri AWS servizi.

Aggiungere tag

Puoi aggiungere tag alle risorse di Amazon Inspector. Queste risorse includono regole di soppressione e configurazioni di scansione CIS. I tag consentono di classificare le AWS risorse in base a criteri specifici. Questo argomento descrive come aggiungere tag alle risorse di Amazon Inspector.

Aggiungere tag alle risorse di Amazon Inspector

Puoi impostare regole di soppressione dei tag e configurazioni di scansione CIS. Le seguenti procedure descrivono come aggiungere tag nella console e con l'API Amazon Inspector.

Aggiungere tag nella console

Puoi aggiungere tag alle risorse di Amazon Inspector nella console.

Aggiungere tag alle regole di soppressione

È possibile aggiungere tag alle regole di soppressione durante la creazione. Per ulteriori informazioni, vedere Creazione di una regola di soppressione.

È inoltre possibile modificare una regola di soppressione per includere i tag. Per ulteriori informazioni, vedere Modifica di una regola di soppressione.

Aggiungere tag a una configurazione di scansione CIS

È possibile aggiungere tag a una configurazione di scansione CIS durante la creazione. Per ulteriori informazioni, vedere Creazione di una configurazione di scansione CIS.

È inoltre possibile modificare una configurazione di scansione CIS per includere i tag. Per ulteriori informazioni, vedere Modifica di una configurazione di scansione CIS.

Aggiungere tag con l'API Amazon Inspector

Puoi aggiungere tag alle risorse di Amazon Inspector con l'API Amazon Inspector.

Aggiungere tag alle risorse di Amazon Inspector

Utilizza l'`TagResource`API per aggiungere tag alle risorse di Amazon Inspector. È necessario includere l'ARN della risorsa e la coppia chiave-valore per il tag nel comando. Il comando di esempio

seguente utilizza una risorsa ARN vuota per un filtro di soppressione. La chiave è `CostAllocation` e il valore è. `dev` Per informazioni sui tipi di risorse per Amazon Inspector, consulta Azioni, risorse e chiavi di condizione per Amazon Inspector2 nel Service Authorization Reference.

```
aws inspector2 tag-resource \
--resource-arn "arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/
filter/${FilterId}" \
--tags CostAllocation=dev \
--region us-west-2
```

Aggiungere tag alle regole di soppressione durante la creazione

Utilizza l'`CreateFilter`API per aggiungere tag a una regola di soppressione durante la creazione.

```
aws inspector2 create-filter \
--name "ExampleSuppressionRuleECR" \
--action SUPPRESS \
--filter-criteria 'resourceType=[{comparison="EQUALS", value="AWS_ECR_IMAGE"}]' \
--tags Owner=ApplicationSecurity \
--region us-west-2
```

Aggiungere tag a una configurazione di scansione CIS

Utilizzate l'`CreateCisScanConfiguration`API per aggiungere un tag a una configurazione di scansione CIS.

```
aws inspector2 create-cis-scan-configuration \
--scan-name "CreateConfigWithTagsSample" \
--security-level LEVEL_2 \
--targets accountIds=SELF,targetResourceTags={InspectorCisScan=True} \
--schedule 'daily={startTime={timeOfDay=11:10,timezone=UTC}}' \
--tags Owner=SecurityEngineering \
--region us-west-2
```

Rimozione dei tag

Puoi rimuovere i tag dalle risorse di Amazon Inspector. Queste risorse includono regole di soppressione e configurazioni di scansione CIS. I tag consentono di classificare le AWS risorse in base a criteri specifici. Questo argomento descrive come rimuovere i tag dalle risorse di Amazon Inspector.

Rimuovere i tag dalle risorse di Amazon Inspector

Puoi rimuovere i tag dalle regole di soppressione e dalle configurazioni di scansione CIS. Le seguenti procedure descrivono come rimuovere i tag nella console e con l'API Amazon Inspector.

Rimuovere i tag nella console

Puoi rimuovere i tag dalle risorse di Amazon Inspector nella console.

Rimuovere i tag dalle regole di soppressione

È possibile rimuovere un tag da una regola di soppressione modificando la regola di soppressione in modo che non includa più il tag. Per ulteriori informazioni, vedere Modifica di una regola di soppressione.

Rimozione di tag da una configurazione di scansione CIS

È possibile rimuovere un tag da una configurazione di scansione CIS modificando la configurazione di scansione CIS in modo che non includa più il tag. Per ulteriori informazioni, vedere Modifica di una configurazione di scansione CIS.

Rimuovere i tag con l'API Amazon Inspector

Puoi rimuovere un tag da una risorsa Amazon Inspector con l'API Amazon Inspector.

Rimuovere i tag dalle risorse di Amazon Inspector

Utilizza l'`UntagResource`API per rimuovere i tag dalle risorse di Amazon Inspector.

Il seguente frammento mostra un esempio di come rimuovere un tag da una risorsa Amazon Inspector utilizzando. `UntagResource` È necessario includere l'ARN della risorsa e la chiave per il tag nel comando. L'esempio seguente utilizza una risorsa ARN vuota per un filtro di soppressione. La chiave è `CostAllocation`. Per informazioni sui tipi di risorse per Amazon Inspector, consulta Azioni, risorse e chiavi di condizione per Amazon Inspector2 nel Service Authorization Reference.

```
aws inspector2 untag-resource \
--resource-arn "arn:${Partition}:inspector2:${Region}:${Account}:owner/${OwnerId}/cis-configuration/${CISScanConfigurationId}" \
--tag-keys CostAllocation \
--region us-west-2
```

Monitoraggio dell'utilizzo e dei costi in Amazon Inspector

Puoi utilizzare la console e l'API Amazon Inspector per proiettare i costi mensili di Amazon Inspector per il tuo ambiente. Se sei l'amministratore di Amazon Inspector per un ambiente con più account, puoi visualizzare il costo totale del tuo ambiente e le metriche di costo per tutti gli account membri. Questa sezione descrive come accedere alle statistiche di utilizzo e calcolare i costi di utilizzo.

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. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su 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:

EC2 Scansione Amazon

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 EC2 per la scansione delle istanze. 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 EC2 la scansione di Amazon si tratta del numero totale di ore negli ultimi 30 giorni in cui Amazon Inspector ha fornito copertura attiva per ogni EC2 istanza in un account. Ad esempio, 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:
  - EC2 scansione: il costo riflette il numero medio di EC2 istanze coperte da Amazon Inspector negli ultimi 30 giorni.
  - Scansione dei contenitori ECR: il costo riflette la somma del numero di scansioni iniziali delle immagini e delle scansioni ripetute delle immagini 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

In Amazon Inspector, ogni tipo di scansione ha una traccia gratuita. Quando attivi un tipo di scansione, ti iscrivi automaticamente a una prova gratuita di 15 giorni per quel tipo di scansione. Una volta iniziata, la prova gratuita scade automaticamente dopo 15 giorni, anche se si disattiva il tipo di scansione.

> **Note**
>
> La versione di prova gratuita non si applica alla scansione CIS.

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
- Identity and Access Management per Amazon Inspector
- Monitoraggio di Amazon Inspector
- Convalida della conformità per Amazon Inspector
- Resilienza in Amazon Inspector
- Sicurezza dell'infrastruttura in Amazon Inspector
- Risposta agli incidenti in Amazon Inspector
- Accedi ad Amazon Inspector utilizzando un endpoint di interfaccia (AWS PrivateLink

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.
- SSL/TLS Da utilizzare per comunicare con AWS le risorse. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail. Per informazioni sull'utilizzo dei CloudTrail percorsi per acquisire AWS le attività, consulta Lavorare con i CloudTrail percorsi nella Guida per l'AWS CloudTrail utente.
- 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 140-3 per accedere AWS tramite un'interfaccia a riga di comando o un'API, usa un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo 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 altro Servizi AWS utilizzando la console, l'API o. AWS CLI AWS SDKs 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
- Crittografia in transito

Crittografia dei dati a riposo

Per impostazione predefinita, Amazon Inspector archivia i dati inattivi utilizzando soluzioni di AWS crittografia. Amazon Inspector crittografa i dati, come i seguenti:

- Inventario delle risorse raccolto con. AWS Systems Manager
- Inventario delle risorse analizzato dalle immagini di Amazon Elastic Container Registry
- Risultati di sicurezza generati utilizzando chiavi AWS di crittografia di proprietà di AWS Key Management Service

Non è possibile gestire, utilizzare o visualizzare le chiavi AWS di proprietà. Tuttavia, non è necessario agire o modificare i programmi 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 il. AWS KMS APIs Per ulteriori informazioni, vedere Creazione di chiavi di crittografia AWS KMS simmetriche nella guida per l'utente. AWS KMS

> **Note**
>
> A partire dal 13 giugno 2025, il principale servizio nelle AWS KMS richieste registrate CloudTrail durante lo snippet encryption/decryption di codice passerà da «codeguru-reviewer» a «q».

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 AWS servizi. AWS Systems Manager raccoglie i dati di telemetria dalle EC2 istanze di proprietà del cliente a cui vengono inviati AWS tramite un canale protetto da Transport Layer Security (TLS) per la valutazione. I risultati delle scansioni delle funzioni Amazon ECR e AWS Lambda inviati a Security Hub vengono crittografati utilizzando un canale protetto da TLS. Per ulteriori informazioni, vedere Protezione dei dati in Systems Manager per capire come SSM crittografa i dati in transito.

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 sul metodo consigliato per la firma delle richieste, consulta Signature Version 4 AWS per le richieste API nella Guida per l'utente IAM.

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)AWS in IAM nella Guida per l'utente 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. Conserva le credenziali dell'utente root e utilizzale 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 IAM.

Identità federata

Come procedura consigliata, richiedi agli utenti umani, compresi gli utenti che richiedono l'accesso come amministratore, di utilizzare la federazione con un provider di identità per accedere Servizi AWS utilizzando credenziali temporanee.

Un'identità federata è un utente dell'elenco utenti aziendale, di un provider di identità Web AWS Directory Service, della directory Identity Center o di qualsiasi utente che accede utilizzando le Servizi AWS credenziali fornite tramite un'origine di identità. Quando le identità federate accedono Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. Puoi creare utenti e gruppi in IAM Identity Center oppure puoi connetterti e sincronizzarti con un set di utenti e gruppi nella tua fonte di identità per utilizzarli su tutte le tue applicazioni. Account AWS Per ulteriori informazioni su IAM Identity Center, consulta Cos'è IAM Identity Center? 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, se si hanno 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 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, potresti avere un gruppo denominato IAMAdminse concedere a quel 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 Casi d'uso per utenti IAM nella Guida per l'utente 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. Per assumere temporaneamente un ruolo IAM in AWS Management Console, puoi passare da un ruolo utente a un ruolo IAM (console). 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 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 Create a role for a third-party identity provider (federation) nella Guida per l'utente 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 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 Accesso a risorse multi-account in IAM nella Guida per l'utente 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 normale che quel 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 inoltrato (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 Forward access sessions.
- Ruolo di servizio: 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 Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente 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'azione 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' EC2 istanza e che AWS CLI effettuano richieste AWS API. Questa soluzione è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

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 IAM.

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni 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 operazioni 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.

Le policy IAM definiscono le autorizzazioni relative a un'operazione, a prescindere dal metodo utilizzato per eseguirla. Ad esempio, supponiamo di disporre di una policy che consente l'operazione `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 sull'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 ruolo IAM). Tali policy definiscono le operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente 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 IAM.

Policy basate sulle risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Esempi di policy basate sulle 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 utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni 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.

Elenchi di controllo degli accessi () ACLs

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3 e Amazon VPC sono esempi di servizi che supportano. AWS WAF ACLs Per ulteriori informazioni ACLs, consulta la panoramica della lista di controllo degli accessi (ACL) nella Amazon Simple Storage Service Developer Guide.

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 funzionalità 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 IAM.
- Politiche di controllo del servizio (SCPs): SCPs 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 di proprietà dell' Account AWS azienda. Se abiliti tutte le funzionalità di un'organizzazione, puoi applicare le politiche di controllo del servizio (SCPs) a uno o tutti i tuoi account. L'SCP limita le autorizzazioni per le entità presenti negli account dei membri, inclusa ciascuna di esse. Utente root dell'account AWS Per ulteriori informazioni su Organizations and SCPs, consulta le politiche di controllo dei servizi nella Guida AWS Organizations per l'utente.
- Politiche di controllo delle risorse (RCPs): RCPs sono politiche JSON che puoi utilizzare per impostare le autorizzazioni massime disponibili per le risorse nei tuoi account senza aggiornare le politiche IAM allegate a ciascuna risorsa di tua proprietà. L'RCP limita le autorizzazioni per le risorse negli account dei membri e può influire sulle autorizzazioni effettive per le identità, incluse le Utente root dell'account AWS, indipendentemente dal fatto che appartengano o meno all'organizzazione. Per ulteriori informazioni su Organizations e RCPs, incluso un elenco di

Servizi AWS tale supporto RCPs, vedere Resource control policies (RCPs) nella Guida per l'AWS Organizations utente.

- 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 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 o meno una richiesta quando sono coinvolti più tipi di policy, consulta la 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
ACLs	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì

Funzionalità IAM	Supporto per Amazon Inspector
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 operazioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Definizione di autorizzazioni personalizzate IAM con policy gestite dal cliente nella Guida per l'utente 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. Esempi di policy basate sulle 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 utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le operazioni 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 Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Azioni politiche per Amazon Inspector

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy AWS JSON per specificare chi ha accesso a cosa. In altre parole, quale principale può eseguire operazioni 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 operazioni 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. In altre parole, 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'operazione. 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). È possibile eseguire questa operazione per operazioni 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 relativi ARNs, consulta Risorse definite da Amazon Inspector nel Service Authorization Reference. Per sapere con quali azioni è possibile 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. In altre parole, quale principale può eseguire operazioni 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. È possibile 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.

È possibile anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, è possibile 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

ACLs in Amazon Inspector

Supporti ACLs: no

Le liste di controllo degli accessi (ACLs) controllano quali principali (membri dell'account, utenti o ruoli) dispongono delle autorizzazioni per accedere a una risorsa. ACLs sono simili alle politiche basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con Amazon Inspector

Supporta ABAC (tag nelle policy): parzialmente

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 Definizione delle autorizzazioni con autorizzazione ABAC nella Guida per l'utente 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 Passaggio da un ruolo utente a un ruolo IAM (console) nella Guida per l'utente 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 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 Create a role to delegate permissions to an Servizio AWS nella Guida per l'utente 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 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'azione 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 operazioni 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 (console) nella Guida per l'utente IAM.

Per informazioni dettagliate sulle azioni e sui tipi di risorse definiti da Amazon Inspector, incluso il formato di ARNs per ogni 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 AWSo Policy gestite da AWS per le funzioni dei processi nella Guida per l'utente IAM.

- Applica le autorizzazioni con privilegio minimo: quando imposti le autorizzazioni con le policy IAM, concedi solo le autorizzazioni richieste per eseguire un'attività. È possibile 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 IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse è possibile 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 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 il Sistema di analisi degli accessi IAM nella Guida per l'utente 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 Protezione dell'accesso API con MFA nella Guida per l'utente 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 Ti 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_v2

È possibile allegare la policy `AmazonInspector2FullAccess` alle identità IAM.

Questa politica garantisce l'accesso completo ad Amazon Inspector e l'accesso ad altri servizi correlati.

Dettagli dell'autorizzazione

Questa policy include le seguenti autorizzazioni:

- `inspector2`— Consente l'accesso completo ad Amazon Inspector APIs.
- `codeguru-security`— Consente agli amministratori di recuperare i risultati di sicurezza e le impostazioni di configurazione per un account.
- `iam`— Consente ad Amazon Inspector di creare ruoli collegati ai servizi e. `AWSServiceRoleForAmazonInspector2` `AWSServiceRoleForAmazonInspector2Agentless` `AWSServiceRoleForAmazonInspector2`è necessario per consentire ad Amazon Inspector di eseguire operazioni come il recupero di informazioni su istanze Amazon EC2 , repository Amazon ECR e immagini di contenitori Amazon ECR. È inoltre necessario decrittografare gli snapshot di Amazon EBS crittografati con chiavi. AWS KMS Per ulteriori informazioni, consulta Utilizzo di ruoli collegati ai servizi per Amazon Inspector.
- `organizations`— `AllowServicePrincipalBasedAccessToOrganizationApis` consente solo ai responsabili del servizio di creare ruoli collegati ai servizi per Account AWS, registrarne uno Account AWS come amministratore delegato per un'organizzazione ed elencare gli amministratori delegati di un'organizzazione.

`AllowOrganizationalBasedAccessToOrganizationApis`consente al titolare della polizza di recuperare informazioni, in particolare a livello di risorsa, su un'unità organizzativa. ARNs `AllowAccountsBasedAccessToOrganizationApis`consente al titolare della polizza di recuperare informazioni, in particolare a livello di risorsa, su un. ARNs Account AWS`AllowAccessToOrganizationApis`consente al titolare della polizza di visualizzare le informazioni Servizi AWS integrate con un'organizzazione e con l'organizzazione.

```
{
  "Version" : "2012-10-17",
  "Statement" : [
    {
      "Sid" : "AllowFullAccessToInspectorApis",
      "Effect" : "Allow",
      "Action" : "inspector2:*",
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCodeGuruApis",
      "Effect" : "Allow",
      "Action" : [
        "codeguru-security:BatchGetFindings",
        "codeguru-security:GetAccountConfiguration"
      ],
      "Resource" : "*"
    },
    {
      "Sid" : "AllowAccessToCreateSlr",
      "Effect" : "Allow",
      "Action" : "iam:CreateServiceLinkedRole",
      "Resource" : "*",
      "Condition" : {
        "StringEquals" : {
          "iam:AWSServiceName" : [
            "agentless.inspector2.amazonaws.com",
            "inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowServicePrincipalBasedAccessToOrganizationApis",
```

```
      "Effect" : "Allow",
      "Action" : [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource" : "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "inspector2.amazonaws.com",
            "agentless.inspector2.amazonaws.com"
          ]
        }
      }
    },
    {
      "Sid" : "AllowOrganizationalBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeOrganizationalUnit"
      ],
      "Resource" : "arn:*:organizations::*:ou/o-*/ou-*"
    },
    {
      "Sid" : "AllowAccountsBasedAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:DescribeAccount"
      ],
      "Resource" : "arn:*:organizations::*:account/o-*/*"
    },
    {
      "Sid" : "AllowAccessToOrganizationApis",
      "Effect" : "Allow",
      "Action" : [
        "organizations:ListAWSServiceAccessForOrganization",
        "organizations:DescribeOrganization"
      ],
      "Resource" : "*"
    }
  ]
}
```

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 ruoli collegati ai servizi e. `AWSServiceRoleForAmazonInspector2` `AWSServiceRoleForAmazonInspector2Agentless` `AWSServiceRoleForAmazonInspector2`è necessario per consentire ad Amazon Inspector di eseguire operazioni come il recupero di informazioni sulle EC2 istanze Amazon, i repository Amazon ECR e le immagini dei contenitori. È inoltre necessario che Amazon Inspector analizzi la tua rete VPC e descriva gli account associati alla tua organizzazione. `AWSServiceRoleForAmazonInspector2Agentless`è necessario per consentire ad Amazon Inspector di eseguire operazioni, come il recupero di informazioni sulle EC2 istanze Amazon e gli snapshot di Amazon EBS. È inoltre necessario decrittografare gli snapshot di Amazon EBS crittografati con chiavi. AWS KMS 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 Quando attivi l'accesso affidabile per Amazon Inspector in AWS Organizations, 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": [
 {
  "Sid": "AllowFullAccessToInspectorApis",
  "Effect": "Allow",
  "Action": "inspector2:*",
  "Resource": "*"
 },
 {
  "Sid": "AllowAccessToCodeGuruApis",
  "Effect": "Allow",
  "Action": [
   "codeguru-security:BatchGetFindings",
   "codeguru-security:GetAccountConfiguration"
  ],
  "Resource": "*"
 },
 {
  "Sid": "AllowAccessToCreateSlr",
  "Effect": "Allow",
  "Action": "iam:CreateServiceLinkedRole",
  "Resource": "*",
  "Condition": {
   "StringEquals": {
    "iam:AWSServiceName": [
     "agentless.inspector2.amazonaws.com",
     "inspector2.amazonaws.com"
    ]
   }
  }
 },
 {
  "Sid": "AllowAccessToOrganizationApis",
  "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 politica deve essere associata a un ruolo che concede le autorizzazioni alle EC2 istanze Amazon per eseguire scansioni CIS dell'istanza. Puoi utilizzare un ruolo IAM per gestire le credenziali temporanee per le applicazioni in esecuzione su un' EC2 istanza e che effettuano richieste API. AWS CLI AWS Ciò è preferibile alla memorizzazione delle chiavi di accesso all'interno dell' EC2 istanza. Per assegnare un AWS ruolo a un' EC2 istanza e renderlo disponibile per tutte le sue applicazioni, create un profilo di istanza collegato all'istanza. Un profilo di istanza contiene il ruolo e consente ai programmi in esecuzione sull' EC2 istanza di ottenere credenziali temporanee. Per ulteriori informazioni, consulta Utilizzare un ruolo IAM per concedere le autorizzazioni alle applicazioni in esecuzione su EC2 istanze Amazon nella IAM User Guide.

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 FullAccess_v2 — Nuova politica	Amazon Inspector ha aggiunto una nuova policy gestita che fornisce l'accesso completo ad Amazon Inspector e l'accesso ad altri servizi correlati.	3 luglio 2025
AmazonInspector2 ServiceRolePolicy — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto una nuova autorizzazione che consente ad Amazon Inspector di descrivere indirizzi IP e gateway Internet.	29 aprile 2025

Modifica	Descrizione	Data
AmazonInspector2 ServiceRolePolicy — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono l'accesso in sola lettura alle azioni di Amazon ECS e Amazon EKS.	25 marzo 2025
AmazonInspector2 ServiceRolePolicy — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto nuove autorizzazioni che consentono ad Amazon Inspector di restituire i tag di funzione. AWS Lambda	31 luglio 2024
AmazonInspector2 FullAccess — Aggiornamenti a una politica esistente	Amazon Inspector ha aggiunto autorizzazioni che consentono ad Amazon Inspector di creare il ruolo collegato al servizio. `AWSServiceRoleForAmazonInspector2Agentless` Ciò consente agli utenti di eseguire scansioni basate su agenti e scansioni senza agenti quando abilitano Amazon Inspector.	24 aprile 2024
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

Modifica	Descrizione	Data
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 politica relativa ai ruoli collegati ai servizi per consentire la scansione dell'istanza senza agenti. EC2	27 novembre 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 di vulnerability intelligence per rilevare le vulnerabilità dei pacchetti.	22 settembre 2023
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 EC2 istanze Amazon che fanno parte dei gruppi target di Elastic Load Balancing.	31 agosto 2023

Modifica	Descrizione	Data
AmazonInspector2 ReadOnlyAccess — Aggiornamenti a una policy esistente	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
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

Modifica	Descrizione	Data
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
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 Amazon Deep Inspector. EC2	17 aprile 2023

Modifica	Descrizione	Data
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 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

Modifica	Descrizione	Data
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
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

Modifica	Descrizione	Data
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
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

Modifica	Descrizione	Data
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 su altri servizi che supportano ruoli collegati ai servizi, consulta i AWS servizi che funzionano con IAM e cerca i servizi con Sì nella colonna Ruoli collegati ai servizi. Scegli un Sì con un link per consultare la documentazione relativa ai ruoli collegati ai servizi per quel servizio.

Autorizzazioni di ruolo collegate ai servizi per Amazon Inspector

Amazon Inspector utilizza la policy gestita denominata. `AWSServiceRoleForAmazonInspector2` Questo ruolo collegato al servizio si fida che il `inspector2.amazonaws.com` servizio assuma il 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 EC2 istanze Amazon 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 policy IAM che potrebbero creare vulnerabilità di sicurezza nel 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 l'autorizzazione a 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 azioni selezionate di Elastic Load Balancing per eseguire scansioni di rete delle EC2 istanze che fanno parte dei gruppi target di Elastic Load Balancing.
- Utilizza le azioni Amazon ECS e Amazon EKS per consentire l'accesso in sola lettura per visualizzare cluster e attività e descrivere le attività.

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:DescribeAddresses",
   "ec2:DescribeAvailabilityZones",
   "ec2:DescribeCustomerGateways",
   "ec2:DescribeEgressOnlyInternetGateways",
   "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",
     "lambda:ListTags",
     "cloudwatch:GetMetricData"
    ],
    "Resource": "*"
   },
   {
    "Sid": "GatherInventory",
    "Effect": "Allow",
    "Action": [
     "ssm:CreateAssociation",
     "ssm:StartAssociationsOnce",
     "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": "GatherInventoryDeleteAssociation",
   "Effect": "Allow",
   "Action": [
    "ssm:DeleteAssociation"
   ],
   "Resource": [
    "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"
      }
     }
    },
    {
     "Sid": "AllowListAccessToECSAndEKS",
     "Effect": "Allow",
```

```
    "Action": [
        "ecs:ListClusters",
        "ecs:ListTasks",
        "eks:ListClusters"
    ],
    "Resource": [
        "*"
    ],
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
        }
    }
    },
    {
    "Sid": "AllowAccessToECSTasks",
    "Effect": "Allow",
    "Action": [
        "ecs:DescribeTasks"
    ],
    "Resource": "arn:aws:ecs:*:*:task/*",
    "Condition": {
        "StringEquals": {
            "aws:ResourceAccount": "${aws:PrincipalAccount}"
     }
    }
   }
  ]
}
```

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 EC2 qualsiasi istanza 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 su EC2 istanze, volumi e istantanee.
  - Usa le azioni di EC2 tagging di Amazon per etichettare gli snapshot per le scansioni con la `InspectorScan` chiave tag.
  - Utilizza le azioni Amazon EC2 Snapshot per creare istantanee, etichettarle con la chiave `InspectorScan` tag e quindi eliminare istantanee di volumi Amazon EBS a cui è stata assegnata la 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 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 servizio 2Agentless. AWSService RoleForAmazonInspector 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 i servizi che supportano politiche basate sulle risorse o liste di controllo degli accessi (ACLs), puoi utilizzare tali politiche per consentire alle persone di accedere 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 IAM.
- Per informazioni sulle differenze di utilizzo tra ruoli e policy basate su risorse per l'accesso multi-account, consulta Accesso a risorse multi-account in IAM nella Guida per l'utente IAM.

Monitoraggio di Amazon Inspector

Il monitoraggio è una parte importante per mantenere la disponibilità, l'affidabilità e le prestazioni di Amazon Inspector e di altre AWS soluzioni. AWS fornisce strumenti per monitorare Amazon Inspector, segnalare i problemi che si verificano e intraprendere azioni per porvi rimedio:

- Amazon EventBridge è un AWS servizio che utilizza gli eventi per connettere tra loro i componenti delle applicazioni, semplificando la creazione di applicazioni scalabili basate sugli eventi. EventBridge offre un flusso di dati in tempo reale dalle applicazioni, dalle applicazioni Software-as-a-Service (SaaS), dai AWS servizi e dai percorsi, in modo da poter monitorare gli eventi che si verificano nei servizi e creare architetture basate sugli eventi.
- AWS CloudTrailè un AWS servizio che acquisisce le chiamate API e gli eventi correlati effettuati da o per conto dell'utente. Account AWS CloudTrail invia i file di log a un bucket Amazon S3 da te specificato, in modo da poter identificare quali utenti e account hanno chiamato AWS, l'indirizzo IP di origine da cui sono state effettuate le chiamate e quando sono avvenute le chiamate.

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 trail, è comunque possibile visualizzare gli eventi più recenti nella console di CloudTrail in Event history (Cronologia 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 alle operazioni `CreateFindingsReport`, `ListCoverage` e `UpdateOrganizationConfiguration` generano voci nei file di log 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, consulta 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 informazioni sull'azione richiesta, la data e l'ora dell'azione, i parametri della richiesta e così via. CloudTrail i file di registro non sono una traccia ordinata dello stack delle chiamate API pubbliche, quindi non vengono visualizzati in un ordine specifico.

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 specifici programmi di conformità, consulta Servizi AWS la sezione Scope by Compliance Program Servizi AWS 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:

- Governance e conformità per la sicurezza: queste guide all'implementazione di soluzioni illustrano considerazioni relative all'architettura e i passaggi per implementare le funzionalità di sicurezza e conformità.
- Riferimenti sui servizi conformi ai requisiti HIPAA: elenca i servizi HIPAA idonei. Non tutti Servizi AWS sono idonei alla normativa 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)).
- Evaluating Resources with Rules nella AWS Config Developer Guide: 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.

- Amazon GuardDuty: Servizio AWS rileva potenziali minacce ai tuoi carichi di lavoro Account AWS, ai contenitori e ai dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty può aiutarti a soddisfare vari requisiti di conformità, come lo standard PCI DSS, soddisfacendo i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità.
- AWS Audit Manager— Ciò Servizio AWS consente di verificare continuamente l' AWS utilizzo per semplificare la gestione del rischio 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 zone di disponibilità multiple, fisicamente separate e isolate, collegate a 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 indicato nel modello di responsabilitàAWS condivisa alla voce «Security of the Cloud», AWS è responsabile della protezione dell'infrastruttura che gestisce tutti i servizi nel AWS cloud. AWS è inoltre responsabile di qualsiasi risposta agli incidenti associata al servizio Amazon Inspector.

In qualità di AWS cliente, condividi la responsabilità di mantenere la sicurezza nel AWS cloud. Ciò significa che sei tu a controllare la sicurezza che scegli di implementare, che include tutti AWS gli strumenti e le funzionalità a cui accedi. Significa anche che sei responsabile della risposta agli incidenti dalla tua parte del modello di responsabilità condivisa.

Stabilendo una linea di base di sicurezza che soddisfi tutti gli obiettivi delle applicazioni eseguite nel AWS cloud, puoi rilevare le deviazioni a cui puoi rispondere. Poiché la risposta agli incidenti è un argomento complesso, consulta le seguenti risorse per comprendere meglio l'impatto della risposta agli incidenti e come le tue scelte potrebbero influenzare gli obiettivi aziendali: AWS Security Incident Response Guide,AWS Security Best Practices e AWS Cloud Adoption Framework: Security Perspective.

Accedi ad Amazon Inspector utilizzando un endpoint di interfaccia (AWS PrivateLink

Puoi utilizzarlo AWS PrivateLink per creare una connessione privata tra il tuo VPC e Amazon Inspector. Puoi accedere ad Amazon Inspector come se fosse nel tuo VPC, senza l'uso di un gateway Internet, un dispositivo NAT, una connessione VPN o una connessione. AWS Direct Connect Le istanze nel tuo VPC non necessitano di indirizzi IP pubblici per accedere ad Amazon Inspector.

Stabilisci questa connessione privata creando un endpoint di interfaccia attivato da AWS PrivateLink. In ciascuna sottorete viene creata un'interfaccia di rete endpoint da abilitare per l'endpoint di interfaccia. Si tratta di interfacce di rete gestite dai richiedenti che fungono da punto di ingresso per il traffico destinato ad Amazon Inspector.

Per ulteriori informazioni, consulta Access Servizi AWS through nella Guida. AWS PrivateLinkAWS PrivateLink

Considerazioni per Amazon Inspector

Prima di configurare un endpoint di interfaccia per Amazon Inspector, consulta le considerazioni nella Guida.AWS PrivateLink

Amazon Inspector supporta l'esecuzione di chiamate a tutte le sue azioni API tramite l'endpoint dell'interfaccia.

Le policy degli endpoint VPC non sono supportate per Amazon Inspector. Per impostazione predefinita, l'accesso completo ad Amazon Inspector è consentito tramite l'endpoint dell'interfaccia. In alternativa, puoi associare un gruppo di sicurezza alle interfacce di rete degli endpoint per controllare il traffico verso Amazon Inspector attraverso l'endpoint dell'interfaccia.

Crea un endpoint di interfaccia per Amazon Inspector

Puoi creare un endpoint di interfaccia per Amazon Inspector utilizzando la console Amazon VPC o (). AWS Command Line Interface AWS CLI Per ulteriori informazioni, consulta la sezione Creazione di un endpoint di interfaccia nella Guida per l'utente di AWS PrivateLink .

Quando crei un endpoint di interfaccia per Amazon Inspector, utilizza uno dei seguenti nomi di servizio:

```
com.amazonaws.region.inspector2
```

```
com.amazonaws.region.inspector-scan
```

Sostituiscilo *region* con il Regione AWS codice applicabile. Regione AWS

Se abiliti il DNS privato per l'endpoint dell'interfaccia, puoi effettuare richieste API ad Amazon Inspector utilizzando il nome DNS regionale predefinito, ad esempio`service-name.us-east-1.amazonaws.com` , `service-name.us-east-1.api.aws.com` o per gli Stati Uniti orientali (Virginia settentrionale).

Integrazioni con Amazon Inspector

Amazon Inspector si integra con altri servizi. AWS Questi servizi possono importare dati da Amazon Inspector, quindi puoi visualizzare i risultati in diversi modi. Consulta le seguenti opzioni di integrazione per saperne di più.

Integrazione di Amazon Inspector con Amazon ECR

Amazon Elastic Container Registry (Amazon ECR) è AWS un registro di immagini di container gestito che supporta registri privati. I registri privati di Amazon ECR ospitano immagini di container in un'architettura altamente disponibile e scalabile. Puoi usare Amazon Inspector per scansionare le immagini dei container che risiedono nel tuo repository Amazon ECR alla ricerca di pacchetti di sistemi operativi e pacchetti di linguaggi di programmazione vulnerabili. Per ulteriori informazioni, consulta Integrazione di Amazon Inspector con Amazon Elastic Container Registry (Amazon ECR).

Integrazione di Amazon Inspector con AWS Security Hub

AWS Security Hubfornisce una visione completa dello stato di sicurezza AWS e ti aiuta a controllare il tuo ambiente rispetto agli standard e alle migliori pratiche del settore della sicurezza Security Hub raccoglie dati di sicurezza da AWS account, servizi e prodotti supportati. Puoi utilizzare Security Hub per importare i dati dei risultati di Amazon Inspector e creare una posizione centrale per i risultati in tutti i tuoi servizi AWS integrati AWS e prodotti Partner Network. Per ulteriori informazioni, consulta Integrazione di Amazon Inspector con AWS Security Hub.

Integrazione di Amazon Inspector con Amazon Elastic Container Registry (Amazon ECR)

Amazon Elastic Container Registry è un registro di container completamente gestito che supporta immagini e AWS artefatti Docker e OCI. Se usi Amazon ECR, puoi attivare Enhanced Scanning per il registro dei container. Quando attivi la scansione avanzata, Amazon Inspector rileva e scansiona automaticamente le immagini dei container alla ricerca di pacchetti di sistemi operativi e linguaggi di programmazione vulnerabili. Questa integrazione consente di visualizzare i risultati di Amazon Inspector per le immagini dei container e di gestire la frequenza e l'ambito delle scansioni nella console Amazon ECR. Per ulteriori informazioni, consulta Scansione delle immagini dei container Amazon ECR con Amazon Inspector.

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. Tipi di scansione automatizzati in 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 in AWS. Questo ti aiuta a controllare il tuo ambiente rispetto agli standard e alle migliori pratiche del settore della sicurezza. Security Hub raccoglie dati di sicurezza da AWS account, servizi e prodotti supportati. È possibile utilizzare queste informazioni per analizzare le tendenze di sicurezza e identificare i problemi di sicurezza. Quando attivi l'integrazione di Amazon Inspector con Security Hub, Amazon Inspector può inviare i risultati a Security Hub e Security Hub può analizzarli come parte del tuo livello di sicurezza.

Centrale di sicurezza monitora i problemi di sicurezza sotto forma di risultati. Alcuni risultati possono essere il risultato di problemi di sicurezza rilevati in altri AWS servizi o prodotti di terze parti. Security Hub utilizza una serie di regole per rilevare problemi di sicurezza e generare risultati e fornisce strumenti per gestirli. Security Hub archivia i risultati di Amazon Inspector una volta che i risultati sono stati chiusi in Amazon Inspector. Puoi anche visualizzare una cronologia dei risultati e dei dettagli delle scoperte, nonché monitorare lo stato di un'indagine su un risultato.

Security Hub elabora i risultati nel AWS Security Finding Format (ASFF). Questo formato include dettagli quali identificatori univoci, livelli di gravità, risorse interessate, indicazioni sulla correzione, stato del flusso di lavoro e informazioni contestuali.

> **Note**
>
> I risultati di sicurezza generati da Amazon Inspector Code Security non sono disponibili per questa integrazione. Tuttavia, puoi accedere a questi risultati particolari nella console Amazon Inspector e tramite l'API Amazon Inspector.

Argomenti

- Visualizzazione dei risultati di Amazon Inspector in AWS Security Hub
- Attivazione e configurazione dell'integrazione di Amazon Inspector con Security Hub
- Disattivazione del flusso di risultati da un'integrazione
- Visualizzazione dei controlli di sicurezza per Amazon Inspector in Security Hub

Visualizzazione dei risultati di Amazon Inspector in AWS Security Hub

Puoi visualizzare i risultati di Amazon Inspector Classic e Amazon Inspector in Security Hub.

> **Note**
>
> Per filtrare solo in base ai risultati di Amazon Inspector, aggiungili `"aws/inspector/ProductVersion": "2"` alla barra dei filtri. 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 di Amazon Inspector con Security Hub

Puoi attivare l'integrazione con Amazon Inspector AWS Security Hub abilitando Security Hub. Dopo aver abilitato Security Hub, l'integrazione con Amazon Inspector AWS Security Hub viene attivata automaticamente e Amazon Inspector inizia a inviare tutti i risultati a Security Hub utilizzando AWS il Security Finding Format (ASFF).

Disattivazione del flusso di risultati da un'integrazione

Per impedire ad Amazon Inspector di inviare i risultati a Security Hub, puoi utilizzare la console o l'API di Security Hub e.. AWS CLI

Visualizzazione dei controlli di sicurezza per Amazon Inspector in Security Hub

Security Hub analizza i risultati dei prodotti supportati AWS e di terze parti ed esegue controlli di sicurezza automatici e continui rispetto alle regole per generare risultati propri. Le regole sono rappresentate dai controlli di sicurezza, che aiutano a determinare se i requisiti di uno standard vengono soddisfatti.

Amazon Inspector utilizza controlli di sicurezza per verificare se le funzionalità di Amazon Inspector sono o devono essere abilitate. Le caratteristiche principali comprendono:

- EC2 Scansione Amazon
- Scansione Amazon ECR
- Scansione standard Lambda
- Scansione del codice Lambda

Per ulteriori informazioni, consulta i controlli di Amazon Inspector nella Guida per l'AWS Security Hub utente.

Sistemi operativi e linguaggi di programmazione supportati per Amazon Inspector

Amazon Inspector è in grado di scansionare le applicazioni software installate nei seguenti sistemi:

- Istanze Amazon Elastic Compute Cloud (Amazon EC2)

> **Note**
>
> Per EC2 le istanze Amazon, Amazon Inspector può eseguire la scansione alla ricerca di vulnerabilità dei pacchetti nei sistemi operativi che supportano la scansione basata su agenti. Amazon Inspector può anche scansionare le vulnerabilità dei pacchetti nei sistemi operativi e nei linguaggi di programmazione che supportano la scansione ibrida. Amazon Inspector non esegue la scansione delle vulnerabilità della toolchain. La versione del compilatore del linguaggio di programmazione utilizzata per creare l'applicazione introduce queste vulnerabilità.

- Immagini dei container archiviate nei repository Amazon Elastic Container Registry (Amazon ECR)

> **Note**
>
> 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. Amazon Inspector non esegue la scansione delle vulnerabilità della toolchain in. Rust La versione del compilatore del linguaggio di programmazione utilizzata per creare l'applicazione introduce queste vulnerabilità.

- AWS Lambda funzioni

> **Note**
>
> Per le funzioni Lambda, Amazon Inspector è in grado di rilevare le vulnerabilità dei pacchetti del linguaggio di programmazione e delle vulnerabilità del codice. Amazon Inspector non esegue la scansione delle vulnerabilità della toolchain. La versione del compilatore del linguaggio di programmazione utilizzata per creare l'applicazione introduce queste vulnerabilità.

Quando Amazon Inspector analizza le risorse, Amazon Inspector recupera più di 50 feed di dati per generare risultati su vulnerabilità ed esposizioni comuni (). CVEs Esempi di queste fonti includono avvisi di sicurezza dei fornitori, feed di dati e feed di intelligence sulle minacce, nonché il National Vulnerability Database (NVD) e MITRE. Amazon Inspector aggiorna i dati sulle vulnerabilità dai feed di origine almeno una volta al giorno.

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 linguaggi di programmazione e i runtime supportati da Amazon Inspector per diverse risorse e tipi di scansione. Sono inoltre elencati i sistemi operativi fuori produzione.

> **Note**
>
> 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
- Sistemi operativi fuori produzione
- Linguaggi di programmazione compatibili
- Runtime supportati

Sistemi operativi supportati

Questa sezione elenca i sistemi operativi supportati da Amazon Inspector.

Sistemi operativi supportati: Amazon EC2 scanning

La tabella seguente elenca i sistemi operativi supportati da Amazon Inspector per la scansione delle istanze Amazon EC2 . Specifica l'avviso di sicurezza del fornitore per ciascun sistema operativo e quali sistemi operativi supportano la scansione basata su agenti e la scansione senza agenti.

Quando si utilizza il metodo di scansione basato su agenti, si configura l'agente SSM per eseguire scansioni continue su tutte le istanze idonee. Amazon Inspector consiglia di configurare una versione

dell'agente SSM successiva alla 3.2.2086.0. Per ulteriori informazioni, consulta Working with the SSM Agent nella Amazon EC2 Systems Manager User Guide.

I rilevamenti del sistema operativo Linux sono supportati solo per l'archivio predefinito del gestore di pacchetti (rpm e dpkg) e non includono applicazioni di terze parti, repository di supporto esteso (RHEL EUS, E4S, AUS e TUS) e repository opzionali (flussi di applicazioni). Amazon Inspector analizza il kernel in esecuzione alla ricerca di vulnerabilità. Per alcuni sistemi operativi, ad esempioUbuntu, è necessario un riavvio affinché gli aggiornamenti vengano visualizzati nei risultati attivi.

Sistema operativo	Versione	Avvisi sulla 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
Server Debian (Bullseye)	11	DSA	Sì	Sì
Server Debian (Bookworm)	12	DSA	Sì	Sì
Fedora	41	CVE	Sì	Sì
Fedora	42	CVE	Sì	Sì
openSUSE Leap	15.6	CVE	Sì	Sì

Sistema operativo	Versione	Avvisi sulla sicurezza dei fornitori	Supporto per la scansione senza agente	Supporto per la scansione basato su agenti
Oracle Linux (Oracle)	8	ELSA	Sì	Sì
Oracle Linux (Oracle)	9	ELSA	Sì	Sì
Red Hat Enterprise Linux (RHEL)	8	RISSA	Sì	Sì
Red Hat Enterprise Linux (RHEL)	9	RHSA	Sì	Sì
Rocky Linux	8	RLSA	Sì	Sì
Rocky Linux	9	RLSA	Sì	Sì
SUSE Linux Enterprise Server (SLES)	15.6	CAVERNA SUUSA	Sì	Sì
Ubuntu (Xenial)	16.04	USN, Ubuntu Pro (esm-infra e esm-apps)	Sì	Sì
Ubuntu (Bionico)	18.04	USN, Ubuntu Pro (esm-infra e esm-apps)	Sì	Sì
Ubuntu (focale)	20.04	USN, Ubuntu Pro (esm-infra e esm-apps)	Sì	Sì

Sistema operativo	Versione	Avvisi sulla sicurezza dei fornitori	Supporto per la scansione senza agente	Supporto per la scansione basato su agenti
Ubuntu (Jammy)	22.04	USN, Ubuntu Pro (esm-infra e esm-apps)	Sì	Sì
Ubuntu (Noble Numbat)	24.04	USN, Ubuntu Pro (esm-infra & esm-apps)	Sì	Sì
Ubuntu (Oracular Oriole)	24.10	USN	Sì	Sì
Ubuntu (Plucky Puffin)	25.04	USN	Sì	Sì
Windows Server	2016	MSKB	No	Sì
Windows Server	2019	MSKB	No	Sì
Windows Server	2022	MSKB	No	Sì
Windows Server	2025	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

Sistema operativo	Versione	Avvisi sulla sicurezza dei fornitori	Supporto per la scansione senza agente	Supporto per la scansione basato su agenti
macOS (Sonoma)	14	APPLE-SV	No	Sì

Sistemi operativi supportati: scansione Amazon ECR con Amazon Inspector

La tabella seguente elenca i sistemi operativi supportati da Amazon Inspector per la scansione delle immagini dei container nei repository Amazon ECR. Inoltre, specifica l'avviso di sicurezza del fornitore per ciascun sistema operativo.

Sistema operativo	Versione	Avvisi di sicurezza del fornitore
Alpine Linux (Alpine)	3.19	Alpine SecDB
Alpine Linux (Alpine)	3.20	Alpine SecDB
Alpine Linux (Alpine)	3.21	Alpine SecDB
Alpine Linux (Alpine)	3.22	Alpine SecDB
AlmaLinux	8	ALSA
AlmaLinux	9	ALSA
Amazon Linux (AL2)	AL2	ALAS
Amazon Linux 2023 (AL2023)	AL2023	ALAS
BusyBox	—	—
Chainguard	–	CVE
Debian Server (Bullseye)	11	DSA
Debian Server (Bookworm)	12	DSA

Sistema operativo	Versione	Avvisi di sicurezza del fornitore
Fedora	41	CVE
Fedora	42	CVE
openSUSE Leap	15.6	CVE
Oracle Linux (Oracle)	8	ELSA
Oracle Linux (Oracle)	9	ELSA
Photon OS	4	PHSA
Photon OS	5	PHSA
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)	15.6	SUSE CVE
Ubuntu (Xenial)	16.04	USN, Ubuntu Pro (esm-infra & esm-apps)
Ubuntu (Bionic)	18.04	USN, Ubuntu Pro (esm-infra & esm-apps)
Ubuntu (Focal)	20.04	USN, Ubuntu Pro (esm-infra & esm-apps)
Ubuntu (Jammy)	22.04	USN, Ubuntu Pro (esm-infra & esm-apps)

Sistema operativo	Versione	Avvisi di sicurezza del fornitore
Ubuntu (Noble Numbat)	24.04	USN, Ubuntu Pro (esm-infra & esm-apps)
Ubuntu (Oracular Oriole)	24.10	USN
Ubuntu (Plucky Puffin)	25.04	USN
Wolfi	–	CVE

Sistemi operativi supportati: scansione CIS

La tabella seguente elenca i sistemi operativi supportati da Amazon Inspector per le scansioni CIS. Inoltre, specifica la versione del benchmark CIS per ogni sistema operativo.

> **Note**
>
> Gli standard CIS sono destinati ai sistemi operativi x86_64. Alcuni controlli potrebbero non essere valutati o restituire istruzioni di riparazione non valide su risorse basate su ARM.

Sistema operativo	Versione	Versione benchmark CIS
Amazon Linux 2	AL2	3.0.0
Amazon Linux 2023	AL2023	1.0.0
Red Hat Enterprise Linux (RHEL)	8	3.0.0
Red Hat Enterprise Linux (RHEL)	9	2.0.0
Rocky Linux	8	2.0.0
Rocky Linux	9	1.0.0

Sistema operativo	Versione	Versione benchmark CIS
SUSE Linux Enterprise Server	15	2.0.1
Ubuntu (Bonic)	18.04	2.1.0
Ubuntu (focale)	20.04	2.0.1
Ubuntu (Jammy)	22.04	1.0.0
Ubuntu (Noble Numbat)	24.04	1.0.0
Windows Server	2016	3.0.0
Windows Server	2019	2.0.0
Windows Server	2022	2.0.0

Sistemi operativi fuori produzione

Nelle tabelle seguenti sono elencati quali sistemi operativi sono stati interrotti e quando sono stati interrotti.

Anche se Amazon Inspector non fornisce il supporto completo per i seguenti sistemi operativi fuori produzione, Amazon Inspector continua a scansionare le istanze Amazon EC2 e le immagini dei container Amazon ECR su cui sono eseguite. Come best practice di sicurezza, consigliamo di passare alla versione supportata di un sistema operativo fuori produzione. I risultati generati da Amazon Inspector per un sistema operativo fuori produzione devono essere utilizzati solo a scopo informativo.

In conformità alla politica del fornitore, i seguenti sistemi operativi non ricevono più gli aggiornamenti delle patch. È possibile che non vengano rilasciati nuovi avvisi di sicurezza per i sistemi operativi fuori produzione. I fornitori possono rimuovere gli avvisi e i rilevamenti di sicurezza esistenti dai propri feed per i sistemi operativi che raggiungono la fine del supporto standard. Di conseguenza, Amazon Inspector può smettere di generare risultati per noti. CVEs

Sistemi operativi fuori produzione: Amazon scanning EC2

Sistema operativo	Versione	Discontinuo
Amazon Linux (AL1)	2012	31 dicembre 2021
CentOS Linux (CentOS)	7	30 giugno 2024
CentOS Linux (CentOS)	8	31 dicembre 2021
Server Debian (Jessie)	8	30 giugno 2020
Server Debian (Stretch)	9	30 giugno 2022
Server Debian (Buster)	10	30 giugno 2024
Fedora	33	30 novembre 2021
Fedora	34	7 luglio 2022
Fedora	35	13 dicembre 2022
Fedora	36	16 maggio 2023
Fedora	37	15 dicembre 2023
Fedora	38	21 maggio 2024
Fedora	39	26 novembre 2024
Fedora	40	13 maggio 2025
openSUSE Leap	15.2	1° dicembre 2021
OpenSUSE Leap	15.3	1 dicembre 2022
openSUSE Leap	15.4	7 dicembre 2023
OpenSUSE Leap	15.5	December 31, 2024
Oracle Linux (Oracle)	6	1 marzo 2021
Oracle Linux (Oracle)	7	31 dicembre 2024

Sistema operativo	Versione	Discontinuo
Red Hat Enterprise Linux (RHEL)	6	30 novembre 2020
Red Hat Enterprise Linux (RHEL)	7	30 giugno 2024
SUSE Linux Enterprise Server (SLES)	12	30 giugno 2016
SUSE Linux Enterprise Server (SLES)	12.1	31 maggio 2017
SUSE Linux Enterprise Server (SLES)	12.2	31 marzo 2018
SUSE Linux Enterprise Server (SLES)	12.3	30 giugno 2019
SUSE Linux Enterprise Server (SLES)	12.4	30 giugno 2020
SUSE Linux Enterprise Server (SLES)	12,5	31 ottobre 2024
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
SUSE Linux Enterprise Server (SLES)	15.3	31 dicembre 2022
SUSE Linux Enterprise Server (SLES)	15,4	31 dicembre 2023

Sistema operativo	Versione	Discontinuo
SUSE Linux Enterprise Server (SLES)	15,5	31 dicembre 2024
Ubuntu (affidabile)	12.04	28 aprile 2017
Ubuntu (affidabile)	14.04	1 aprile 2024
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
Ubuntu (Minotauro Mantico)	23.10	11 luglio 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)	3.2	1 maggio 2017
Linux Alpine (Alpine)	3.3	1° novembre 2017
Linux Alpine (Alpine)	3.4	1 maggio 2018
Linux Alpine (Alpine)	3.5	1° novembre 2018
Linux Alpine (Alpine)	3.6	1 maggio 2019
Linux Alpine (Alpine)	3.7	1° novembre 2019

Sistema operativo	Versione	Discontinuo
Linux Alpine (Alpine)	3.8	1 maggio 2020
Linux Alpine (Alpine)	3.9	1 novembre 2020
Linux Alpine (Alpine)	3.10	1 maggio 2021
Alpine Linux (Alpine)	3.11	1° novembre 2021
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
Alpine Linux (Alpine)	3.16	May 23, 2024
Alpine Linux (Alpine)	3.17	November 22, 2024
Alpine Linux (Alpine)	3.18	May 09 2025
Amazon Linux (AL1)	2012	31 dicembre 2021
CentOS Linux (CentOS)	7	30 giugno 2024
CentOS Linux (CentOS)	8	31 dicembre 2021
Server Debian (Jessie)	8	30 giugno 2020
Server Debian (Stretch)	9	30 giugno 2022
Server Debian (Buster)	10	30 giugno 2024
Fedora	33	30 novembre 2021
Fedora	34	7 luglio 2022
Fedora	35	13 dicembre 2022

Sistema operativo	Versione	Discontinuo
Fedora	36	16 maggio 2023
Fedora	37	15 dicembre 2023
Fedora	38	21 maggio 2024
Fedora	39	26 novembre 2024
Fedora	40	13 maggio 2025
openSUSE Leap	15.2	1° dicembre 2021
OpenSUSE Leap	15.3	1 dicembre 2022
OpenSUSE Leap	15.4	December 7, 2023
OpenSUSE Leap	15.5	December 31, 2024
Oracle Linux (Oracle)	6	1 marzo 2021
Oracle Linux (Oracle)	7	31 dicembre 2024
Photon OS	2	2 dicembre 2021
Photon OS	3	1 marzo 2024
Red Hat Enterprise Linux (RHEL)	6	30 giugno 2020
Red Hat Enterprise Linux (RHEL)	7	30 giugno 2024
SUSE Linux Enterprise Server (SLES)	12	30 giugno 2016
SUSE Linux Enterprise Server (SLES)	12.1	31 maggio 2017

Sistema operativo	Versione	Discontinuo
SUSE Linux Enterprise Server (SLES)	12.2	31 marzo 2018
SUSE Linux Enterprise Server (SLES)	12.3	30 giugno 2019
SUSE Linux Enterprise Server (SLES)	12.4	30 giugno 2020
SUSE Linux Enterprise Server (SLES)	12,5	31 ottobre 2024
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
SUSE Linux Enterprise Server (SLES)	15.3	31 dicembre 2022
SUSE Linux Enterprise Server (SLES)	15,4	31 dicembre 2023
SUSE Linux Enterprise Server (SLES)	15,5	31 dicembre 2024
Ubuntu (affidabile)	12.04	28 aprile 2017
Ubuntu (affidabile)	14.04	1 aprile 2024
Ubuntu (Groovy)	20.10	22 luglio 2021
Ubuntu (Hirsute)	21.04	20 gennaio 2022

Sistema operativo	Versione	Discontinuo
Ubuntu (Impish)	21.10	31 luglio 2022
Ubuntu (Kinetic)	22.10	July 20, 2023
Ubuntu (Lunar Lobster)	23.04	January 25, 2024
Ubuntu (Minotauro Mantico)	23.10	11 luglio 2024

Linguaggi di programmazione compatibili

Questa sezione elenca i linguaggi di programmazione supportati da Amazon Inspector.

Linguaggi di programmazione supportati: Amazon EC2 agentless scanning

Amazon Inspector attualmente supporta i seguenti linguaggi di programmazione per l'esecuzione di scansioni senza agente su istanze Amazon idonee. EC2 Per ulteriori informazioni, consulta la sezione Scansione senza agente.

> **Note**
>
> Amazon Inspector non esegue la scansione delle vulnerabilità della toolchain in and. Go Rust La versione del compilatore del linguaggio di programmazione utilizzata per creare l'applicazione introduce queste vulnerabilità.

- C#
- Go
- Java
- JavaScript
- PHP
- Python
- Ruby
- Rust

Linguaggi di programmazione supportati: Amazon EC2 deep inspection

Amazon Inspector attualmente supporta i seguenti linguaggi di programmazione per l'esecuzione di scansioni di ispezione approfondita su istanze Amazon EC2 Linux. Per ulteriori informazioni, consulta Amazon Inspector deep inspection per istanze Amazon basate su Linux. EC2

- Java(formati di archivio.ear, .jar, .par e.war)
- JavaScript
- Python

Amazon Inspector utilizza Systems Manager Distributor per distribuire il plug-in per l'ispezione approfondita dell'istanza Amazon. EC2

> **Note**
>
> L'ispezione approfondita non è supportata per i sistemi operativi Bottlerocket.

Per eseguire scansioni di ispezione approfondita, Systems Manager Distributor e Amazon Inspector devono supportare il sistema operativo delle istanze EC2 Amazon. Per informazioni sui sistemi operativi supportati in Systems Manager Distributor, vedere Piattaforme e architetture di pacchetti supportate nella Guida per l'utente di Systems Manager.

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:

> **Note**
>
> Amazon Inspector non esegue la scansione delle vulnerabilità della toolchain in. Rust La versione del compilatore del linguaggio di programmazione utilizzata per creare l'applicazione introduce queste vulnerabilità.

- C#
- Go
- Gotoolchain

- Java
- JavaJDK
- JavaScript
- PHP
- Python
- Ruby
- Rust

Runtime supportati

Questa sezione elenca i runtime supportati da Amazon Inspector.

Runtime supportati: scansione standard di Amazon Inspector Lambda

La scansione standard di Amazon Inspector Lambda attualmente supporta i seguenti runtime per i linguaggi di programmazione che può utilizzare per la scansione delle funzioni Lambda alla ricerca di vulnerabilità nei pacchetti software di terze parti:

> **Note**
>
> Amazon Inspector non esegue la scansione delle vulnerabilità della toolchain in. Rust La versione del compilatore del linguaggio di programmazione utilizzata per creare l'applicazione introduce queste vulnerabilità.

- Go
  - go1.x
- Java
  - java8
  - java8.al2
  - java11
  - java17
  - java21
- .NET

  - .NET 6
  - .NET 8
- Node.js
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
  - nodejs22.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
  - python3.12
  - python3.13
- Ruby
  - ruby2.7
  - ruby3.2
  - ruby3.3
- Custom runtimes
  - AL2
  - AL2023

Runtime supportati: scansione del codice Amazon Inspector Lambda

La scansione del codice Amazon Inspector Lambda attualmente supporta i seguenti runtime per i linguaggi di programmazione che può utilizzare durante la scansione delle funzioni Lambda alla ricerca di vulnerabilità nel codice:

- Java

  - java8
  - java8.al2
  - java11
  - java17
- .NET
  - .NET 6
  - .NET 8
- Node.js
  - nodejs12.x
  - nodejs14.x
  - nodejs16.x
  - nodejs18.x
  - nodejs20.x
- Python
  - python3.7
  - python3.8
  - python3.9
  - python3.10
  - python3.11
  - python3.12
- Ruby
  - ruby2.7
  - ruby3.2
  - ruby3.3

Disattivazione di Amazon Inspector

Puoi disattivare Amazon Inspector nella console Amazon Inspector o con l'API Amazon Inspector. Se disattivi tutti i tipi di scansione per un account, Amazon Inspector viene disattivato automaticamente per quell'account.

Se disattivi Amazon Inspector per un account, tutti i tipi di scansione vengono disattivati per quell'account. Inoltre, tutte le impostazioni di scansione di Amazon Inspector, inclusi filtri, regole di soppressione e risultati, vengono eliminate per l'account.

Quando disattivi Amazon Inspector Amazon Scan, EC2 Amazon Inspector elimina le seguenti associazioni SSM:

- `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 Windows ospita. Per ulteriori informazioni, consulta Istanza di scansione Windows EC2 .

> **Note**
>
> Una volta disattivato Amazon Inspector, non dovrai più sostenere costi di servizio. Tuttavia, puoi riattivare Amazon Inspector in qualsiasi momento.

Per informazioni su come disattivare i tipi di scansione per diverse risorse, consulta Disattivazione di un tipo di scansione.

Prerequisiti

A seconda del tipo di account, considera quanto segue:

- Se il tuo account è un account Amazon Inspector autonomo, puoi disattivare Amazon Inspector in qualsiasi momento.
- Se il tuo account è un account membro in un ambiente con più account, non puoi disattivare Amazon Inspector. Devi contattare l'amministratore delegato della tua organizzazione per disattivare Amazon Inspector.

- Se sei l'amministratore delegato di un'organizzazione, devi dissociare tutti i tuoi account membro prima di disattivare Amazon Inspector.

> **Note**
>
> Quando disattivi Amazon Inspector come amministratore delegato, disattivi la funzionalità di attivazione automatica per la tua organizzazione.

Disattiva Amazon Inspector

> **Note**
>
> Prima di disattivare Amazon Inspector, valuta la possibilità di esportare i risultati.

Console

Per disattivare Amazon Inspector

1. Accedi utilizzando le tue credenziali, quindi apri la console https://console.aws.amazon.com/inspector/ Amazon Inspector su 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 l'account IDs che stai disattivando e `EC2, ECR, LAMBDA` se desideri disattivare tutte le scansioni, l'account verrà disattivato. `resourceTypes`

Quote Amazon Inspector

Questa sezione elenca le quote di Amazon Inspector per. Regione AWS

Risorsa	Default	Commenti
Account membri	10.000	Il numero massimo di account membro associati a un account amministratore delegato di Amazon Inspector. Il limite si basa su Quotas for. AWS Organizations
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 EC2 della rete Amazon	10.000	Il numero massimo di risultati della EC2 rete Amazon per AWS account. Non è possibile richiedere un aumento della quota.
Configurazioni di scansione CIS	500	Il numero massimo di configurazioni di scansione CIS. 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 Classic nel. Riferimenti generali di AWS Per un elenco delle quote associate a AWS Organizations, consulta AWS Organizations le quote di servizio nel. Riferimenti generali di AWS

Regioni ed endpoint

Questo argomento include tabelle che mostrano gli endpoint per Amazon Inspector e Amazon Inspector Scan. Include anche tabelle che mostrano quali Regioni AWS supportano le funzionalità di Amazon Inspector. Per visualizzare Regioni AWS dove è disponibile Amazon Inspector, consulta l'endpoint e le quote di Amazon Inspector nel. Riferimenti generali di Amazon Web Services

Endpoint di servizio per Amazon Inspector

La tabella seguente mostra gli endpoint del servizio per Amazon Inspector. La convenzione di denominazione per gli endpoint Amazon Inspector è. `inspector2.Region.amazonaws.com`

Nome della regione	Regione	Endpoint	Protocollo
Canada occidentale (Calgary)	ca-west-1	inspector2.ca-west-1.amazonaws.com ispettor2.ca-west-1.api.aws.com	HTTPS
US East (N. Virginia)	us-east-1	inspector2.us-east-1.amazonaws.com ispettor2.us-east-1.api.aws.com inspector2-fips.us-east-1.amazonaws.com	HTTPS
Stati Uniti orientali (Ohio)	us-east-2	inspector2.us-east-2.amazonaws.com ispettor2.us-east-2.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
		inspector2-fips.us-east-2.amazonaws.com	
US West (N. California)	us-west-1	inspector2.us-west-1.amazonaws.com ispector2.us-west-1.api.aws.com inspector2-fips.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	inspector2.us-west-2.amazonaws.com ispector2.us-west-2.api.aws.com inspector2-fips.us-west-2.amazonaws.com	HTTPS
Africa (Cape Town)	af-south-1	inspector2.af-south-1.amazonaws.com ispettor2.af-south-1.api.aws.com	HTTPS
Asia Pacifico (Hong Kong)	ap-east-1	inspector2.ap-east-1.amazonaws.com ispector2.ap-east-1.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacific (Sydney)	ap-southeast-2	inspector2.ap-southeast-2.amazonaws.com ispector2.ap-southeast-2.api.aws.com	HTTPS
Asia Pacifico (Giacarta)	ap-southeast-3	inspector2.ap-southeast-3.amazonaws.com ispector2.ap-southeast-3.api.aws.com	HTTPS
Asia Pacifico (Melbourne)	ap-southeast-4	inspector2.ap-southeast-4.amazonaws.com ispector2.ap-southeast-4.api.aws.com	HTTPS
Asia Pacifico (Malesia)	ap-southeast-5	inspector2.ap-southeast-5.amazonaws.com inspector2.ap-southeast-5.api.aws.com	HTTPS
Asia Pacifico (Tailandia)	ap-southeast-7	inspector2.ap-southeast-7.amazonaws.com inspector2.ap-southeast-7.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacific (Mumbai)	ap-south-1	inspector2.ap-south-1.amazonaws.com ispector2.ap-south-1.api.aws.com	HTTPS
Asia Pacific (Hyderabad)	ap-south-2	inspector2.ap-south-2.amazonaws.com ispector2.ap-south-2.api.aws.com	HTTPS
Asia Pacifico (Osaka-Locale)	ap-northeast-3	inspector2.ap-northeast-3.amazonaws.com ispector2.ap-northeast-3.api.aws.com	HTTPS
Asia Pacifico (Seul)	ap-northeast-2	inspector2.ap-northeast-2.amazonaws.com ispector2.ap-northeast-2.api.aws.com	HTTPS
Asia Pacific (Singapore)	ap-southeast-1	inspector2.ap-southeast-1.amazonaws.com ispector2.ap-southeast-1.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacific (Sydney)	ap-southeast-2	inspector2.ap-southeast-2.amazonaws.com ispector2.ap-southeast-2.api.aws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	inspector2.ap-northeast-1.amazonaws.com ispettore 2.ap-northeast-1.api.aws.com	HTTPS
Canada (Central)	ca-central-1	inspector2.ca-central-1.amazonaws.com ispettor2.ca-central-1.api.aws.com	HTTPS
Europe (Frankfurt)	eu-central-1	inspector2.eu-central-1.amazonaws.com ispector2.eu-central-1.api.aws.com	HTTPS
Europa (Irlanda)	eu-west-1	inspector2.eu-west-1.amazonaws.com ispector2.eu-west-1.api.aws.com	HTTPS
Europe (London)	eu-west-2	inspector2.eu-west-2.amazonaws.com ispector2.eu-west-2.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Europa (Milano)	eu-south-1	inspector2.eu-south-1.amazonaws.com ispector2.eu-south-1.api.aws.com	HTTPS
Europa (Spagna)	region-eu-south-2	ispettore 2. region-eu-south- 2.amazonaws.com ispettore 2. region-eu-south-2.api.aws.com	HTTPS
Europe (Paris)	eu-west-3	inspector2.eu-west-3.amazonaws.com ispector2.eu-west-3.api.aws.com	HTTPS
Europa (Stoccolma)	eu-north-1	inspector2.eu-north-1.amazonaws.com ispector2.eu-north-1.api.aws.com	HTTPS
Europa (Zurigo)	eu-central-2	inspector2.eu-central-2.amazonaws.com ispettor2.eu-central-2.api.aws.com	HTTPS
Israele (Tel Aviv)	il-central-1	inspector2.il-central-1.amazonaws.com ispector2.il-central-1.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Medio Oriente (Emirati Arabi Uniti)	me-central-1	inspector2.me-central-1.amazonaws.com ispector2.me-central-1.api.aws.com	HTTPS
Medio Oriente (Bahrein)	me-south-1	inspector2.me-south-1.amazonaws.com ispector2.me-south-1.api.aws.com	HTTPS
Messico (centrale)	mx-central-1	inspector2.mx-central-1.amazonaws.com inspector2.mx-central-1.api.aws.com	HTTPS
Sud America (São Paulo)	sa-east-1	inspector2.sa-east-1.amazonaws.com ispector2.sa-east-1.api.aws.com	HTTPS
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	ispettore 2. us-gov-east-1. amazonaws.com ispettore 2. us-gov-east-1.api.aws.com ispettore 2-fips. us-gov-east-1. amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	ispettore 2. us-gov-west-1. amazonaws.com ispettore 2. us-gov-west-1.api.aws.com ispettore 2-fips. us-gov-west-1. amazonaws.com	HTTPS

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
Canada occidentale (Calgary)	ca-west-1	inspector-scan.ca-west-1.amazonaws.com ispettore-scan.ca-west-1.api.aws.com	HTTPS
Stati Uniti orientali (Ohio)	us-east-2	inspector-scan.us-east-2.amazonaws.com inspector-scan.us-east-2.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
		inspector-scan-fips.us-east-2.amazonaws.com	
US East (N. Virginia)	us-east-1	inspector-scan.us-east-1.amazonaws.com inspector-scan.us-east-1.api.aws.com inspector-scan-fips.us-east-1.amazonaws.com	HTTPS
US West (N. California)	us-west-1	inspector-scan.us-west-1.amazonaws.com ispettore-scan.us-west-1.api.aws.com inspector-scan-fips.us-west-1.amazonaws.com	HTTPS
US West (Oregon)	us-west-2	inspector-scan.us-west-2.amazonaws.com ispettore-scan.us-west-2.api.aws.com inspector-scan-fips.us-west-2.amazonaws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Africa (Cape Town)	af-south-1	inspector-scan.af-south-1.amazonaws.com ispettore-scan.af-south-1.api.aws.com	HTTPS
Asia Pacifico (Hong Kong)	ap-east-1	inspector-scan.ap-east-1.amazonaws.com ispettore-scan.ap-east-1.api.aws.com	HTTPS
Asia Pacifico (Giacarta)	ap-southeast-3	inspector-scan.ap-southeast-3.amazonaws.com inspector-scan.ap-southeast-3.api.aws.com	HTTPS
Asia Pacific (Mumbai)	ap-south-1	inspector-scan.ap-south-1.amazonaws.com ispettore-scan.ap-south-1.api.aws.com	HTTPS
Asia Pacifico (Osaka-Locale)	ap-northeast-3	inspector-scan.ap-northeast-3.amazonaws.com ispettore-scan.ap-northeast-3.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Seul)	ap-northeast-2	inspector-scan.ap-northeast-2.amazonaws.com ispettore-scan.ap-northeast-2.api.aws.com	HTTPS
Asia Pacific (Hyderabad)	ap-south-2	inspector-scan.ap-south-2.amazonaws.com ispettore-scan.ap-south-2.api.aws.com	HTTPS
Asia Pacific (Singapore)	ap-southeast-1	inspector-scan.ap-southeast-1.amazonaws.com ispettore-scan.ap-southeast-1.api.aws.com	HTTPS
Asia Pacific (Sydney)	ap-southeast-2	inspector-scan.ap-southeast-2.amazonaws.com ispettore-scan.ap-southeast-2.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Asia Pacifico (Melbourne)	ap-southeast-4	inspector-scan.ap-southeast-4.amazonaws.com inspector-scan.ap-southeast-4.api.aws.com	HTTPS
Asia Pacifico (Malesia)	ap-southeast-5	inspector-scan.ap-southeast-5.amazonaws.com inspector-scan.ap-southeast-5.api.aws.com	HTTPS
Asia Pacifico (Tailandia)	ap-southeast-7	inspector-scan.ap-southeast-7.amazonaws.com ispettore-scan.ap-southeast-7.api.aws.com	HTTPS
Asia Pacifico (Tokyo)	ap-northeast-1	inspector-scan.ap-northeast-1.amazonaws.com ispettore-scan.ap-northeast-1.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Canada (Central)	ca-central-1	inspector-scan.ca-central-1.amazonaws.com ispettore-scan.ca-central-1.api.aws.com	HTTPS
Europe (Frankfurt)	eu-central-1	inspector-scan.eu-central-1.amazonaws.com inspector-scan.eu-central-1.api.aws.com	HTTPS
Europa (Irlanda)	eu-west-1	inspector-scan.eu-west-1.amazonaws.com inspector-scan.eu-west-1.api.aws.com	HTTPS
Europe (London)	eu-west-2	inspector-scan.eu-west-2.amazonaws.com inspector-scan.eu-west-2.api.aws.com	HTTPS
Europa (Milano)	eu-south-1	inspector-scan.eu-south-1.amazonaws.com inspector-scan.eu-south-1.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Europa (Spagna)	eu-south-2	inspector-scan.eu-south-2.amazonaws.com inspector-scan.eu-south-2.api.aws.com	HTTPS
Europe (Paris)	eu-west-3	inspector-scan.eu-west-3.amazonaws.com inspector-scan.eu-west-3.api.aws.com	HTTPS
Europa (Stoccolma)	eu-north-1	inspector-scan.eu-north-1.amazonaws.com inspector-scan.eu-north-1.api.aws.com	HTTPS
Europa (Zurigo)	eu-central-2	inspector-scan.eu-central-2.amazonaws.com inspector-scan.eu-central-2.api.aws.com	HTTPS
Medio Oriente (Emirati Arabi Uniti)	me-central-1	inspector-scan.me-central-1.amazonaws.com inspector-scan.me-central-1.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
Medio Oriente (Bahrein)	me-south-1	inspector-scan.me-south-1.amazonaws.com ispettore-scan.me-south-1.api.aws.com	HTTPS
Messico (centrale)	mx-central-1	inspector-scan.mx-central-1.amazonaws.com inspector-scan.mx-central-1.api.aws.com	HTTPS
Israele (Tel Aviv)	il-central-1	inspector-scan.il-central-1.amazonaws.com ispettore-scan.il-cetral-1.api.aws.com	HTTPS
Sud America (São Paulo)	sa-east-1	inspector-scan.sa-east-1.amazonaws.com ispettore-scan.sa-east-1.api.aws.com	HTTPS

Nome della regione	Regione	Endpoint	Protocollo
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1	ispector-scan. us-gov-east-1. amazonaws .com ispector-scan. us-gov-east-1.api.aws.com inspector-scan-fip s. us-gov-east-1. amazonaws.com	HTTPS
AWS GovCloud (Stati Uniti occidentali)	us-gov-west-1	ispector-scan. us-gov-west-1. amazonaws .com ispector-scan. us-gov-west-1.api.aws.com inspector-scan-fip s. 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

EC2 Scansione senza agente per le regioni Amazon EC2

La tabella seguente mostra Regioni AWS dove EC2 è attualmente disponibile la scansione senza agente per Amazon.

Nome della regione	Codice regione
US East (N. Virginia)	us-east-1
Stati Uniti orientali (Ohio)	us-east-2

Nome della regione	Codice regione
Stati Uniti occidentali (California settentri onale)	us-west-1
US West (Oregon)	us-west-2
Africa (Cape Town)	af-south-1
Asia Pacifico (Hong Kong)	ap-east-1
Asia Pacifico (Tokyo)	ap-northeast-1
Asia Pacifico (Seoul)	ap-northeast-2
Asia Pacifico (Osaka-Locale)	ap-northeast-3
Asia Pacific (Mumbai)	ap-south-1
Asia Pacific (Hyderabad)	ap-south-2
Asia Pacific (Singapore)	ap-southeast-1
Asia Pacific (Sydney)	ap-southeast-2
Asia Pacifico (Giacarta)	ap-southeast-3
Asia Pacifico (Melbourne)	ap-southeast-4
Asia Pacifico (Malesia)	ap-southeast-5
Asia Pacifico (Tailandia)	ap-southeast-7
Canada (Central)	ca-central-1
Canada occidentale (Calgary)	ca-west-1
Europa (Stoccolma)	eu-north-1
Europe (Frankfurt)	eu-central-1
Europa (Zurigo)	eu-central-2

Nome della regione	Codice regione
Europa (Irlanda)	eu-west-1
Europe (London)	eu-west-2
Europe (Paris)	eu-west-3
Europa (Milano)	eu-south-1
Europa (Spagna)	eu-south-2
Israele (Tel Aviv)	il-central-1
Medio Oriente (Emirati Arabi Uniti)	me-central-1
Medio Oriente (Bahrein)	me-south-1
Messico (centrale)	mx-central-1
Sud America (São Paulo)	sa-east-1
AWS GovCloud (Stati Uniti orientali)	us-gov-east-1
AWS GovCloud (Stati Uniti occidentali)	us-gov-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

Nome della regione	Codice regione
Asia Pacific (Tokyo)	ap-northeast-1
Europe (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
Europa (Stoccolma)	eu-north-1
Asia Pacific (Singapore)	ap-southeast-1

> **Important**
>
> Se tenti di abilitare la scansione del codice Lambda con l'API Amazon Inspector Enable Regione AWS in un luogo in cui la scansione del codice Lambda non è disponibile, ricevi il seguente errore di accesso negato:
>
> ```
> An error occurred (AccessDeniedException) when calling the Enable operation:
> Lambda code scanning is not supported in unsupported-Regione AWS
> ```

Regioni di sicurezza del codice Amazon Inspector

La tabella seguente mostra Regioni AWS dove Amazon Inspector Code Security è attualmente disponibile.

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

Nome della regione	Codice regione
Asia Pacific (Tokyo)	ap-northeast-1
Europe (Frankfurt)	eu-central-1
Europe (Ireland)	eu-west-1
Europe (London)	eu-west-2
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

La tabella seguente descrive le modifiche importanti in ogni versione della Amazon Inspector User Guide, a partire da novembre 2021. Per ricevere notifiche sugli aggiornamenti della documentazione, puoi iscriverti a un feed RSS.

Modifica	Descrizione	Data
Nuova policy	Amazon Inspector aggiunge una nuova policy gestita che fornisce l'accesso completo ad Amazon Inspector e l'accesso ad altri servizi correlati. Per ulteriori informazioni, consulta le politiche AWS gestite per Amazon Inspector.	3 luglio 2025
Funzionalità aggiornate	Amazon Inspector è ora disponibile in nuove versioni. Regioni AWS Per ulteriori informazioni, consulta Regioni ed endpoint.	1 luglio 2025
Funzionalità aggiornate	Amazon Inspector aggiorna il periodo di conservazione dei risultati chiusi. Amazon Inspector rimuove i risultati dopo 3 giorni se le risorse associate vengono eliminate , terminate o non sono più idonee per la scansione. Per ulteriori informazioni, consulta Comprendere i risultati di Amazon Inspector.	25 giugno 2025
Funzionalità aggiornate	Amazon Inspector aggiorna i sistemi operativi supportati per	18 giugno 2025

	la EC2 scansione Amazon e la scansione Amazon ECR. Amazon EC2 scanning ora supporta la Fedora versione 42 e la Ubuntu versione 25.04. La scansione Amazon ECR ora supporta la Alpine versione 3.22, la Fedora versione 42 e la Ubuntu versione 25.04. Per ulteriori informazioni, consulta Sistemi operativi e linguaggi di programmazione supportati per Amazon Inspector.	
Nuova caratteristica	Amazon Inspector ora analizza il codice sorgente delle applicazioni di prime parti, le dipendenze delle applicazioni di terze parti e Infrastructure as Code per individuare eventuali vulnerabilità. Per ulteriori informazioni, consulta Amazon Inspector Code Security.	17 giugno 2025

Aggiornamento per il plugin	Amazon Inspector viene informato di uno scenario in cui il plug-in Amazon Inspector SSM potrebbe generare un rilevamento di vulnerabilità per e. `CVE-2025-0913` `CVE-2025-4673` È stato confermato che il plug-in Amazon Inspector SSM non ne risente ed è stato distribuito un aggiornamento per risolvere questo CVEs rilevamento.	13 giugno 2025
Nuova caratteristica	Amazon Inspector ora può mostrare le immagini dei container utilizzate attivamente e l'ultima volta che le immagini dei container sono state utilizzate in un cluster. Per ulteriori informazioni, consulta Mappare le immagini dei container ai container in esecuzione.	16 maggio 2025
Nuova caratteristica	Amazon Inspector ora può mostrare le immagini dei container utilizzate attivamente e l'ultima volta che le immagini dei container sono state utilizzate in un cluster. Per ulteriori informazioni, consulta Mappare le immagini dei container ai container in esecuzione.	16 maggio 2025

Aggiornamenti ai sistemi operativi supportati	Amazon Inspector aggiunge il supporto per BusyBox Per ulteriori informazioni, consulta Sistemi operativi e linguaggi di programmazione supportati per Amazon Inspector.	13 maggio 2025
Politica aggiornata	Amazon Inspector aggiunge una nuova autorizzazione al ruolo collegato al servizio denominato. `AmazonInspector2ServiceRolePolicy` Questa autorizzazione consente di descriver e gli indirizzi IP e i gateway Internet. Per ulteriori informazioni, consulta le politiche AWS gestite per Amazon Inspector.	29 aprile 2025
Aggiornamento per il plugin	Amazon Inspector viene a conoscenza di uno scenario in cui il plug-in Amazon Inspector SSM potrebbe generare un rilevamento di vulnerabilità. `CVE-2025-22871` È stato confermato che il plug-in Amazon Inspector SSM non ne risente ed è stato distribuito un aggiornamento per risolvere questo CVEs rilevamento.	21 aprile 2025

Aggiornamento per il plugin	Amazon Inspector viene informato di uno scenario in cui il plug-in Amazon Inspector SSM potrebbe generare un rilevamento di vulnerabilità per, e. `CVE-2020-8911` `CVE-2020-8912` `CVE-2024-45337` È stato confermato che Amazon Inspector non è interessato da questi problemi CVEs ed è stato distribuito un aggiornamento per risolvere questo rilevamento.	18 aprile 2025
Aggiornamenti al capitolo Amazon Inspector SBOM Generator	Amazon Inspector aggiorna la versione di Amazon Inspector SBOM Generator. Per ulteriori informazioni, consulta Versioni precedenti di Amazon Inspector SBOM Generator.	16 aprile 2025
Aggiornamenti al capitolo Amazon Inspector SBOM Generator	Amazon Inspector aggiunge un nuovo argomento al capitolo Amazon Inspector SBOM Generator. Questo argomento descrive come tenere Sbomgen traccia delle informazioni sulla licenza in una distinta base del software. Per ulteriori informazioni, consulta la raccolta di licenze Amazon Inspector SBOM Generator.	16 aprile 2025

Aggiornamenti alle politiche gestite	Amazon Inspector aggiunge autorizzazioni che consenton o l'accesso in sola lettura alle azioni di Amazon ECS e Amazon EKS. Per ulteriori informazioni, consulta Autorizzazioni dei ruoli collegati ai servizi per Amazon Inspector.	25 marzo 2025
Aggiornamenti ai sistemi operativi supportati	Amazon Inspector non supporta SUSE Linux Enterprise Server 12.5 più la scansione per Amazon e EC2 Amazon ECR. Per ulteriori informazioni, consulta Sistemi operativi e linguaggi di programmazione supportati per Amazon Inspector.	21 marzo 2025
Aggiornamenti ai sistemi operativi supportati	Amazon Inspector aggiunge il supporto per Chainguard e alla scansione Wolfi Amazon ECR. Per ulteriori informazi oni, consulta Sistemi operativi e linguaggi di programma zione supportati per Amazon Inspector.	21 marzo 2025
Aggiornamenti al sommario	Amazon Inspector aggiunge un capitolo sull'etichettatura delle risorse di Amazon Inspector. Per ulteriori informazioni, consulta Taggare le risorse di Amazon Inspector.	25 febbraio 2025

Aggiornamenti al sommario	Amazon Inspector aggiunge un nuovo argomento al capitolo Amazon Inspector SBOM Generator. Per ulteriori informazioni, consulta la raccolta completa di sistemi operativi Amazon Inspector SBOM Generator.	28 gennaio 2025
Funzionalità aggiornate	Amazon Inspector aggiunge nodejs202.x e python3.1 3 amplia il suo elenco di runtime supportati per la scansione standard Lambda. Per ulteriori informazioni, consulta Sistemi operativi e linguaggi di programma zione supportati per Amazon Inspector.	24 gennaio 2025
Funzionalità aggiornate	Amazon Inspector rimuove Oracle Linux (Oracle) 7 e SUSE Linux Enterprise Server (SLES) 15.5 dal suo elenco di sistemi operativi supportat i per Amazon e EC2 Amazon ECR. Per ulteriori informazi oni, consulta Sistemi operativi e linguaggi di programma zione supportati per Amazon Inspector.	31 dicembre 2024

Funzionalità aggiornate	Amazon Inspector aggiunge Ubuntu 24.10 al suo elenco di sistemi operativi supportati per Amazon e EC2 Amazon ECR. Per ulteriori informazioni, consulta Sistemi operativi e linguaggi di programmazione supportati per Amazon Inspector.	12 dicembre 2024
Aggiornamenti al sommario	Amazon Inspector aggiunge nuovi argomenti al capitolo Amazon Inspector SBOM Generator. Per ulteriori informazioni, consulta Amazon Inspector SBOM Generator.	9 dicembre 2024
Funzionalità aggiornate	Amazon Inspector aggiorna la `amazon:inspector:sbom_generator` tabella per aggiungere e rimuovere namespace. Per ulteriori informazioni, consulta Utilizzo degli spazi dei nomi CyclonedX con Amazon Inspector.	9 dicembre 2024
Funzionalità aggiornate	Amazon Inspector aggiorna la sua funzionalità di integrazione CI/CD per supportare le azioni di scansione con. CodePipeline Per ulteriori informazioni, consulta Usare le azioni di scansione di Amazon Inspector con. CodePipeline	26 novembre 2024

Aggiornamenti al sommario	Amazon Inspector riorganizza il sommario per includere un capitolo per Amazon Inspector SBOM Generator. Per ulteriori informazioni, consulta Amazon Inspector SBOM Generator.	22 novembre 2024
Funzionalità aggiornate	Amazon Inspector rimuove Fedora 39 dal suo elenco di sistemi operativi supportati per Amazon e EC2 Amazon ECR. Per ulteriori informazi oni, consulta Sistemi operativi e linguaggi di programma zione supportati per Amazon Inspector.	22 novembre 2024
Funzionalità aggiornate	Amazon Inspector rimuove Alpine 3.17 dal suo elenco di sistemi operativi supportat i per Amazon ECR. Per ulteriori informazioni, consulta Sistemi operativi e linguaggi di programmazione supportati per Amazon Inspector.	22 novembre 2024
Funzionalità aggiornate	Amazon Inspector aggiunge Sbomgen versioni alle versioni precedenti di Amazon Inspector SBOM Generator.	19 novembre 2024

Funzionalità aggiornate	Amazon Inspector viene aggiunto AL2 come runtime supportato. Per ulteriori informazioni, consulta Sistemi operativi e linguaggi di programmazione supportati per Amazon Inspector.	26 agosto 2024
Funzionalità aggiornate	Amazon Inspector ha aggiunto una nuova dichiarazione alla AmazonInspector2ServiceRolePolicy policy. La nuova istruzione consente ad Amazon Inspector di restituire i tag di funzione. AWS Lambda	31 luglio 2024
Funzionalità aggiornate	Amazon Inspector rilascia nuovi controlli di sicurezza . Per ulteriori informazioni, consulta i controlli di Amazon Inspector nella Guida per l'AWS Security Hub utente.	11 luglio 2024
Funzionalità aggiornate	Amazon Inspector SBOM Generator ora analizza i file Dockerfile e le immagini dei container Docker alla ricerca di configurazioni errate che possono introdurre vulnerabilità di sicurezza. Per ulteriori informazioni, consulta Amazon Inspector Dockerfile checks.	10 giugno 2024

Funzionalità aggiornate	Amazon Inspector aggiorna la funzionalità di integrazione CI/CD per supportare CodeCatalyst le azioni, in modo da poter aggiungere scansioni di vulnerabilità di Amazon Inspector ai flussi di lavoro. CodeCatalyst Per ulteriori informazioni, consulta Utilizzo delle azioni. CodeCatalyst	7 giugno 2024
Funzionalità aggiornate	Amazon Inspector include un'opzione per scaricare un file CSV dei risultati della scansione CIS. Per ulteriori informazioni, consulta Visualizzazione e download dei risultati delle scansioni CIS nelle scansioni di Center for Internet Security (CIS) per le istanze Amazon. EC2	3 maggio 2024
Funzionalità aggiornate	Amazon Inspector aggiorna la funzionalità di integrazione CI/CD per supportar laGitHub Actions, in modo da poter aggiungere scansioni di vulnerabilità di Amazon Inspector ai flussi di lavoro. GitHub Per ulteriori informazioni, consulta Usare Amazon Inspector con. GitHub Actions	29 aprile 2024

Funzionalità aggiornate	Amazon Inspector aggiorna la policy gestita `AmazonInspector2FullAccess`, quindi crea il ruolo collegato al servizio. `AWSServiceRoleForAmazonInspector2Agentless` Ciò consente agli utenti di eseguire scansioni basate su agenti e scansioni senza agenti quando abilitano Amazon Inspector.	24 aprile 2024
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 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.	23 gennaio 2024
Nuova funzionalità	Amazon Inspector ora può eseguire scansioni del Center for Internet Security (CIS) sulle 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 CI/CD pipeline. 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' EC2 istanza per una scansione senza agenti. Per ulteriori informazioni sulla politica, consulta la sezione Scansione senza agente.	27 novembre 2023

Nuova funzionalità	Amazon Inspector ora supporta la scansione delle EC2 istanze Amazon Linux 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 macOS. EC2 Vedi Sistemi operativi supportati: Amazon EC2 scan 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 EC2 le istanze 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 EC2 istanze Amazon che fanno parte dei gruppi target di 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 crittogra fare 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 Amazon EC2 Deep Inspection.	17 aprile 2023
Nuova caratteristica	Amazon Inspector aggiunge supporto aggiuntivo per EC2 le istanze Linux 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 scansiona il codice sviluppatore delle tue 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.