Guida per gli sviluppatori di AWS IoT Device Defender

AWS IoT Device Defender

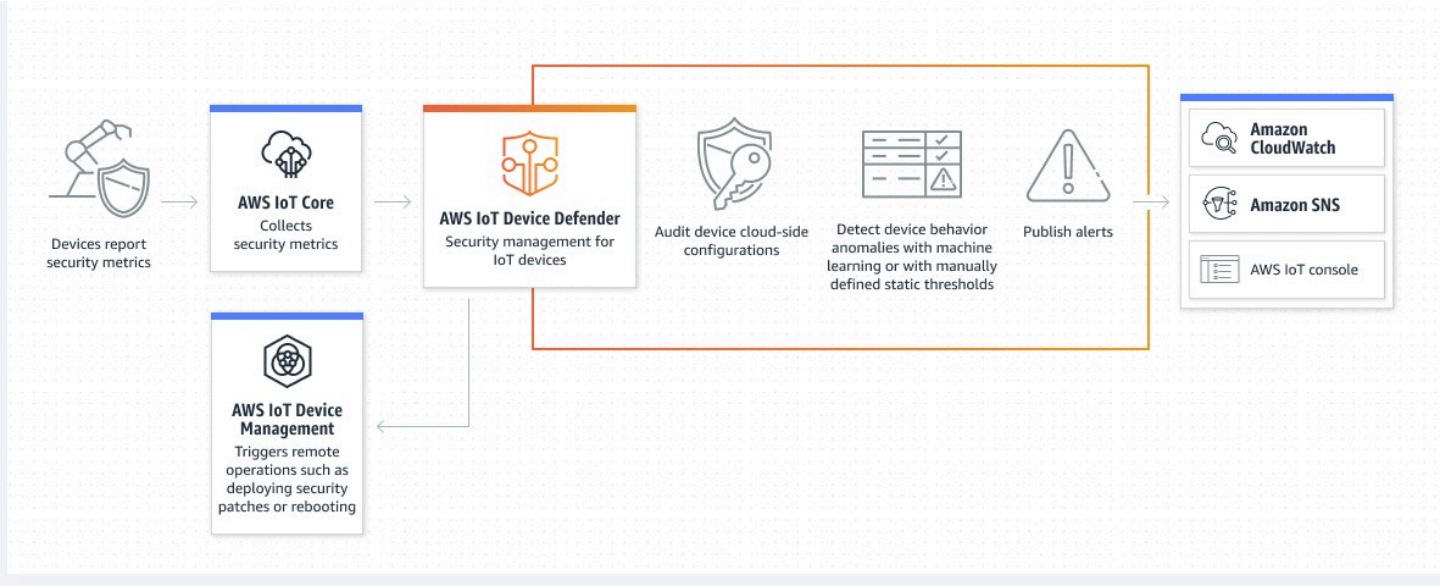
AWS IoT Device Defender: Guida per gli sviluppatori di AWS IoT Device Defender

Table of Contents

Cos'è AWS IoT Device Defender?

Usa AWS IoT Device Defender, un servizio di sicurezza e monitoraggio che permette di eseguire l'audit della configurazione dei dispositivi, monitorare i dispositivi connessi e mitigare i rischi di sicurezza. Con AWS IoT Device Defender hai la possibilità di applicare policy di sicurezza coerenti in tutto il parco istanze di dispositivi AWS IoT e di rispondere rapidamente quando i dispositivi vengono compromessi. I parchi istanze IoT possono essere costituiti da un numero elevato di dispositivi con funzionalità diverse, usati per lunghi periodi di tempo e distribuiti in varie aree geografiche. Queste caratteristiche rendono la configurazione di un parco istanze complessa e soggetta a errori. Poiché i dispositivi presentano spesso vincoli di potenza di elaborazione, memoria e capacità di storage, ciò limita l'uso della crittografia e di altre forme di sicurezza nei dispositivi stessi.

I dispositivi usano spesso software con vulnerabilità note. Questi fattori rendono i parchi istanze IoT un bersaglio interessante per gli hacker e rendono difficile proteggere il parco istanze di dispositivi su base continuativa. AWS IoT Device Defender risolve queste sfide fornendo gli strumenti per identificare i problemi di sicurezza e il mancato rispetto delle best practice. AWS IoT Device Defender è in grado di eseguire l'audit dei parchi istanze di dispositivi per verificare che vengano rispettate le best practice di sicurezza e per rilevare eventuali comportamenti anomali. Il diagramma seguente mostra l'architettura di base di AWS IoT Device Defender e il modo in cui si relaziona a servizi come AWS IoT Core, Amazon CloudWatch e Amazon SNS.



Argomenti

- Caratteristiche di AWS IoT Device Defender
- Nozioni di base su AWS IoT Device Defender
- Servizi correlati
- Accesso a AWS IoT Device Defender
- Prezzi di AWS IoT Device Defender

È il primo utilizzo di AWS IoT Device Defender?

Se usi AWS IoT Device Defender per la prima volta, ti consigliamo di iniziare leggendo le sezioni seguenti:

- Funzionamento di AWS IoT Device Defender
- Caratteristiche di AWS IoT Device Defender
- Nozioni di base su AWS IoT Device Defender
- Servizi correlati
- Accesso a AWS IoT Device Defender
- Prezzi di AWS IoT Device Defender

Funzionamento di AWS IoT Device Defender

AWS IoT Device Defender è un servizio di sicurezza e monitoraggio completamente gestito che ti aiuta a proteggere il parco istanze di dispositivi IoT. AWS IoT Device Defender verifica le risorse IoT associate ai tuoi dispositivi per confermare che siano conformi alle best practice di sicurezza. I controlli di audit inviano avvisi in caso di rischi per la sicurezza rilevati e forniscono informazioni pertinenti per contribuire a mitigare eventuali problemi. AWS IoT Device Defender monitora inoltre continuamente le metriche di sicurezza del cloud e dei dispositivi per rilevarne i comportamenti imprevisti e identificare eventuali dispositivi compromessi. È possibile avviare controlli di audit su richiesta o su base pianificata per valutare le configurazioni dei dispositivi IoT.

AWS IoT Device Defender utilizza AWS IoT Core per incorporare il contesto delle interazioni dei dispositivi per aumentare l'accuratezza dei controlli di audit. AWS IoT Device Defender raccoglie e analizza le metriche di sicurezza di alto valore dei dispositivi connessi per rilevare i comportamenti anomali. Quando si utilizza Rules Detect, i dati delle metriche vengono continuamente valutati rispetto ai comportamenti definiti dall'utente. Quando si utilizza ML Detect, i dati metrici vengono

continuamente valutati da modelli di machine learning (ML) creati automaticamente per identificare le anomalie.

I risultati delle attività di audit pianificate e delle eventuali anomalie rilevate nelle attività dei dispositivi vengono pubblicati nella console e AWS IoT e nell'API AWS IoT Device Defender. Sono accessibili tramite Amazon CloudWatch. Inoltre, puoi configurare AWS IoT Device Defender per l'invio dei risultati ad argomenti di Amazon SNS per l'integrazione con i dashboard di sicurezza o l'avvio di flussi di lavoro di correzione automatizzati.

AWS IoT Device Defender supporta un'ampia gamma di casi d'uso, inclusi i seguenti:

- Proteggi i tuoi dispositivi: puoi controllare le risorse relative ai dispositivi rispetto alle best practice di sicurezza di AWS IoT per rilevare le vulnerabilità dei dispositivi. Gli audit di AWS IoT Device Defender possono identificare e scoprire i rischi per i dispositivi e a verificare l'adozione delle misure di sicurezza.
- Rileva comportamenti insoliti dei dispositivi: puoi individuare le modifiche negli schemi di connessione, rivelare le comunicazioni dei dispositivi con endpoint non autorizzati e identificare i cambiamenti negli schemi di traffico dei dispositivi in entrata e in uscita.
- Ottieni approfondimenti per mitigare i rischi: puoi intraprendere azioni per mitigare i problemi rilevati in un risultato di audit o un allarme di Detect.
- Migliora e mantieni la sicurezza dei dispositivi: puoi utilizzare gli approfondimenti ottenuti dai controlli Audit e Detect per diagnosticare e porre rimedio a possibili violazioni della sicurezza.
- Migliora la sicurezza dei dispositivi: puoi individuare un dispositivo configurato in modo errato, verificare lo stato dei parchi istanze di dispositivi e individuare le metriche di comportamento imprevisto dei dispositivi.

Caratteristiche di AWS IoT Device Defender

Di seguito sono riportate alcune delle funzionalità principali di AWS IoT Device Defender.

Caratteristiche chiave

Audit	AWS IoT Device Defender verifica le risorse relative ai dispositivi rispetto alle best practice di sicurezza AWS IoT. Nella Guida per l'utente

	di IAM AWS IoT Device Defender riporta le configurazioni che non sono conformi alle best practice di sicurezza, come le policy eccessiva mente permissive che possono consentire a un dispositivo di leggere e aggiornare i dati per molti altri dispositivi.
Rules Detect	AWS IoT Device Defender rileva i comportam enti insoliti del dispositivo che possono essere indicativi di una compromissione monitoran do continuamente le metriche di sicurezza di alto valore del dispositivo e di AWS IoT Core. È possibile specificare il normale comportam ento del dispositivo per un gruppo di dispositi vi impostando i comportamenti (regole) per queste metriche. AWS IoT Device Defender monitora e valuta ogni punto dati riportato per queste metriche rispetto ai comportamenti (regole) definiti dall'utente e avvisa l'utente se viene rilevata un'anomalia.
Rilevamento ML	AWS IoT Device Defender imposta automatic amente i comportamenti dei dispositivi con i modelli di machine learning (ML) utilizzando i dati del dispositivo in base a sei metriche lato cloud e sette metriche lato dispositivo per un periodo di 14 giorni consecutivi. Quindi riqualifi ca i modelli ogni giorno (purché disponga di dati sufficienti per l'addestramento) per aggiornare i comportamenti previsti del dispositivo in base agli ultimi 14 giorni successivi alla creazione dei modelli iniziali. AWS IoT Device Defender monitora e identifica i punti dati anomali per questi parametri con i modelli di ML e attiva un allarme se viene rilevata un'anomalia.

Avviso	AWS IoT Device Defender pubblica gli allarmi sulla console AWS IoT, Amazon CloudWatch e Amazon SNS.
Mitigazione	AWS IoT Device Defender può essere utilizzato per indagare sui problemi fornendo informazioni contestuali e storiche sul dispositivo, come metadati, statistiche e avvisi cronologici relativi al dispositivo. È inoltre possibile usare le azioni di mitigazione predefinite di AWS IoT Device Defender per eseguire passaggi di mitigazione sugli allarmi Audit e Detect, ad esempio aggiungere elementi a un gruppo di oggetti, sostituire la versione predefinita della policy e aggiornare il certificato del dispositivo.

Nozioni di base su AWS IoT Device Defender

I seguenti tutorial forniscono le nozioni di base su AWS IoT Device Defender.

- Configurazione
- Guida di ML Detect
- Guida di audit
- Personalizzare quando e come visualizzare i risultati dell'audit AWS IoT Device Defender

Servizi correlati

- AWS IoT Greengrass: AWS IoT Greengrass fornisce l'integrazione predefinita con AWS IoT Device Defender per monitorare i comportamenti dei dispositivi su base continuativa.
- AWS IoT Device Management: puoi utilizzare l'indicizzazione del parco istanze di Gestione del dispositivo AWS IoT per indicizzare, ricercare e aggregare le violazioni identificate da AWS IoT Device Defender.

Accesso a AWS IoT Device Defender

Puoi utilizzare la console AWS IoT Device Defender o l'API per accedere a AWS IoT Device Defender.

Prezzi di AWS IoT Device Defender

Con AWS IoT Device Defender, si pagano solo i servizi usati. Non sono previste tariffe minime né utilizzi del servizio obbligatori. Tuttavia, le funzionalità Audit e Detect vengono fatturate separatamente. I prezzi di audit sono calcolati per numero di dispositivi al mese. Quando attivi Audit, l'addebito viene calcolato in base al numero di dispositivi principali attivi in un mese. Pertanto, l'aggiunta o la rimozione di controlli di audit non influirebbe sulla fattura mensile quando si utilizza questa funzionalità. Puoi calcolare il costo di AWS IoT Device Defender e quello dell'architettura con un'unica stima utilizzando il Calcolatore dei prezzi AWS.

- AWS Pricing Calculator

Nozioni di base su AWS IoT Device Defender

Avvaliti dei seguenti tutorial per imparare a utilizzare AWS IoT Device Defender.

Argomenti

Configurazione

Prima di usare AWS IoT Device Defender per la prima volta, è necessario completare le seguenti operazioni:

Argomenti

Registrati per creare un Account AWS

Se non disponi di un Account AWS, completa le fasi seguenti per crearne uno.

Per registrarsi a un Account AWS

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

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

   Durante la registrazione di un Account AWS, viene creato un Utente root dell'account AWS. L'utente root dispone dell'accesso a tutte le risorse e tutti i Servizi AWSnell'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.

Al termine del processo di registrazione, riceverai un'e-mail di conferma da AWS. È possibile visualizzare l'attività corrente dell'account e gestire l'account in qualsiasi momento accedendo all'indirizzo https://aws.amazon.com/ e selezionando Il mio account.

Crea un utente con accesso amministrativo

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

Protezione dell'Utente root dell'account AWS

1. Accedi alla AWS Management Consolecome proprietario dell'account scegliendo Utente root e immettendo l'indirizzo email dell'Account AWS. 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 ricevere istruzioni, consulta Abilitare un dispositivo MFA virtuale per l'utente root della Account AWS (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 origine di identità, consulta Configurazione dell'accesso utente con IAM Identity Center directory predefinito nella Guida per l'utente di AWS IAM Identity Center.

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 ricevere assistenza nell'accesso mediante un utente IAM Identity Center, consulta Accedere al portale di accesso AWSnella Guida per l'utente Accedi ad AWS.

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.

Queste attività creano un Account AWS e un utente IAM con privilegi di amministratore per l'account.

Guida di audit

Questo tutorial fornisce istruzioni su come configurare un audit ricorrente, impostare gli allarmi, esaminare i risultati dell'audit e mitigare i problemi di audit.

Argomenti

Prerequisiti

Per completare questo tutorial, è necessario quanto segue:

- Un Account AWS. Se non è stato creato, consulta Configurazione.

Abilita i controlli di auditing

Nella procedura seguente è possibile abilitare i controlli di audit che analizzano le impostazioni e le policy di account e dispositivi per garantire l'applicazione delle misure di sicurezza. In questo tutorial ti chiediamo di abilitare tutti i controlli di audit, ma sei in grado di selezionare qualsiasi controllo desideri.

I prezzi di controllo auditing sono per numero di dispositivi al mese (dispositivi del parco istanze connessi a AWS IoT). Pertanto, l'aggiunta o la rimozione di controlli di audit non influirebbe sulla fattura mensile quando si utilizza questa funzionalità.

1. Apri la AWS IoT console. Nel riquadro di navigazione, apri Sicurezza e scegli Introduzione.
2. Scegli Automazione della verifica di sicurezza AWS IoT. I controlli di verifica vengono attivati automaticamente.
3. Espandi Verifica e scegli Impostazioni per visualizzare i controlli di verifica. Seleziona il nome del controllo di verifica per conoscere le operazioni eseguite dal controllo di verifica. Per ulteriori informazioni sui controlli di audit, consulta Controlli di audit.
4. (Opzionale) Se già disponi di un ruolo che desideri utilizzare, scegli Gestisci le autorizzazioni del servizio, scegli il ruolo dall'elenco, quindi scegli Aggiorna.

Visualizza i risultati di audit

La procedura seguente mostra come visualizzare i risultati di audit. In questo tutorial vengono visualizzati i risultati dei di audit impostati nel tutorial Abilita i controlli di auditing.

Per visualizzare i risultati di audit

1. Apri la AWS IoT console. Nel riquadro di navigazione, espandi Sicurezza, Verifica e quindi scegli Risultati.
2. Seleziona la casella Nome del controllo di verifica che desideri analizzare.
3. In Controlli non conformi, sotto Mitigazione, seleziona i pulsanti informativi per informazioni sul motivo per cui non c'è conformità. Per le linee guida su come effettuare i controlli di non conformità, consulta Controlli di auditing.

Creazione di operazioni di mitigazione dell'audit

Nella procedura seguente, verrà creata un'operazione di mitigazione delle verifiche AWS IoT Device Defender per abilitare la registrazione di AWS IoT. Ogni controllo di audit ha mappato le operazioni di mitigazione che influiranno sul Tipo di operazione scelto per il controllo di audit che desideri correggere. Per ulteriori informazioni, consulta Operazioni di mitigazione.

Per utilizzare la console AWS IoT per creare operazioni di mitigazione

1. Apri la AWS IoT console. Nel riquadro di navigazione, espandi Sicurezza, Rileva e quindi scegli Operazioni di mitigazione.
2. Nella pagina Mitigation actions (Operazioni di mitigazione) scegli Create (Crea).
3. Nella pagina Crea una nuova operazione di mitigazione, in Nome operazione, immetti un nome univoco per l'operazione di mitigazione come, ad esempio, *`EnableErrorLoggingAction`*.
4. In Tipo di operazione, scegli Abilita registrazione AWS IoT.
5. In Autorizzazioni, scegli Crea ruolo. Per Nome ruolo, usa *`IoTMitigationActionErrorLoggingRole`*. Quindi scegli Create (Crea).
6. In Parametri, sotto Ruolo per la registrazione, seleziona `IoTMitigationActionErrorLoggingRole`. Per Log level (Livello di log), scegli `Error`.
7. Scegli Crea.

Applica operazioni di attenuazione ai risultati del controllo audit

La procedura seguente mostra come applicare le operazioni di attenuazione ai risultati dell'audit.

Per mitigare i risultati di audit non conformi

1. Apri la AWS IoT console. Nel riquadro di navigazione, espandi Sicurezza, Verifica e quindi scegli Risultati.
2. Scegli un risultato della verifica a cui desideri rispondere.
3. Controlla i risultati.
4. Scegli Start mitigation actions (Avvia operazioni di mitigazione).
5. Per Registrazione disabilitata, scegli l'operazione di mitigazione che hai creato in precedenza, `EnableErrorLoggingAction`. Per risolvere i problemi, puoi selezionare le operazioni appropriate per ogni esito non conforme.

6. Per Seleziona codici motivo, scegli il codice del motivo che è stato restituito dal controllo di verifica.
7. Scegli Avvia attività. L'esecuzione dell'operazione di mitigazione potrebbe richiedere alcuni minuti.

Per verificare che l'operazione di mitigazione abbia funzionato

1. Nella console AWS IoT, nel riquadro di navigazione scegli Impostazioni.
2. In Registro del servizio, conferma che Livello di log sia `Error (least verbosity)`.

Creazione di un ruolo IAM di verifica AWS IoT Device Defender (facoltativo)

Nella procedura seguente, è possibile creare un ruolo IAM di verifica AWS IoT Device Defender che fornisce a AWS IoT Device Defender l'accesso in lettura per AWS IoT.

Creazione del ruolo di servizio per AWS IoT Device Defender (console IAM)

1. Accedi a AWS Management Console e apri la console IAM all'indirizzo https://console.aws.amazon.com/iam/.
2. Nel pannello di navigazione della console IAM, scegliere Ruoli e quindi Crea ruolo.
3. Scegli il tipo di ruolo Servizio AWS.
4. In Casi d'uso per altri servizi AWS, scegli AWS IoT, quindi scegli IoT - Impostazioni di audit di Device Defender.
5. Seleziona Avanti.
6. (Facoltativo) Impostare un limite delle autorizzazioni. Questa è una caratteristica avanzata disponibile per i ruoli di servizio, ma non per i ruoli collegati ai servizi.

   Apri la sezione Permissions boundary (Limite delle autorizzazioni) e scegli Use a permissions boundary to control the maximum role permissions (Usa un limite delle autorizzazioni per controllare il numero massimo di autorizzazioni del ruolo). IAM include un elenco delle policy gestite da AWS e dal cliente nel tuo account. Selezionare la policy da utilizzare per il limite delle autorizzazioni o scegliere Crea policy per aprire una nuova scheda del browser e creare una nuova policy da zero. Per ulteriori informazioni, consulta Creazione di policy IAM nella Guida per l'utente di IAM. Una volta creata la policy, chiudi la scheda e torna alla scheda originale per selezionare la policy da utilizzare per il limite delle autorizzazioni.
7. Seleziona Avanti.

8. Inserisci un nome del ruolo che consenta di identificarne lo scopo. I nomi dei ruoli devono essere univoci all'interno dell'Account AWS. Non fanno distinzione tra maiuscole e minuscole. Ad esempio, non è possibile creare ruoli denominati sia **`PRODROLE`** che **`prodrole`**. Poiché varie entità possono fare riferimento al ruolo, non è possibile modificare il nome del ruolo dopo averlo creato.
9. (Facoltativo) In Description (Descrizione), inserisci una descrizione per il nuovo ruolo.
10. Scegli Edit (Modifica) nelle sezioni Step 1: Select trusted entities (Fase 1: seleziona le entità attendibili) o Step 2: Select permissions (Fase 2: seleziona autorizzazioni) per modificare i casi d'uso e le autorizzazioni per il ruolo.
11. (Facoltativo) Aggiungi metadati all'utente collegando i tag come coppie chiave-valore. Per ulteriori informazioni sull'utilizzo di tag in IAM, consulta la sezione Applicazione di tag alle risorse IAM nella Guida per l'utente di IAM.
12. Rivedere il ruolo e scegliere Crea ruolo.

Abilita notifiche SNS (facoltativo)

Nella procedura seguente, è possibile abilitare le notifiche Amazon SNS (SNS) per avvisare l'utente quando le verifiche identificano eventuali risorse non conformi. In questo tutorial verranno impostate le notifiche per i controlli di audit abilitati nel tutorial Abilita i controlli di auditing.

1. Se non l'hai già fatto, collega una policy che fornisce l'accesso a SNS attraverso la AWS Management Console. Puoi effettuare questa operazione seguendo le istruzioni in Collegamento di una policy a un gruppo di utenti IAM nella Guida per l'utente IAM e selezionando la policy AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction.
2. Apri la AWS IoT console. Nel riquadro di navigazione, espandi Sicurezza, Verifica e quindi scegli Impostazioni.
3. Nella parte inferiore della pagina Impostazioni di audit di Device Defender, scegli Abilita gli avvisi SNS.
4. Scegli Enabled (Abilitato).
5. Per Argomento, scegli Crea nuovo argomento. Denomina l'argomento *`IoTDDNotifications`* e seleziona Crea. Per Ruolo scegli il ruolo creato in Creazione di un ruolo IAM di verifica AWS IoT Device Defender (facoltativo).
6. Scegli Aggiorna.
7. Se desideri ricevere e-mail o messaggi nelle tue piattaforme Ops tramite SNS, consulta Utilizzo di Amazon Simple Notification Service per notifiche all'utente.

Abilita la registrazione (facoltativo)

Questa procedura descrive come abilitare AWS IoT per registrare le informazioni in CloudWatch Logs. In questo modo è possibile visualizzare i risultati di audit. L'abilitazione della registrazione può comportare spese aggiuntive.

Per attivare la registrazione

1. Apri la AWS IoT console. Nel riquadro di navigazione, seleziona Impostazioni.
2. In Log, scegli Gestisci log.
3. Per Seleziona ruolo, scegli Crea ruolo. Denomina il ruolo *`AWSIoTLoggingRole`* e scegli Crea. Viene collegata automaticamente una policy.
4. Per Livello di log, scegli Debug (livello massimo di dettaglio).
5. Scegli Aggiorna.

Guida a ML Detect

In questa guida introduttiva viene creato un profilo di protezione ML Detect che utilizza Machine Learning (ML) per creare modelli di comportamento previsto basati sui dati cronologici dei parametri provenienti dai dispositivi. È possibile monitorare l'avanzamento della creazione del modello ML da parte di ML Detec. Dopo aver creato il modello ML, è possibile visualizzare ed esaminare continuamente gli allarmi, nonché mitigare i problemi identificati.

Per ulteriori informazioni su ML Detect e i relativi comandi API e CLI, consulta Rilevamento ML.

Questo capitolo contiene le sezioni seguenti:

- Prerequisiti
- Come usare ML Detect nella console
- Come utilizzare ML Detect con CLI

Prerequisiti

- Un Account AWS. Se non è stato creato, consultare Setting up (Configurazione).

Come usare ML Detect nella console

Tutorial

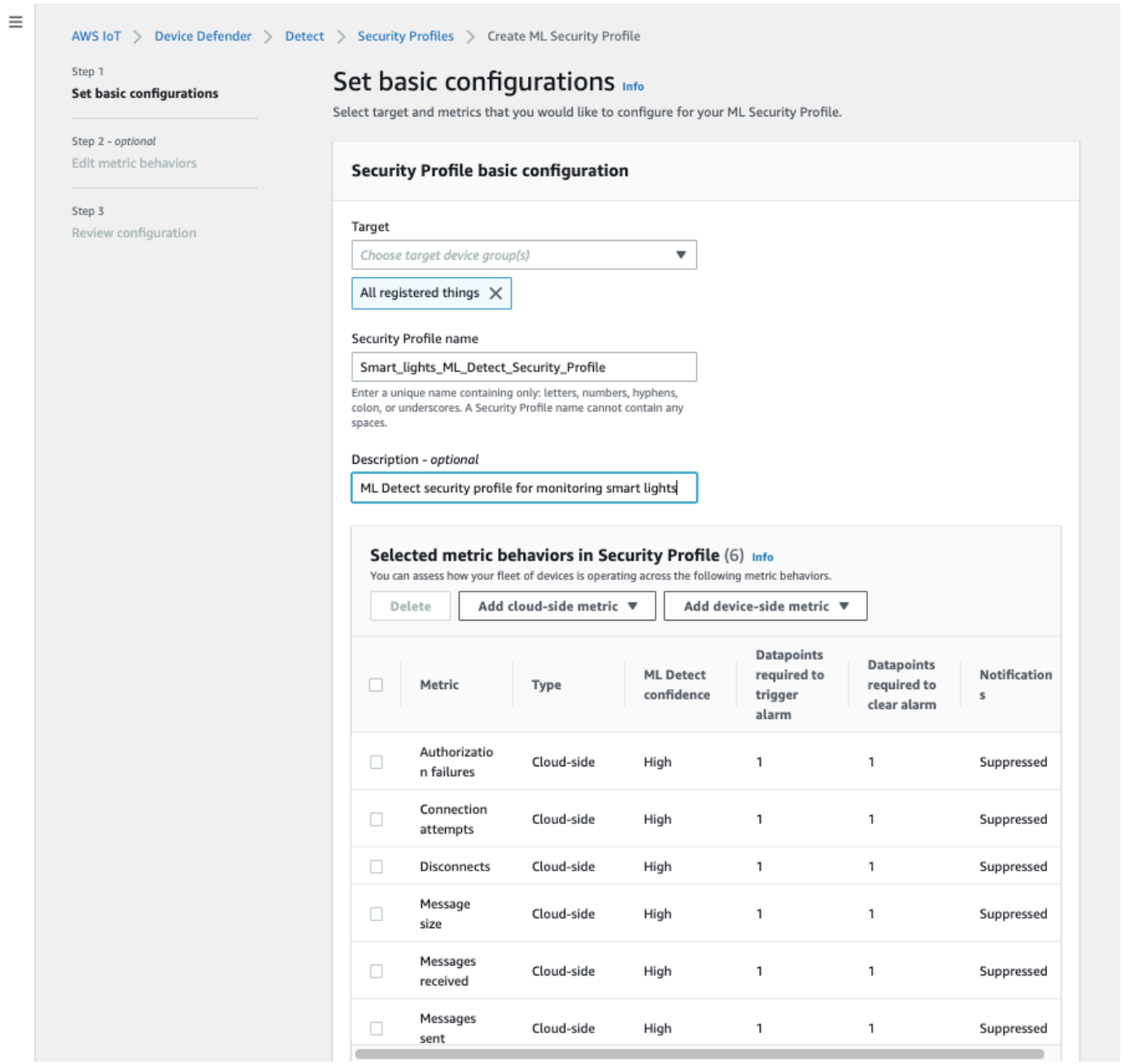
- Abilita ML Detect
- Monitoraggio dello stato del modello ML
- Esamina gli allarmi ML Detect
- Ottimizzare gli allarmi ML
- Contrassegna lo stato di verifica dell'allarme
- Mitigazione dei problemi identificati sul dispositivo

Abilita ML Detect

Le seguenti procedure illustrano come configurare ML Detect nella console.

1. Innanzitutto, assicurati che i tuoi dispositivi creino i datapoint minimi richiesti come definito in Requisiti minimi ML Detect per la formazione continua e il refresh del modello. Per far progredire la raccolta dei dati, assicurati che il tuo profilo di sicurezza sia collegato a una destinazione, che può essere un oggetto o un gruppo di oggetti.
2. In AWS IoT console, nel pannello di navigazione, espandi Defend (Protezione). Scegli Detect (Rilevamento), Security profiles (Profili di sicurezza), Create security profile (Crea profilo di sicurezza), e quindi Create ML anomaly Detect profile (Crea profilo ML Detect anomalia).
3. Sulla pagina Set basic configurations (Imposta configurazioni di base) esegui le operazioni seguenti.

    - In Target seleziona i gruppi di dispositivi di destinazione.
    - In Security profile name (Nome profilo di sicurezza) immetti un nome per il tuo profilo di sicurezza.
    - (Facoltativo) In Description (Descrizione) puoi scrivere una breve descrizione del profilo ML.
    - In Selected metric behaviors in Security Profile (Comportamenti delle metriche selezionati nel profilo di sicurezza), scegli le metriche che desideri monitorare.

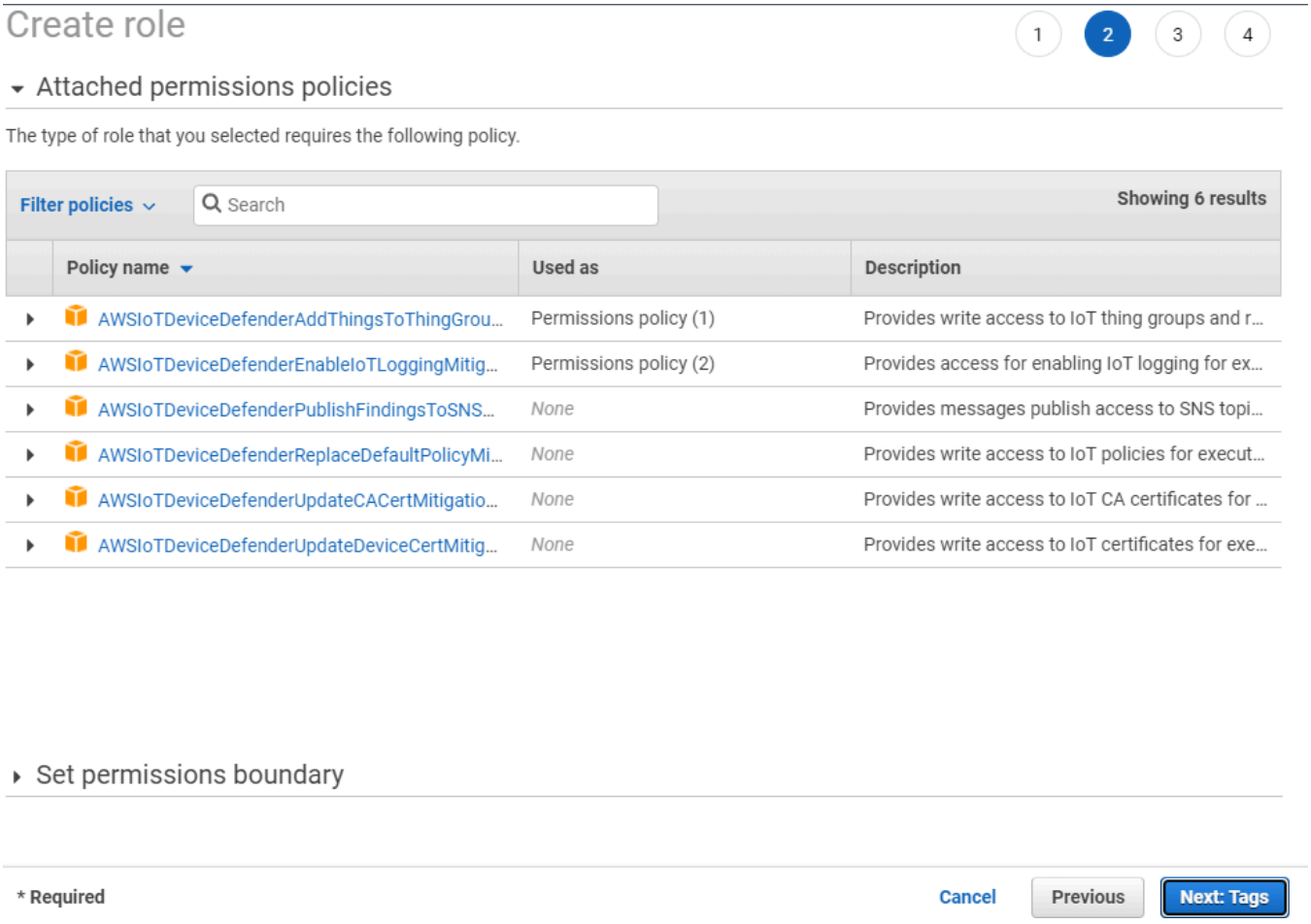


Al termine, selezionare Next (Successivo).

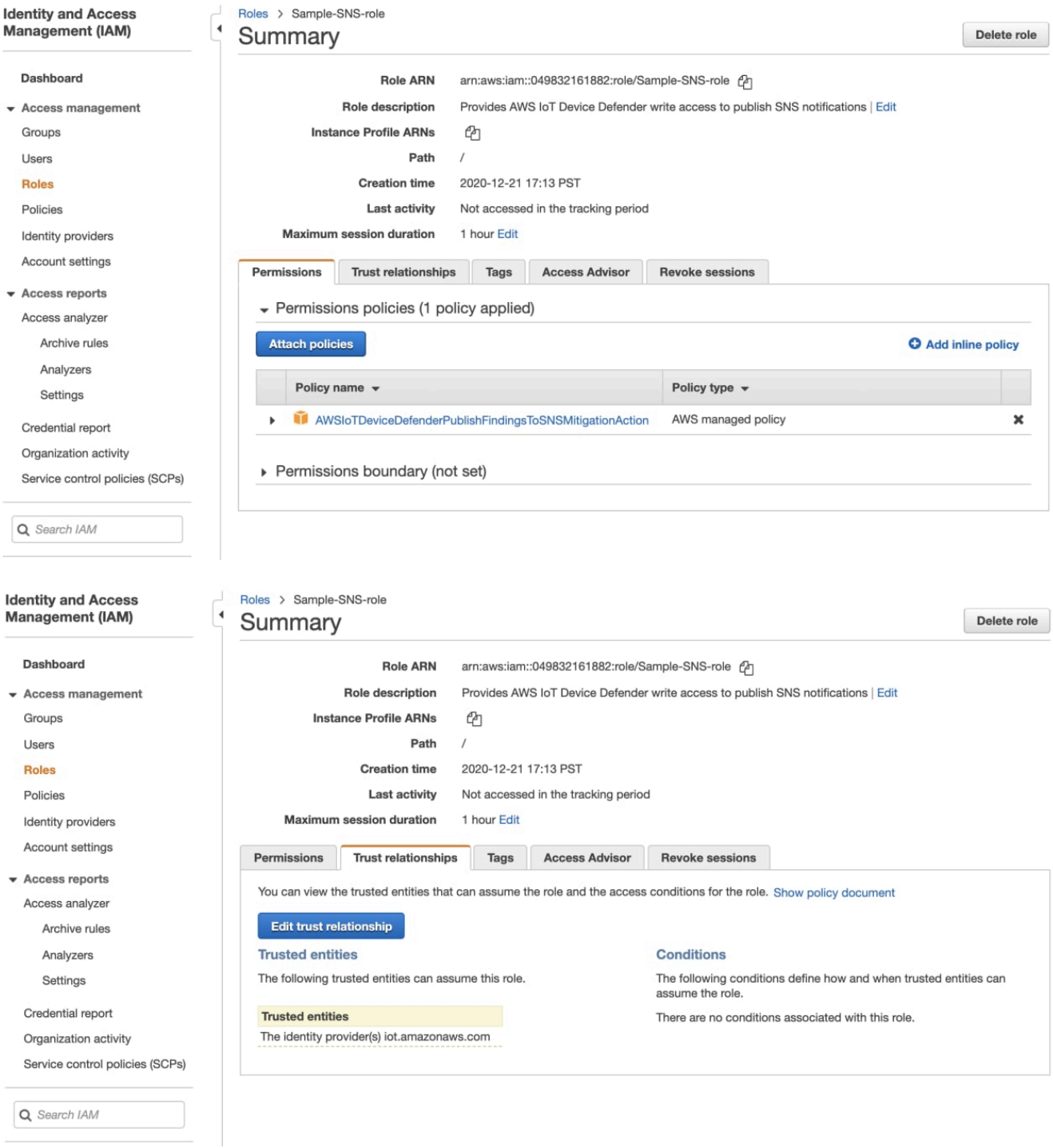
4. Su Set SNS (Imposta SNS) (opzionale), specifica un argomento SNS per le notifiche di avviso quando un dispositivo viola un comportamento nel profilo. Scegliere un ruolo IAM che utilizzerai per pubblicare sull'argomento SNS selezionato.

   Se non disponi ancora di un ruolo SNS, attieniti alla seguente procedura per creare un ruolo con le autorizzazioni e le relazioni di trust corrette richieste.

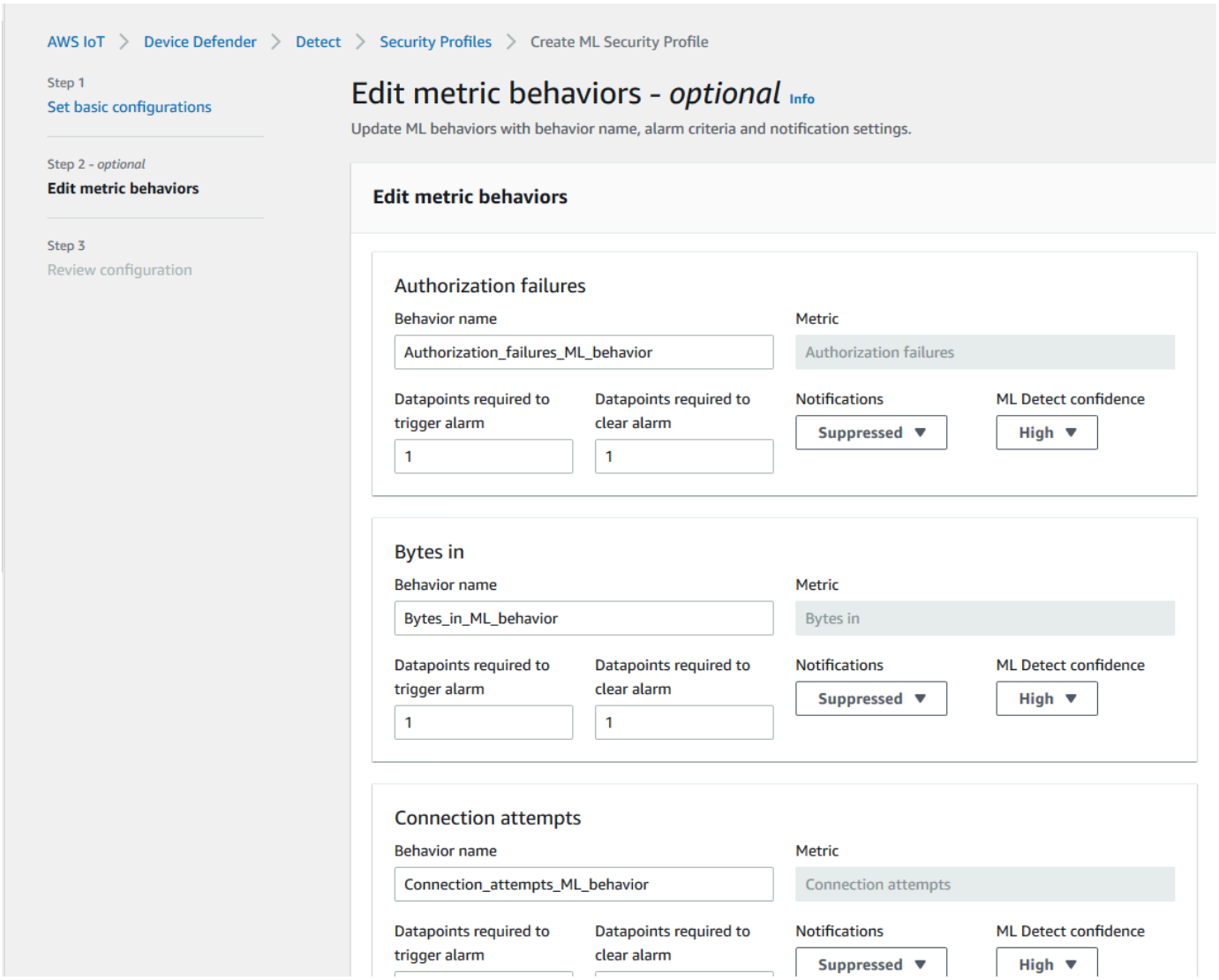
- Passare alla Console IAM. Nel riquadro di navigazione, scegli Ruoli, quindi Crea ruolo.
- In Select type of trusted entity (Seleziona tipo di entità attendibile), seleziona AWS Service (Servizio AWS). Quindi, in Choose a use case (Scegli un caso d'uso), scegli IoT e in Select your use case (Seleziona il caso d'uso), scegli IoT - Device Defender Mitigation Actions (IoT - Operazioni di mitigazione Device Defender). Al termine della configurazione delle autorizzazioni, scegli Next (Avanti).
- In Attached permissions policies (Policy di autorizzazione collegate), assicurati che awSiotDeviceDefenderPublishFindingsToSNSmitigationAction sia selezionato, quindi scegli Next: Tags (Successivo: Tag).



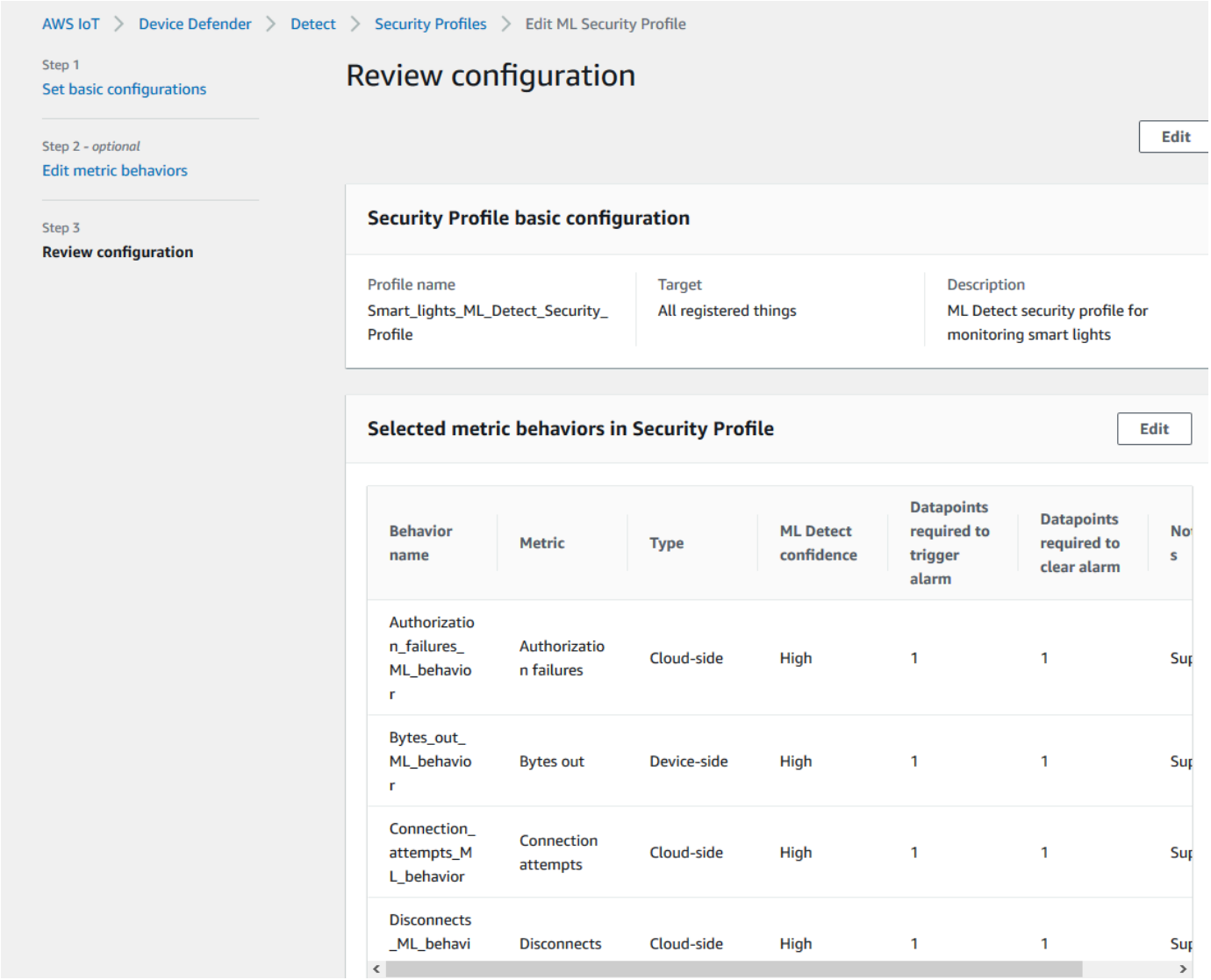
- In Add tags (Aggiunta di tag) (facoltativo) puoi aggiungere i tag da associare al tuo ruolo. Al termine, seleziona Successivo: esamina.
- In Review (Revisione), assegna un nome al tuo ruolo e assicurati che awSiotDeviceDefenderPublishFindingsToSNSmitigationAction sia elencato sotto Permissions (Autorizzazioni) e che Servizi AWS: iot.amazonaws.com sia elencato sotto Trust relationships (Relazioni di trust). Al termine, seleziona Create role (Crea ruolo).



5. Sullla pagina Edit Metric behavior (Modifica comportamento della metrica), è possibile personalizzare le impostazioni di comportamento ML.



6. Al termine, selezionare Next (Successivo).
7. Sulla pagina Review configuration (Verifica della configurazione), verifica i comportamenti che desideri monitorare l'apprendimento automatico e quindi scegli Next (Successivo).



8. Dopo aver creato il tuo profilo di sicurezza, verrai reindirizzato alla pagina Security Profiles (Profili di sicurezza), in cui viene visualizzato il profilo di sicurezza appena creato.

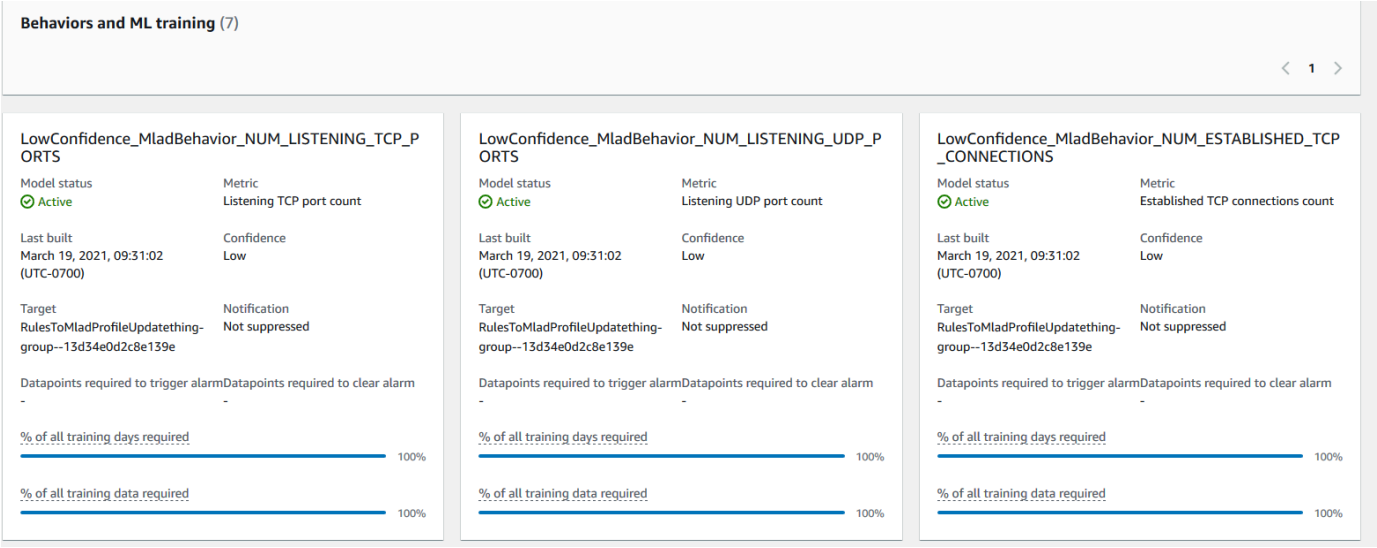
> **Note**
>
> La formazione iniziale e la creazione del modello ML richiedono 14 giorni per essere completate. Puoi aspettarti di vedere gli allarmi al termine in caso di attività anomala sui tuoi dispositivi.

Monitoraggio dello stato del modello ML

Mentre i modelli ML si trovano nel periodo iniziale di allenamento, puoi monitorarne i progressi in qualsiasi momento seguendo le seguenti operazioni.

1. Nel riquadro di spostamento dell'AWS IoT console, espandi Defend (Protezione), poi seleziona Detect (Rileva), e Security profiles (Profili di sicurezza).
2. Sulla pagina Security profiles (Profili di sicurezza), scegli il profilo di sicurezza che desideri rivedere. Quindi, scegli Behaviors and ML training (Comportamenti e formazione ML).
3. Sulla pagina Behaviors and ML training (Comportamenti e formazione ML), controlla l'avanzamento della formazione dei modelli ML.

   Quando lo stato del modello risulta Active (Attivo), inizierà a prendere le decisioni di Detect in base al tuo utilizzo e aggiornerà il profilo ogni giorno.

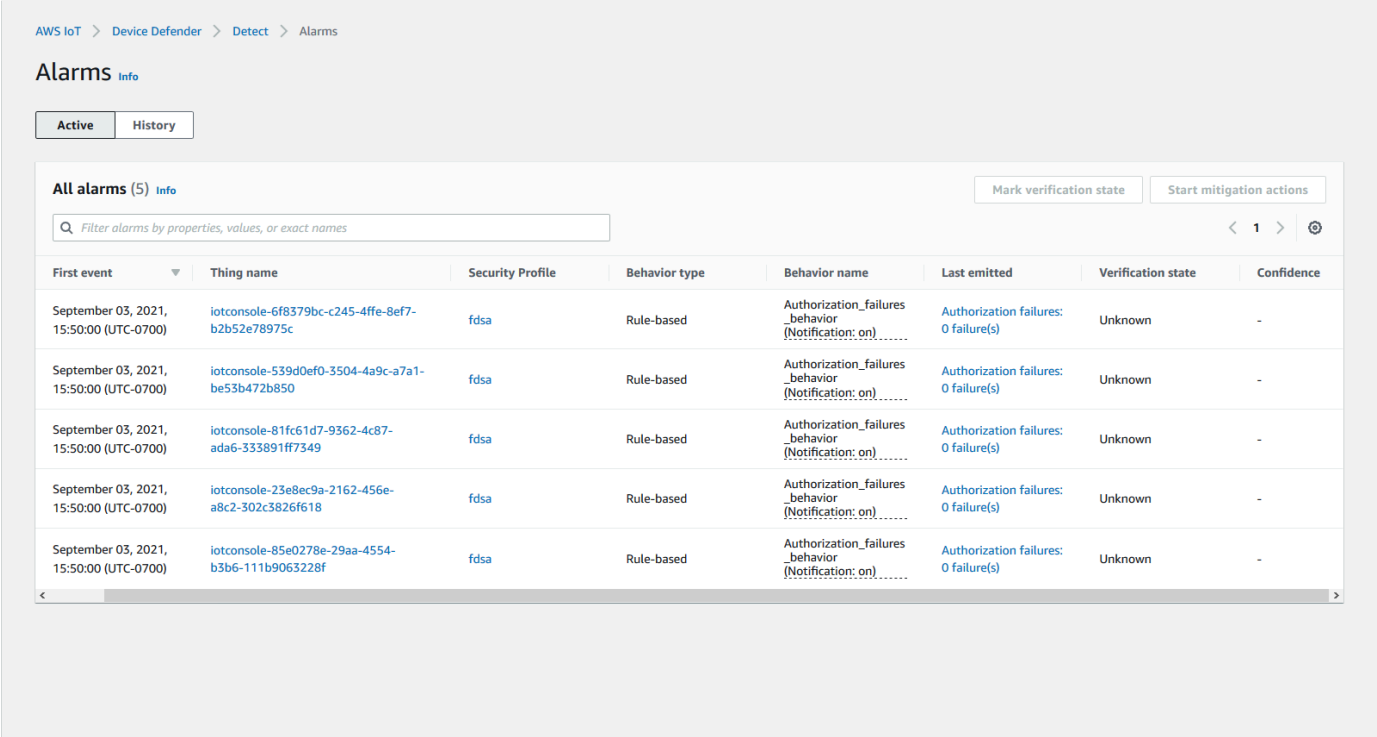


> **Note**
>
> Se il tuo modello non progredisce come previsto, assicurati che i tuoi dispositivi soddisfino il Requisiti minimi.

Esamina gli allarmi ML Detect

Dopo che i modelli ML sono stati creati e sono pronti per l'inferenza dei dati, è possibile visualizzare regolarmente tutti gli allarmi che vengono dedotti dai modelli.

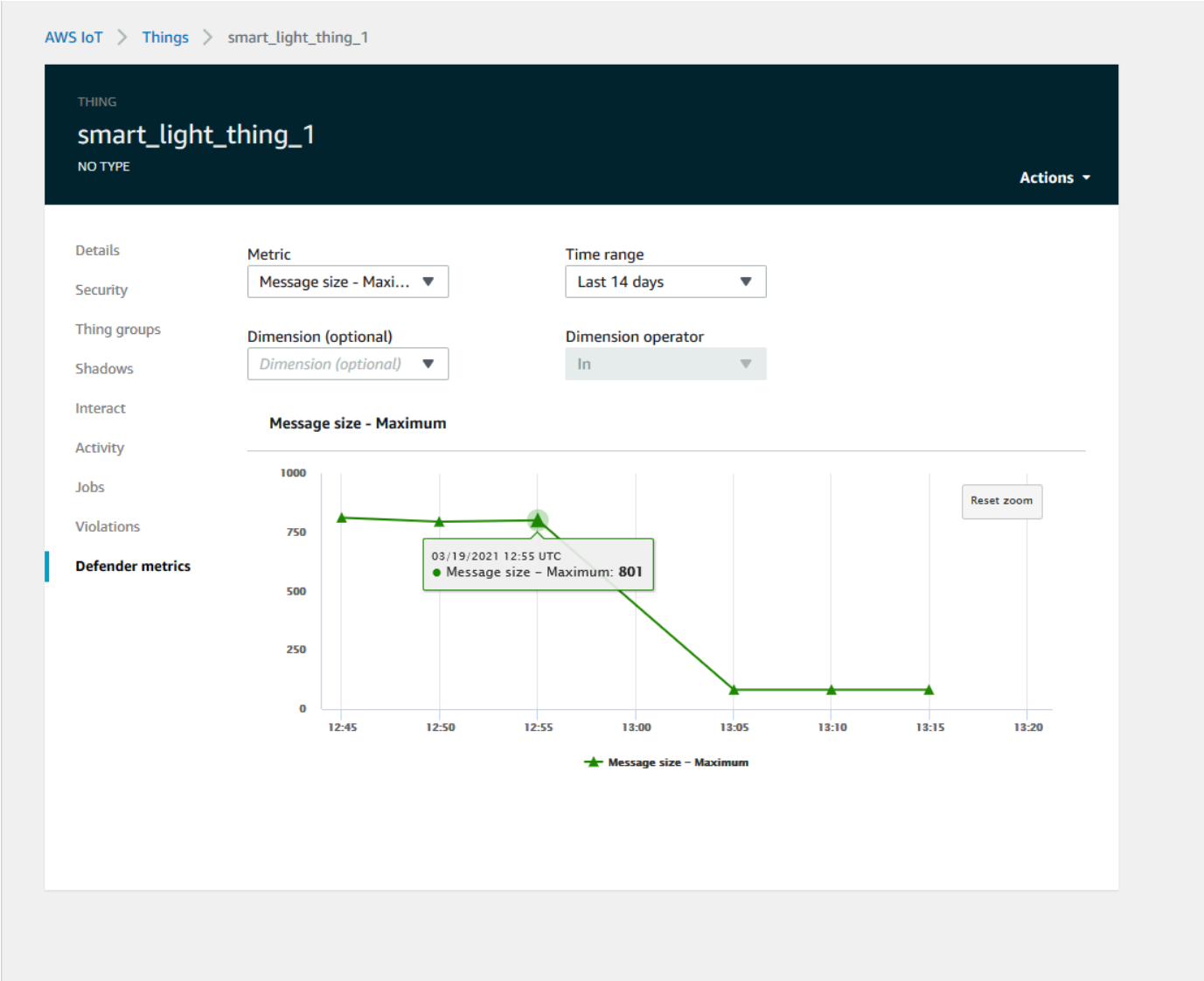
1. Nell'AWS IoT console, nel pannello di navigazione, espandi Defend (Protezione) e poi scegli Detect (Rileva), Alarms (Allarmi).



2. Se accedi alla Cronologia, puoi visualizzare i dettagli sui tuoi dispositivi che non sono più in allarme.

Per ottenere altre informazioni, in Manage (Gestione) scegli Things (Oggetti), seleziona l'oggetto per cui desideri visualizzare maggiori dettagli, quindi vai a Defender metrics (Parametri di

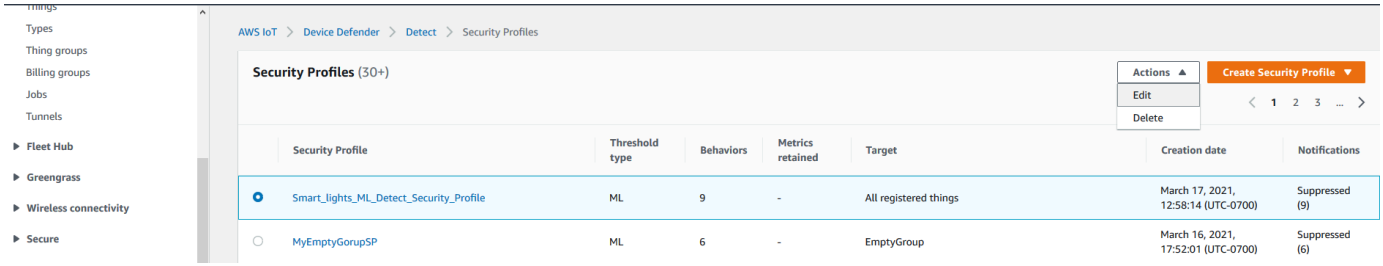
Defender). Puoi accedere al Defender metrics graph (Grafico delle metriche di Defender) ed eseguire l'indagine su qualsiasi cosa in allarme dalla scheda Active (Attivo). In questo caso, il grafico mostra un picco nella dimensione del messaggio, che ha attivato l'allarme. È possibile visualizzare l'allarme che è stato successivamente cancellato.



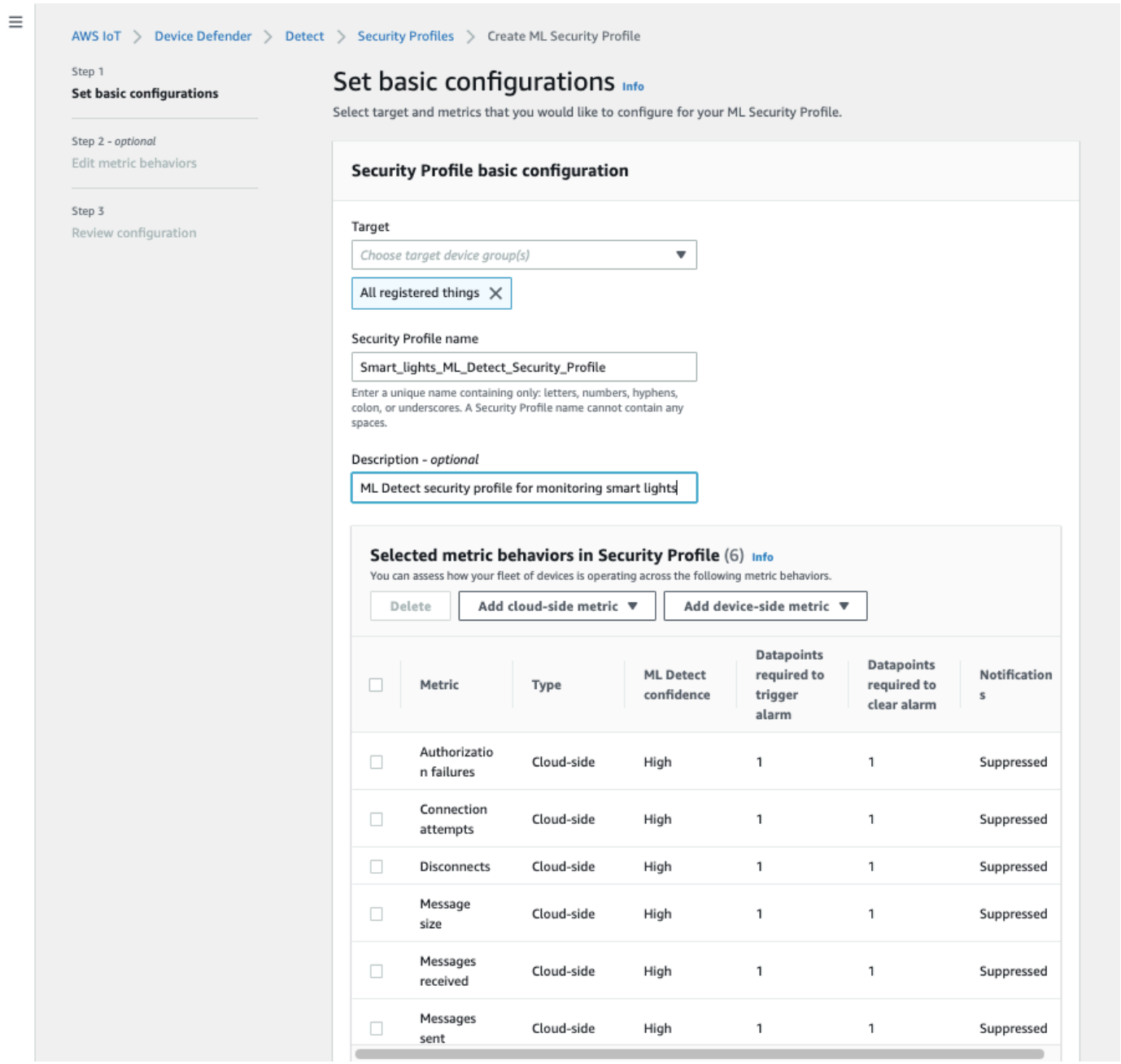
Ottimizzare gli allarmi ML

Una volta che i modelli ML sono stati creati e sono pronti per l'inferenza dei dati, è possibile aggiornare le impostazioni di comportamento ML del profilo di sicurezza per modificare la configurazione. La procedura seguente mostra come aggiornare le impostazioni di comportamento ML del profilo di sicurezza nell'area AWS CLI.

1. Nel riquadro di spostamento dell'AWS IoT console, espandi Defend (Protezione), espandi Detect (Rileva), e seleziona Security profiles (Profili di sicurezza).
2. Sulla pagina Security Profiles (Profili di sicurezza) seleziona la casella di controllo accanto al profilo di sicurezza che desideri esaminare. Scegli Actions (Operazioni), quindi Edit (Modifica).

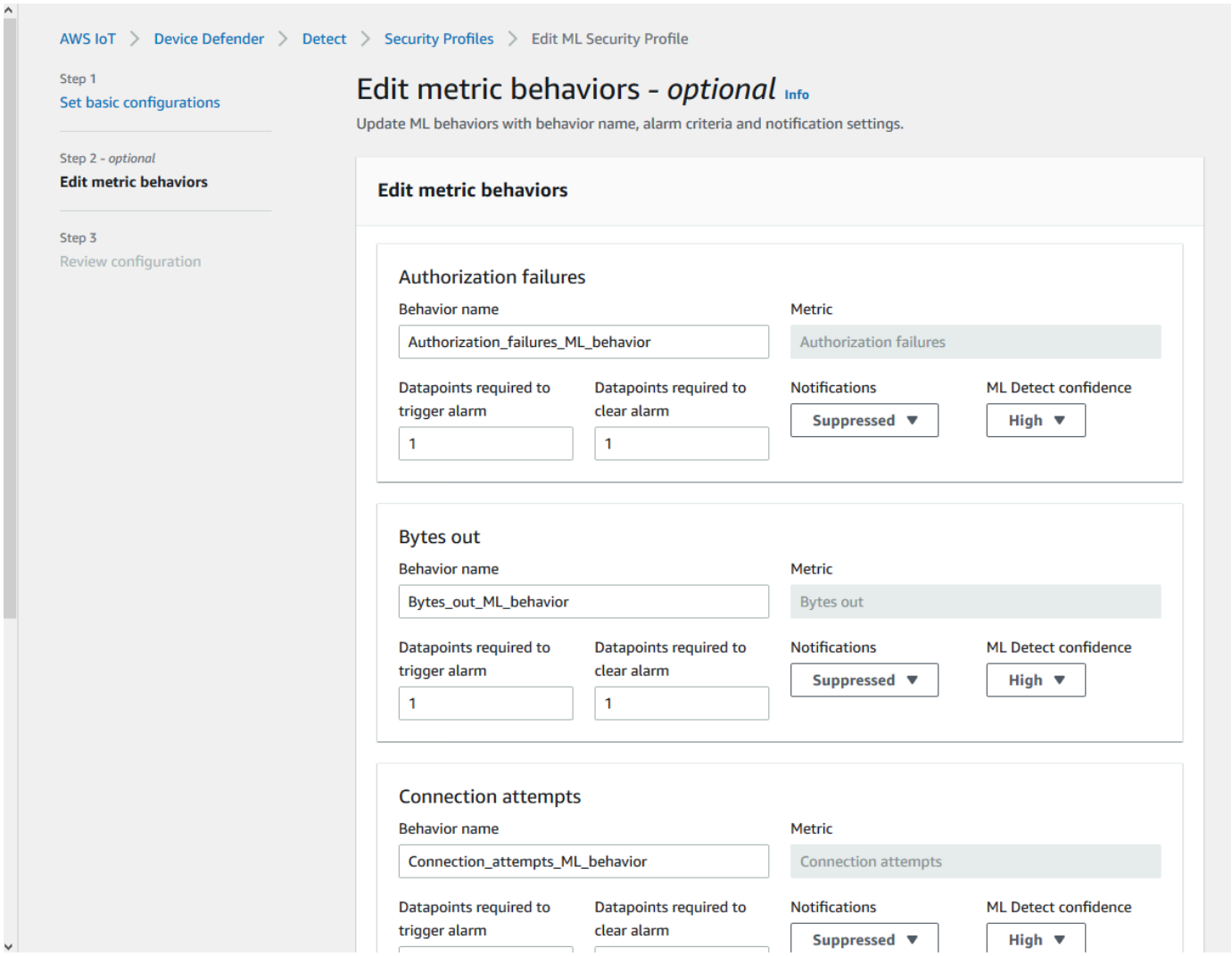


3. In Set basic configurations (Imposta configurazioni di base), è possibile modificare i gruppi di oggetti di destinazione del profilo di sicurezza o modificare le metriche che si desidera monitorare.



4. È possibile aggiornare qualsiasi delle seguenti opzioni accedendo a Edit metric behaviors (Modifica dei comportamenti delle metriche).

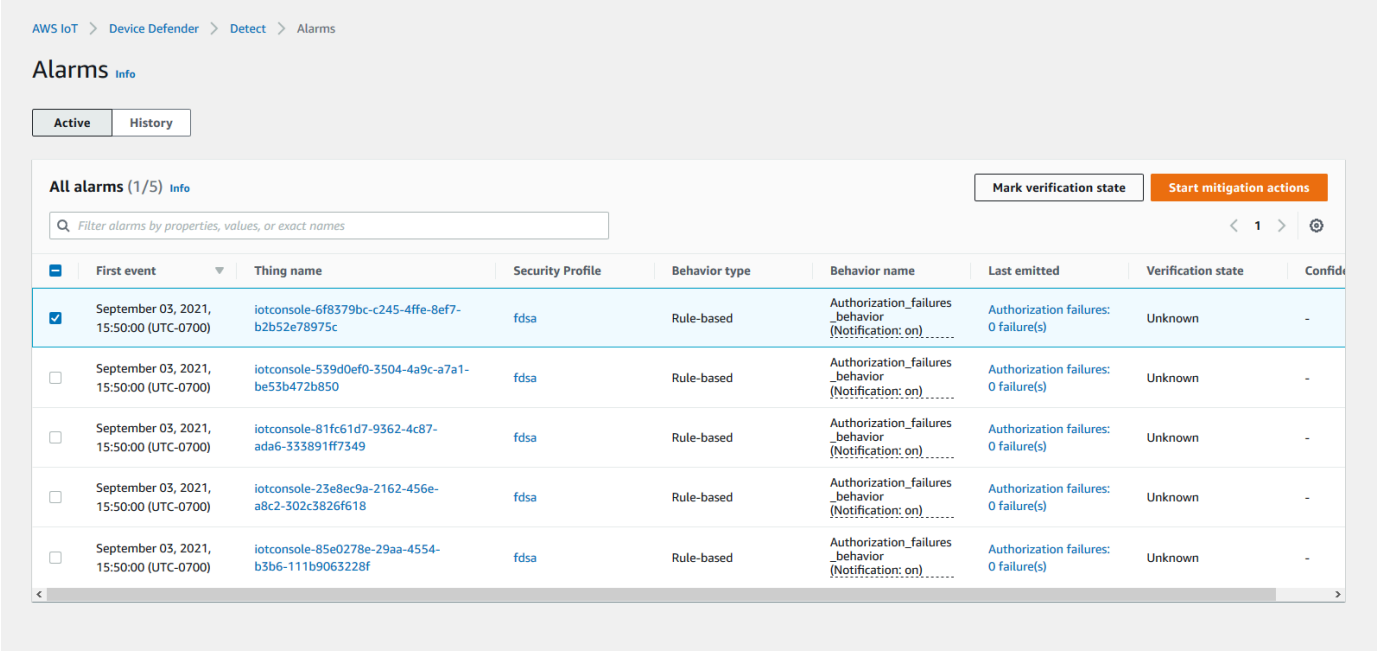
   - I datapoint del modello ML necessari per attivare l'allarme
   - I datapoint del modello ML necessari per attivare l'allarme
   - Il tuo livello di fiducia in ML Detect
   - Le notifiche di ML Detect (ad esempio, Not suppressed (Non soppresso), Suppressed (Soppressione))



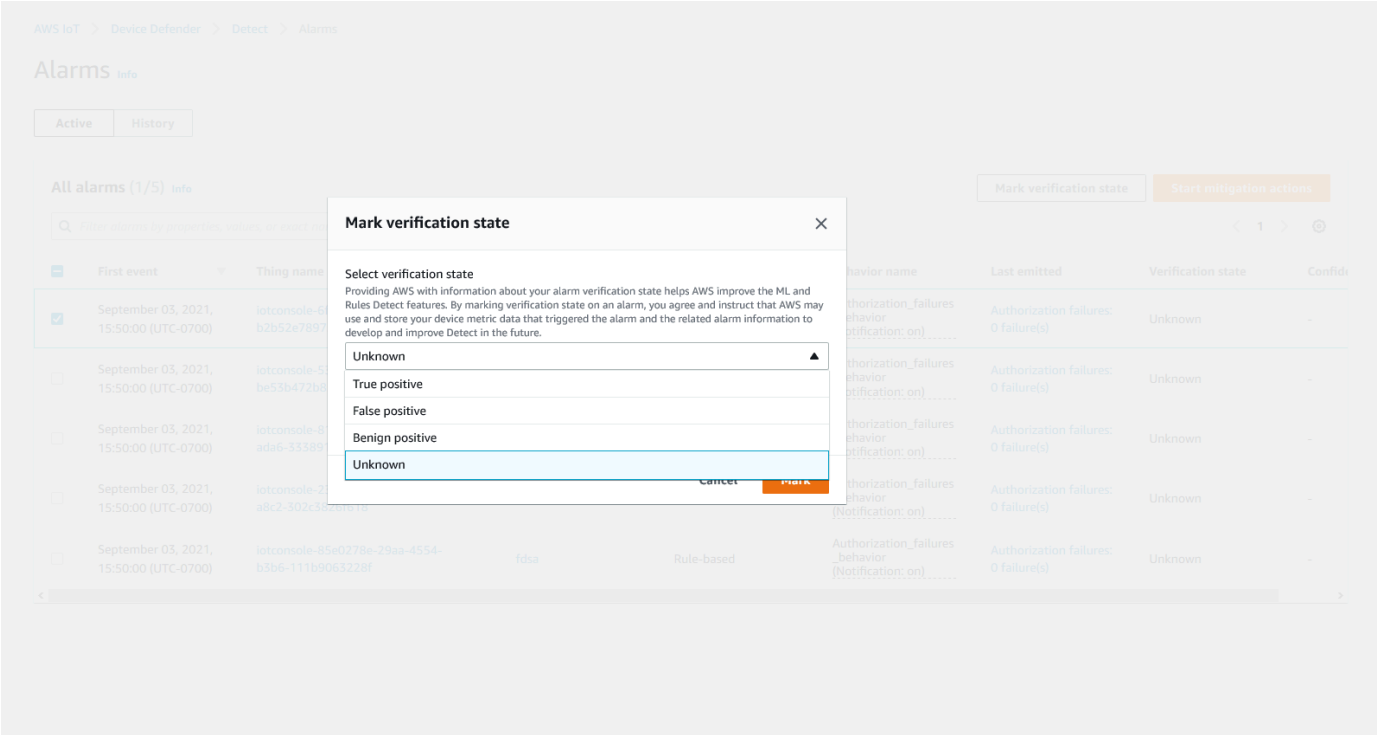
Contrassegna lo stato di verifica dell'allarme

Contrassegna i tuoi allarmi impostando lo stato di verifica e fornendo una descrizione dello stato di verifica. Questo aiuta te e il tuo team a identificare gli allarmi da ignorare.

1. Nella console AWS IoT, nel pannello di navigazione, espandi Defend (Proteggi) e poi scegli Detect (Rileva), Alarms (Allarmi). Seleziona un avviso per contrassegnarne lo stato di verifica.



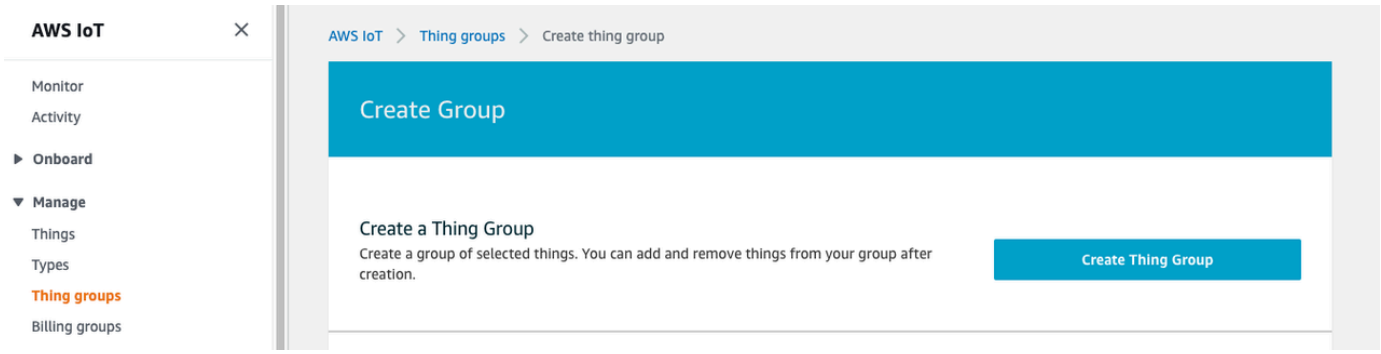
2. Scegli Mark verification state (Contrassegna stato di verifica). Si apre il modale dello stato di verifica.
3. Scegli lo stato di verifica appropriato, inserisci una descrizione della verifica (facoltativa), quindi scegli Mark (Contrassegna). Questa operazione assegna uno stato di verifica e una descrizione all'allarme scelto.



Mitigazione dei problemi identificati sul dispositivo

1. (Opzionale) Prima di impostare le azioni di attenuazione della quarantena, impostiamo un gruppo di quarantena in cui sposteremo il dispositivo in violazione. È anche possibile utilizzare un gruppo esistente.
2. Accedi a Manage (Gestione), Thing groups (Gruppi di oggetti), e poi Create Thing Group (Crea gruppo di oggetti). Nomina il tuo gruppo di oggetti. Per questo tutorial, chiameremo il gruppo di oggetti `Quarantine_group`. In Thing group (Gruppo di oggetti), Security (Sicurezza) applica la policy seguente al gruppo di oggetti.

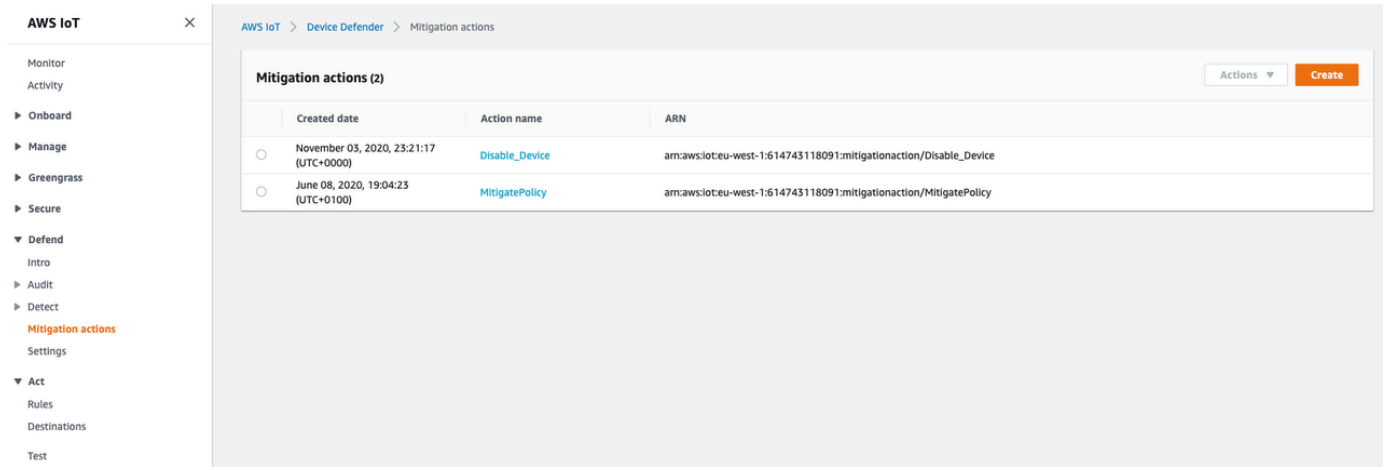
```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Deny",
      "Action": "iot:*",
      "Resource": "*",
    }
  ]
}
```



Al termine, seleziona Create thing group (Crea gruppo di oggetti).

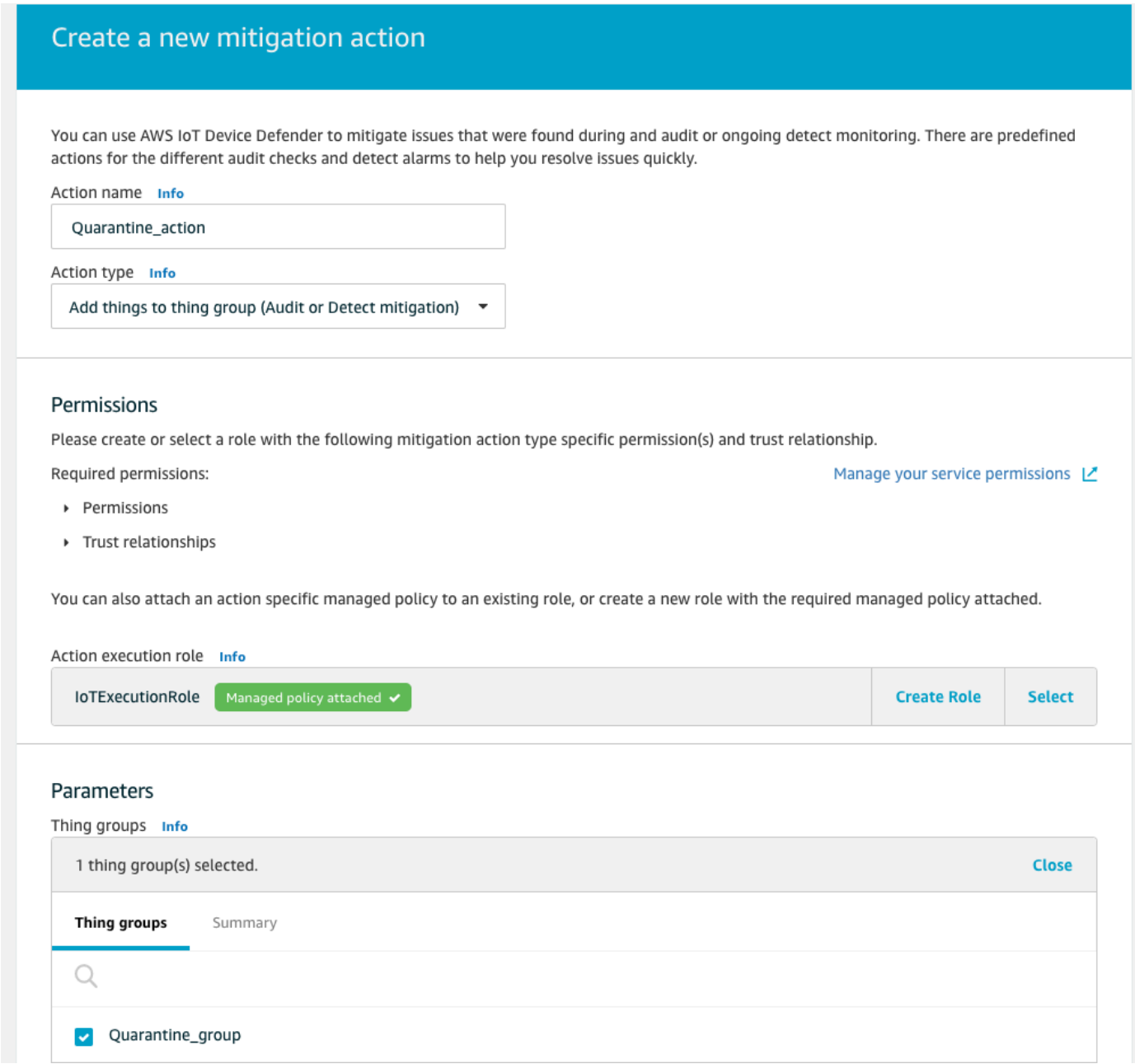
3. Ora che abbiamo creato un gruppo di oggetti, creiamo un'operazione di mitigazione che sposta i dispositivi in allarme nel `Quarantine_group`.

   In Defend (Protezione), Mitigation actions (Operazioni di mitigazione), scegli Create (Crea).



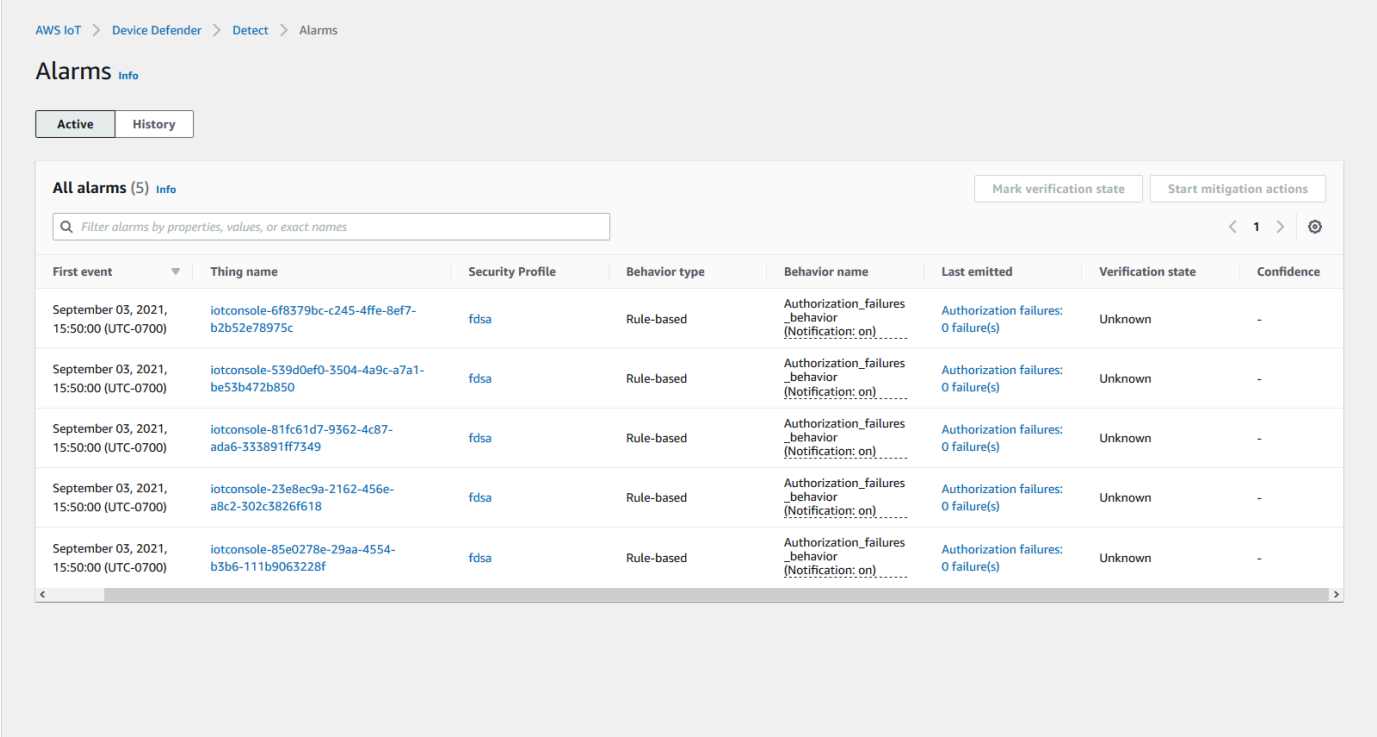
4. Sulla pagina Create a new mitigation action (Creare una nuova operazione di mitigazione) immetti le informazioni riportate di seguito.

   - Action name (Nome operazione): assegna un nome all'operazione di mitigazione, ad esempio **`Quarantine_action`**.
   - Action type (Tipo di operazione): scegli il tipo di operazione. Sceglieremo Add things to thing group (Audit or Detect mitigation) (Aggiungi oggetti al gruppo di oggetti (Audit o Rileva mitigazione).
   - Action execution role (Ruolo per l'esecuzione): crea un ruolo o scegli un ruolo esistente se è stato creato in precedenza.
   - Parameters (Parametri): scegli un gruppo di oggetti. Possiamo usare `Quarantine_group` che abbiamo creato in precedenza.



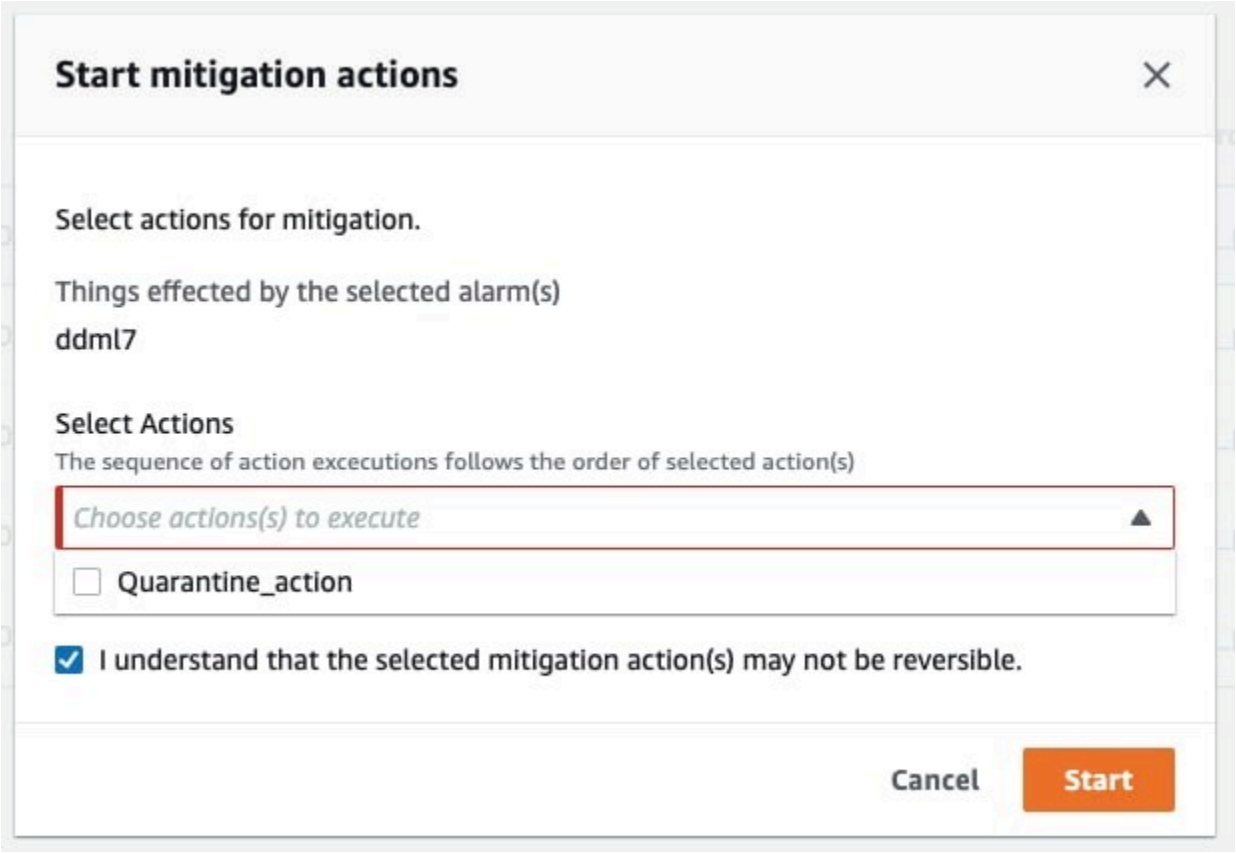
Una volta terminato, scegli Salva. Ora hai un'operazione di mitigazione che sposta i dispositivi in allarme in un gruppo di oggetti di quarantena e un'operazione di mitigazione per isolare il dispositivo durante l'indagine.

5. Accedi a Defender (Protezione), Detect (Rilevamento), Alarms (Allarmi). In Active (Attivo) puoi vedere quali dispositivi sono in stato di allarme.

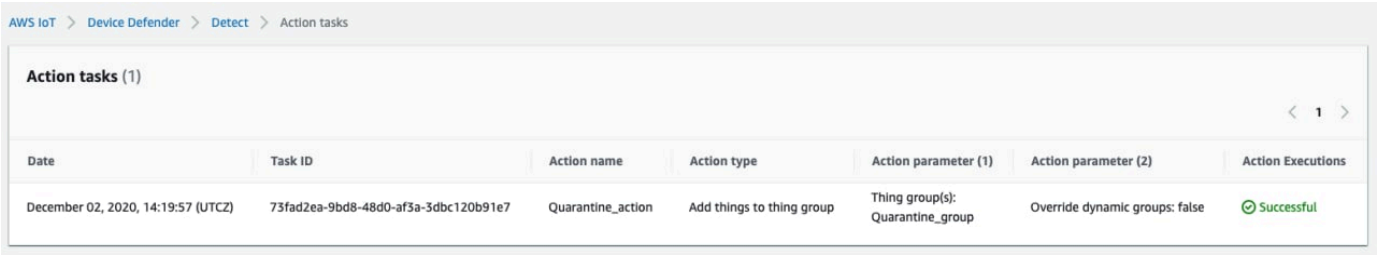


Seleziona il dispositivo che desideri spostare nel gruppo di quarantena e scegli Start Mitigation Actions (Avvia le operazioni di mitigazione).

6. In Start Mitigation Actions (Avvia le operazioni di mitigazione), Start Actions (Avvia operazioni) seleziona l'operazione di mitigazione creata in precedenza. Ad esempio prima sceglieremo **`Quarantine_action`**, poi Start (Avvio). Si apre la pagina Task delle operazioni.



7. Il dispositivo è ora isolato in **`Quarantine_group`** ed è inoltre possibile analizzare la causa principale del problema che ha attivato l'allarme. Dopo aver completato l'indagine, è possibile spostare il dispositivo fuori dal gruppo di oggetti o eseguire ulteriori operazioni.



Come utilizzare ML Detect con CLI

Di seguito viene mostrato come configurare ML Detect utilizzando la CLI.

Tutorial

- Abilita ML Detect
- Monitoraggio dello stato del modello ML

- Esamina gli allarmi ML Detect
- Ottimizzare gli allarmi ML
- Contrassegna lo stato di verifica dell'allarme
- Mitigazione dei problemi identificati sul dispositivo

Abilita ML Detect

La procedura seguente mostra come abilitare ML Detect nella AWS CLI.

1. Assicurati che i tuoi dispositivi creino i datapoint minimi richiesti come definito in ML Rileva i requisiti minimi per la formazione continua e il refresh del modello. Per far progredire la raccolta dei dati, assicurati che i tuoi oggetti si trovino in un gruppo di elementi collegato a un profilo di sicurezza.
2. Creare un profilo di protezione Rileva ML utilizzando il comando `create-security-profile`. Nell'esempio seguente viene creato un profilo di sicurezza denominato *`security-profile-for-smart-lights`* che controlla il numero di messaggi inviati, il numero di errori di autorizzazione, il numero di tentativi di connessione e il numero di disconnessioni. L'esempio utilizza `mlDetectionConfig` per stabilire che il parametro utilizzerà il modello ML Detect.

```
aws iot create-security-profile \
    --security-profile-name security-profile-for-smart-lights \
    --behaviors \
     '[{
    "name": "num-messages-sent-ml-behavior",
    "metric": "aws:num-messages-sent",
    "criteria": {
      "consecutiveDatapointsToAlarm": 1,
      "consecutiveDatapointsToClear": 1,
      "mlDetectionConfig": {
        "confidenceLevel": "HIGH"
      }
    },
    "suppressAlerts": true
  },
  {
    "name": "num-authorization-failures-ml-behavior",
    "metric": "aws:num-authorization-failures",
    "criteria": {
      "consecutiveDatapointsToAlarm": 1,
```

```
      "consecutiveDatapointsToClear": 1,
      "mlDetectionConfig": {
        "confidenceLevel": "HIGH"
      }
    },
    "suppressAlerts": true
  },
  {
    "name": "num-connection-attempts-ml-behavior",
    "metric": "aws:num-connection-attempts",
    "criteria": {
      "consecutiveDatapointsToAlarm": 1,
      "consecutiveDatapointsToClear": 1,
      "mlDetectionConfig": {
        "confidenceLevel": "HIGH"
      }
    },
    "suppressAlerts": true
  },
  {
    "name": "num-disconnects-ml-behavior",
    "metric": "aws:num-disconnects",
    "criteria": {
      "consecutiveDatapointsToAlarm": 1,
      "consecutiveDatapointsToClear": 1,
      "mlDetectionConfig": {
        "confidenceLevel": "HIGH"
      }
    },
    "suppressAlerts": true
  }]'
```

Output:

```
{
    "securityProfileName": "security-profile-for-smart-lights",
    "securityProfileArn": "arn:aws:iot:eu-
west-1:123456789012:securityprofile/security-profile-for-smart-lights"
  }
```

3. Associa ora il tuo profilo di sicurezza a uno o più gruppi di oggetti. Utilizzo dell'[attach-security-profile](#) per collegare un gruppo di oggetti al tuo profilo di sicurezza. L'esempio

seguente associa un gruppo di oggetti denominato *ML_Detect_beta_static_group* con il profilo di sicurezza *security-profile-for-smart-lights*.

```
aws iot attach-security-profile \
--security-profile-name security-profile-for-smart-lights \
--security-profile-target-arn arn:aws:iot:eu-
west-1:123456789012:thinggroup/ML_Detect_beta_static_group
```

Output:

Nessuna.

4. Dopo aver creato il profilo di sicurezza completo, il modello ML inizia la formazione. La formazione iniziale e la costruzione del modello ML richiedono 14 giorni per essere completate. Dopo 14 giorni, in caso di attività anomale sul tuo dispositivo, potrebbero comparire allarmi .

Monitoraggio dello stato del modello ML

Nella seguente procedura viene mostrato come monitorare i modelli di ML in corso di formazione.

- Utilizzo dell'`get-behavior-model-training-summaries` per visualizzare lo stato di avanzamento del modello ML. Nell'esempio seguente viene ottenuto il riepilogo dell'avanzamento della formazione del modello ML per il profilo di sicurezza *security-profile-for-smart-lights*. `modelStatus` indica se un modello ha completato la formazione o è ancora in attesa di compilazione per un particolare comportamento.

```
aws iot get-behavior-model-training-summaries \
   --security-profile-name security-profile-for-smart-lights
```

Output:

```
{
    "summaries": [
        {
            "securityProfileName": "security-profile-for-smart-lights",
            "behaviorName": "Messages_sent_ML_behavior",
            "trainingDataCollectionStartDate": "2020-11-30T14:00:00-08:00",
            "modelStatus": "ACTIVE",
            "datapointsCollectionPercentage": 29.408,
            "lastModelRefreshDate": "2020-12-07T14:35:19.237000-08:00"
```

```
        },
        {
            "securityProfileName": "security-profile-for-smart-lights",
            "behaviorName": "Messages_received_ML_behavior",
            "modelStatus": "PENDING_BUILD",
            "datapointsCollectionPercentage": 0.0
        },
        {
            "securityProfileName": "security-profile-for-smart-lights",
            "behaviorName": "Authorization_failures_ML_behavior",
            "trainingDataCollectionStartDate": "2020-11-30T14:00:00-08:00",
            "modelStatus": "ACTIVE",
            "datapointsCollectionPercentage": 35.464,
            "lastModelRefreshDate": "2020-12-07T14:29:44.396000-08:00"
        },
        {
            "securityProfileName": "security-profile-for-smart-lights",
            "behaviorName": "Message_size_ML_behavior",
            "trainingDataCollectionStartDate": "2020-11-30T14:00:00-08:00",
            "modelStatus": "ACTIVE",
            "datapointsCollectionPercentage": 29.332,
            "lastModelRefreshDate": "2020-12-07T14:30:44.113000-08:00"
        },
        {
            "securityProfileName": "security-profile-for-smart-lights",
            "behaviorName": "Connection_attempts_ML_behavior",
            "trainingDataCollectionStartDate": "2020-11-30T14:00:00-08:00",
            "modelStatus": "ACTIVE",
            "datapointsCollectionPercentage": 32.891999999999996,
            "lastModelRefreshDate": "2020-12-07T14:29:43.121000-08:00"
        },
        {
            "securityProfileName": "security-profile-for-smart-lights",
            "behaviorName": "Disconnects_ML_behavior",
            "trainingDataCollectionStartDate": "2020-11-30T14:00:00-08:00",
            "modelStatus": "ACTIVE",
            "datapointsCollectionPercentage": 35.46,
            "lastModelRefreshDate": "2020-12-07T14:29:55.556000-08:00"
        }
    ]
}
```

> **Note**
>
> Se il tuo modello non progredisce come previsto, assicurati che i tuoi dispositivi soddisfino il Requisiti minimi.

Esamina gli allarmi ML Detect

Dopo che i modelli ML sono stati creati e sono pronti per la valutazione dei dati, è possibile visualizzare regolarmente tutti gli allarmi che vengono dedotti dai modelli. La procedura seguente mostra come visualizzare gli allarmi nella AWS CLI.

- Per visualizzare tutti gli allarmi attivi, utilizza il comando `list-active-violations`.

```
aws iot list-active-violations \
--max-results 2
```

Output:

```
{
    "activeViolations": []
}
```

In alternativa, è possibile visualizzare tutte le violazioni rilevate durante un determinato periodo di tempo utilizzando il comando `list-violation-events`. L'esempio seguente elenca gli eventi di violazione dal 22 settembre 2020 alle ore 5:42:13 GMT, al 26 ottobre 2020 alle ore 5:42:13 GMT.

```
aws iot list-violation-events \
    --start-time 1599500533 \
    --end-time 1600796533 \
    --max-results 2
```

Output:

```
{
    "violationEvents": [
        {
            "violationId": "1448be98c09c3d4ab7cb9b6f3ece65d6",
```

```
            "thingName": "lightbulb-1",
            "securityProfileName": "security-profile-for-smart-lights",
            "behavior": {
                "name": "LowConfidence_MladBehavior_MessagesSent",
                "metric": "aws:num-messages-sent",
                "criteria": {
                    "consecutiveDatapointsToAlarm": 1,
                    "consecutiveDatapointsToClear": 1,
                    "mlDetectionConfig": {
                        "confidenceLevel": "HIGH"
                    }
                },
                "suppressAlerts": true
            },
            "violationEventType": "alarm-invalidated",
            "violationEventTime": 1600780245.29
        },
        {
            "violationId": "df4537569ef23efb1c029a433ae84b52",
            "thingName": "lightbulb-2",
            "securityProfileName": "security-profile-for-smart-lights",
            "behavior": {
                "name": "LowConfidence_MladBehavior_MessagesSent",
                "metric": "aws:num-messages-sent",
                "criteria": {
                    "consecutiveDatapointsToAlarm": 1,
                    "consecutiveDatapointsToClear": 1,
                    "mlDetectionConfig": {
                        "confidenceLevel": "HIGH"
                    }
                },
                "suppressAlerts": true
            },
            "violationEventType": "alarm-invalidated",
            "violationEventTime": 1600780245.281
        }
    ],
    "nextToken":
 "Amo6XIUrsOohsojuIG6TuwSR3X9iUvH2OCksBZg6bed2j21VSnD1uP1pflxKX1+a3cvBRSosIB0xFv40kM6RYBknZ
vxabMe/ZW31Ps/WiZHlr9Wg7R7eEGli59IJ/U0iBQ1McP/ht0E2XA2TTIvYeMmKQQPsRj/
eoV9j7P/wveu7skNGepU/mvpV0O2Ap7hnV5U+Prx/9+iJA/341va
+pQww7jpUeHmJN9Hw4MqW0ysw0Ry3w38hOQWEpz2xwFWAxAARxeIxCxt5c37RK/lRZBlhYqoB
+w2PZ74730h8pICGY4gktJxkwHyyRabpSM/G/f5DFrD9O5v8idkTZzBxW2jrbzSUIdafPtsZHL/
yAMKr3HAKtaABz2nTsOBNre7X2d/jIjjarhon0Dh9l+8I9Y5Ey
```

```
+DIFBcqFTvhibKAafQt3gs6CUiqHdWiCenfJyb8whmDE2qxvdxGElGmRb
+k6kuN5jrZxxw95gzfYDgRHv11iEn8h1qZLD0czkIFBpMppHj9cetHPvM
+qffXGAzKi8tL6eQuCdMLXmVE3jbqcJcjk9ItnaYJi5zKDz9FVbrz9qZZPtZJFHp"
}
```

Ottimizzare gli allarmi ML

Una volta che i modelli ML sono stati creati e sono pronti per la valutazione dei dati, è possibile aggiornare le impostazioni di comportamento ML del profilo di sicurezza per modificare la configurazione. La procedura seguente mostra come aggiornare le impostazioni di comportamento ML del profilo di sicurezza nell'AWS CLI.

- Per modificare le impostazioni del comportamento ML del tuo profilo di sicurezza, usa il comando `update-security-profile`. Nell'esempio seguente viene aggiornata i comportamenti del profilo di sicurezza *`security-profile-for-smart-lights`* modificando il `confidenceLevel` di alcuni dei comportamenti senza sopprimere le notifiche per tutti i comportamenti.

```
aws iot update-security-profile \
    --security-profile-name security-profile-for-smart-lights \
    --behaviors \
     '[{
      "name": "num-messages-sent-ml-behavior",
      "metric": "aws:num-messages-sent",
      "criteria": {
          "mlDetectionConfig": {
              "confidenceLevel" : "HIGH"
          }
      },
      "suppressAlerts": false
  },
  {
      "name": "num-authorization-failures-ml-behavior",
      "metric": "aws:num-authorization-failures",
      "criteria": {
          "mlDetectionConfig": {
              "confidenceLevel" : "HIGH"
          }
      },
      "suppressAlerts": false
  },
```

```
  {
      "name": "num-connection-attempts-ml-behavior",
      "metric": "aws:num-connection-attempts",
      "criteria": {
          "mlDetectionConfig": {
              "confidenceLevel" : "HIGH"
          }
      },
      "suppressAlerts": false
  },
  {
      "name": "num-disconnects-ml-behavior",
      "metric": "aws:num-disconnects",
      "criteria": {
          "mlDetectionConfig": {
              "confidenceLevel" : "LOW"
          }
      },
      "suppressAlerts": false

  }]'
```

Output:

```
 {
    "securityProfileName": "security-profile-for-smart-lights",
    "securityProfileArn": "arn:aws:iot:eu-
west-1:123456789012:securityprofile/security-profile-for-smart-lights",
    "behaviors": [
        {
            "name": "num-messages-sent-ml-behavior",
            "metric": "aws:num-messages-sent",
            "criteria": {
                "mlDetectionConfig": {
                    "confidenceLevel": "HIGH"
                }
            }
        },
        {
            "name": "num-authorization-failures-ml-behavior",
            "metric": "aws:num-authorization-failures",
            "criteria": {
                "mlDetectionConfig": {
```

```
                    "confidenceLevel": "HIGH"
                }
            }
        },
        {
            "name": "num-connection-attempts-ml-behavior",
            "metric": "aws:num-connection-attempts",
            "criteria": {
                "mlDetectionConfig": {
                    "confidenceLevel": "HIGH"
                }
            },
            "suppressAlerts": false
        },
        {
            "name": "num-disconnects-ml-behavior",
            "metric": "aws:num-disconnects",
            "criteria": {
                "mlDetectionConfig": {
                    "confidenceLevel": "LOW"
                }
            },
            "suppressAlerts": true
        }
    ],
    "version": 2,
    "creationDate": 1600799559.249,
    "lastModifiedDate": 1600800516.856
}
```

Contrassegna lo stato di verifica dell'allarme

Puoi contrassegnare gli allarmi con gli stati di verifica come aiuto nella classificazione degli allarmi e nella verifica di anomalie.

- Contrassegna i tuoi allarmi con uno stato di verifica e una descrizione di tale stato. Ad esempio, per impostare lo stato di verifica di un allarme su False positive (Falso positivo), utilizzare il seguente comando:

```
aws iot put-verification-state-on-violation --violation-id 12345  --verification-
state FALSE_POSITIVE --verification-state-description "This is dummy description"
 --endpoint https://us-east-1.iot.amazonaws.com --region us-east-1
```

Output:

Nessuna.

Mitigazione dei problemi identificati sul dispositivo

1. Utilizzo dell'create-thing-group per creare un gruppo di oggetti per l'operazione di mitigazione. Nell'esempio seguente, creiamo un gruppo di oggetti chiamato ThingGroupForDetectMitigationAction.

   ```
   aws iot create-thing-group –thing-group-name ThingGroupForDetectMitigationAction
   ```

   Output:

   ```
   {
    "thingGroupName": "ThingGroupForDetectMitigationAction",
    "thingGroupArn": "arn:aws:iot:us-
   east-1:123456789012:thinggroup/ThingGroupForDetectMitigationAction",
    "thingGroupId": "4139cd61-10fa-4c40-b867-0fc6209dca4d"
   }
   ```

2. In seguito utilizza il comando create-mitigation-action per creare un'operazione di mitigazione. Nell'esempio seguente viene creata un'operazione di mitigazione denominata detect_mitigation_action con l'ARN del ruolo IAM utilizzato per accedere all'operazione di mitigazione. Definiamo il tipo di operazione e i parametri per tale operazione. In questo caso, la nostra mitigazione sposterà le cose nel nostro gruppo di oggetti chiamato ThingGroupForDetectMitigationAction, creato in precedenza.

   ```
   aws iot create-mitigation-action --action-name detect_mitigation_action \
   --role-arn arn:aws:iam::123456789012:role/MitigationActionValidRole \
   --action-params \
   '{
       "addThingsToThingGroupParams": {
           "thingGroupNames": ["ThingGroupForDetectMitigationAction"],
   ```

```
        "overrideDynamicGroups": false
    }
}'
```

Output:

```
{
 "actionArn": "arn:aws:iot:us-
east-1:123456789012:mitigationaction/detect_mitigation_action",
 "actionId": "5939e3a0-bf4c-44bb-a547-1ab59ffe67c3"
}
```

3. Utilizza il comando [start-detect-mitigation-actions-task](#) per avviare le operazioni di mitigazione. `task-id`, `target` e `actions` sono parametri obbligatori.

```
aws iot start-detect-mitigation-actions-task \
    --task-id taskIdForMitigationAction \
    --target '{ "violationIds" : [ "violationId-1", "violationId-2" ] }' \
    --actions "detect_mitigation_action" \
    --include-only-active-violations \
    --include-suppressed-alerts
```

Output:

```
{
    "taskId": "taskIdForMitigationAction"
}
```

4. (Facoltativo) Per visualizzare le esecuzioni delle operazioni di mitigazione incluse in un'attività, utilizza il comando [list-detect-mitigation-actions-executions](#).

```
aws iot list-detect-mitigation-actions-executions \
    --task-id taskIdForMitigationAction \
    --max-items 5 \
    --page-size 4
```

Output:

```
{
    "actionsExecutions": [
        {
```

```
            "taskId": "e56ee95e - f4e7 - 459 c - b60a - 2701784290 af",
            "violationId": "214_fe0d92d21ee8112a6cf1724049d80",
            "actionName": "underTest_MAThingGroup71232127",
            "thingName": "cancelDetectMitigationActionsTaskd143821b",
            "executionStartDate": "Thu Jan 07 18: 35: 21 UTC 2021",
            "executionEndDate": "Thu Jan 07 18: 35: 21 UTC 2021",
            "status": "SUCCESSFUL",
        }
    ]
}
```

5. (Facoltativo) Utilizza il [describe-detect-mitigation-actions-task] per ottenere informazioni su un'operazione di mitigazione.

```
aws iot describe-detect-mitigation-actions-task \
    --task-id taskIdForMitigationAction
```

Output:

```
{
    "taskSummary": {
        "taskId": "taskIdForMitigationAction",
        "taskStatus": "SUCCESSFUL",
        "taskStartTime": 1609988361.224,
        "taskEndTime": 1609988362.281,
        "target": {
            "securityProfileName": "security-profile-for-smart-lights",
            "behaviorName": "num-messages-sent-ml-behavior"
        },
        "violationEventOccurrenceRange": {
            "startTime": 1609986633.0,
            "endTime": 1609987833.0
        },
        "onlyActiveViolationsIncluded": true,
        "suppressedAlertsIncluded": true,
        "actionsDefinition": [
            {
                "name": "detect_mitigation_action",
                "id": "5939e3a0-bf4c-44bb-a547-1ab59ffe67c3",
                "roleArn":
 "arn:aws:iam::123456789012:role/MitigatioActionValidRole",
                "actionParams": {
                    "addThingsToThingGroupParams": {
```

```
                        "thingGroupNames": [
                            "ThingGroupForDetectMitigationAction"
                        ],
                        "overrideDynamicGroups": false
                    }
                }
            }
        ],
        "taskStatistics": {
            "actionsExecuted": 0,
            "actionsSkipped": 0,
            "actionsFailed": 0
        }
    }
}
```

6. (Facoltativo) Per ottenere un elenco delle attività relative alle operazioni di mitigazione, utilizza il comando [list-detect-mitigation-actions-tasks](#).

```
aws iot list-detect-mitigation-actions-tasks \
    --start-time 1609985315 \
    --end-time 1609988915 \
    --max-items 5 \
    --page-size 4
```

Output:

```
{
    "tasks": [
        {
            "taskId": "taskIdForMitigationAction",
            "taskStatus": "SUCCESSFUL",
            "taskStartTime": 1609988361.224,
            "taskEndTime": 1609988362.281,
            "target": {
                "securityProfileName": "security-profile-for-smart-lights",
                "behaviorName": "num-messages-sent-ml-behavior"
            },
            "violationEventOccurrenceRange": {
                "startTime": 1609986633.0,
                "endTime": 1609987833.0
            },
            "onlyActiveViolationsIncluded": true,
```

```
            "suppressedAlertsIncluded": true,
            "actionsDefinition": [
                {
                    "name": "detect_mitigation_action",
                    "id": "5939e3a0-bf4c-44bb-a547-1ab59ffe67c3",
                    "roleArn": "arn:aws:iam::123456789012:role/
MitigatioActionValidRole",
                    "actionParams": {
                        "addThingsToThingGroupParams": {
                            "thingGroupNames": [
                                "ThingGroupForDetectMitigationAction"
                            ],
                            "overrideDynamicGroups": false
                        }
                    }
                }
            ],
            "taskStatistics": {
                "actionsExecuted": 0,
                "actionsSkipped": 0,
                "actionsFailed": 0
            }
        }
    ]
}
```

7. (Facoltativo) Per annullare un'attività delle operazioni di attenuazione, utilizza il comando [cancel-detect-mitigation-actions-task](#).

```
aws iot cancel-detect-mitigation-actions-task \
    --task-id taskIdForMitigationAction
```

Output:

Nessuna.

Personalizzare quando e come visualizzare i risultati dell'audit AWS IoT Device Defender

AWS IoT Device Defender audit fornisce controlli periodici di sicurezza per confermare che i dispositivi AWS IoT e le risorse stiano seguendo le best practice. Per ogni controllo, i risultati di audit

vengono classificati come conformi o non conformi, dove la non conformità risulta nelle icone di avviso della console. Per ridurre il rumore causato dalla ripetizione di problemi noti, la funzione di soppressione della ricerca di audit consente di disattivare temporaneamente queste notifiche di non conformità.

È possibile eliminare i controlli di audit selezionati per una risorsa o un account specifico per un periodo di tempo predeterminato. Un risultato del controllo audit che è stato eliminato viene classificato come risultato soppresso, separato dalle categorie conformi e non conformi. Questa nuova categoria non attiva un allarme come un risultato non conforme. Ciò consente di ridurre i disturbi delle notifiche di non conformità durante i periodi di manutenzione noti, o fino al completamento di un aggiornamento.

Nozioni di base

Nelle sezioni seguenti viene descritto come utilizzare le soppressioni per la ricerca di audit per sopprimere un controllo `Device certificate expiring` nella console e nell'interfaccia a riga di comando. Se desideri seguire una delle dimostrazioni, devi prima creare due certificati in scadenza per Device Defender che possano essere rilevati.

Consulta le informazioni riportate di seguito per creare i tuoi certificati.

- Create and register a CA certificate nella Guida per gli sviluppatori di AWS IoT Core.
- Creare un certificato client utilizzando il certificato CA. Nel passaggio 3, imposta il tuo parametro `days` di **1**.

Se utilizzi l'interfaccia a riga di comando per creare i certificati, immetti il comando seguente.

```
openssl x509 -req \
    -in device_cert_csr_filename \
    -CA root_ca_pem_filename \
    -CAkey root_ca_key_filename \
    -CAcreateserial \
    -out device_cert_pem_filename \
    -days 1 -sha256
```

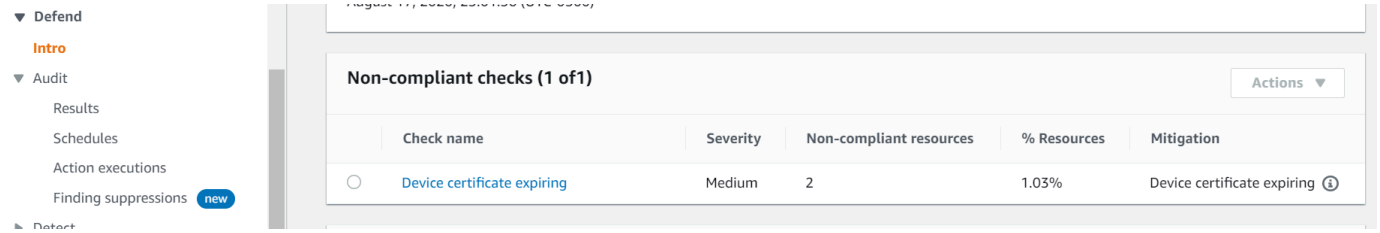
Personalizzare i risultati di audit nella console

Nella procedura dettagliata seguente viene utilizzato un account con due certificati di dispositivo scaduti che attivano un controllo di audit non conforme. In questo scenario, vogliamo disabilitare

l'avviso perché i nostri sviluppatori stanno testando una nuova funzionalità che risolverà il problema. Creiamo una soppressione per ogni certificato per impedire che il risultato di audit non sia conforme per la settimana successiva.

1. Verrà innanzitutto eseguito un audit su richiesta per dimostrare che il controllo del certificato del dispositivo scaduto non è conforme.

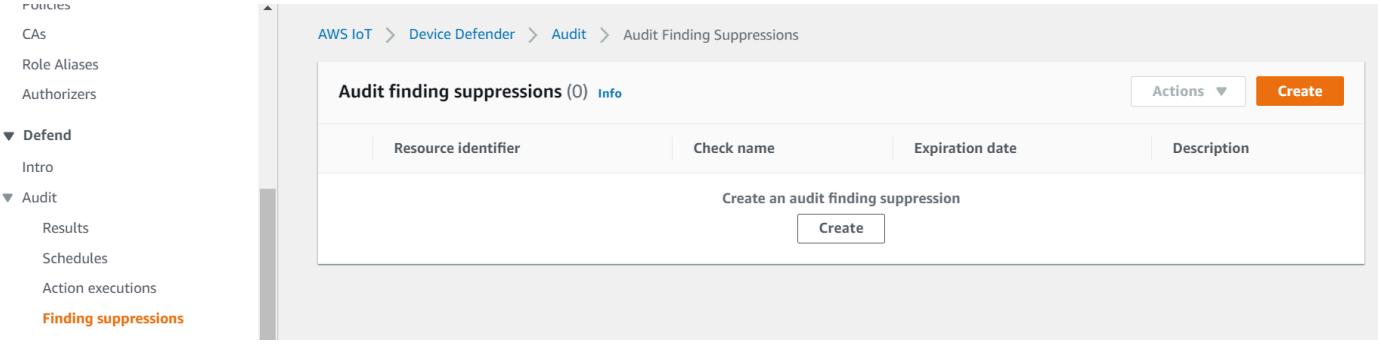
   Dall'AWS IoT console, scegli Defend (Protezione) dalla barra laterale sinistra, quindi Audit (Controllo), e Results (Risultati). Sulla pagina Audit Results (Risultati della verifica), scegli Create (Crea). Si aprirà la finestra Create new audit (Crea nuovo audit). Scegli Create (Crea).



   Dai risultati di audit su richiesta, possiamo vedere che "Certificato dispositivo in scadenza" non è conforme per due risorse.

2. Ora, vorremmo disabilitare l'avviso di controllo non conforme "Certificato dispositivo in scadenza" perché i nostri sviluppatori stanno testando nuove funzionalità che correggeranno l'avviso.

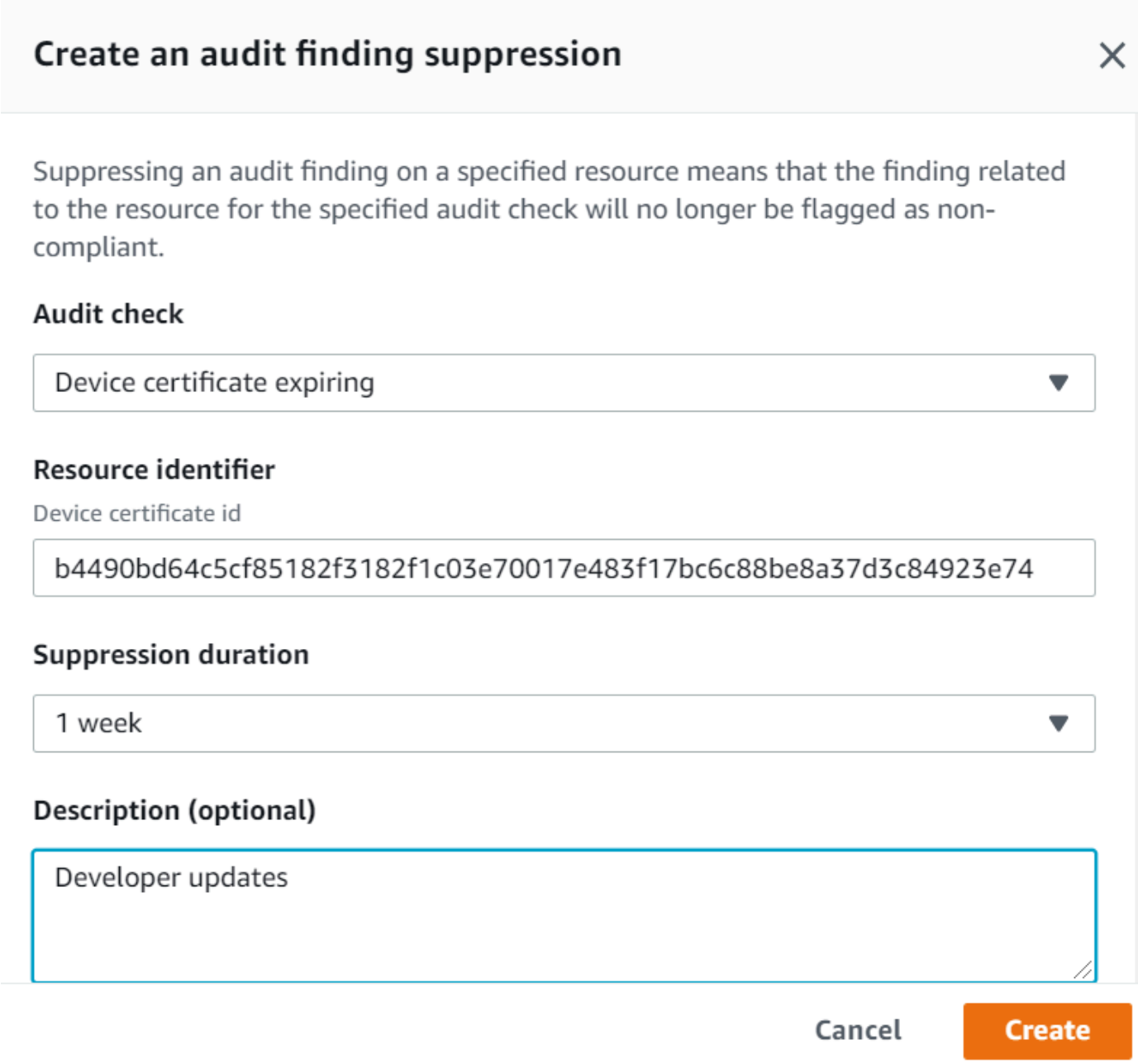
   Dalla barra laterale sinistra sotto Defender (Protezione), scegli Audit (Audit) e quindi scegli Finding suppressions (Ricerca di eliminazioni). Sulla pagina Audit finding suppressions (Verifica delle soppressioni di audit), scegli Create (Crea).



3. Sulla finestra Create an audit finding suppression (Crea una soppressione della ricerca di audit), dobbiamo compilare quanto segue.

   - Audit check (Controllo di audit): selezioniamo `Device certificate expiring`, perché questo è il controllo di audit che vorremmo sopprimere.

- Resource identifier (Identificatore di risorsa): inseriamo l'ID del certificato del dispositivo di uno dei certificati per cui vorremmo eliminare i risultati del audit.
- Suppression duration (Durata dell'eliminazione): selezioniamo `1 week`, perché è per quanto tempo vorremmo sopprimere il controllo audit `Device certificate expiring`.
- Description (Descrizione) (facoltativa): aggiungiamo una nota che descrive il motivo per cui stiamo sopprimendo questa ricerca di audit.

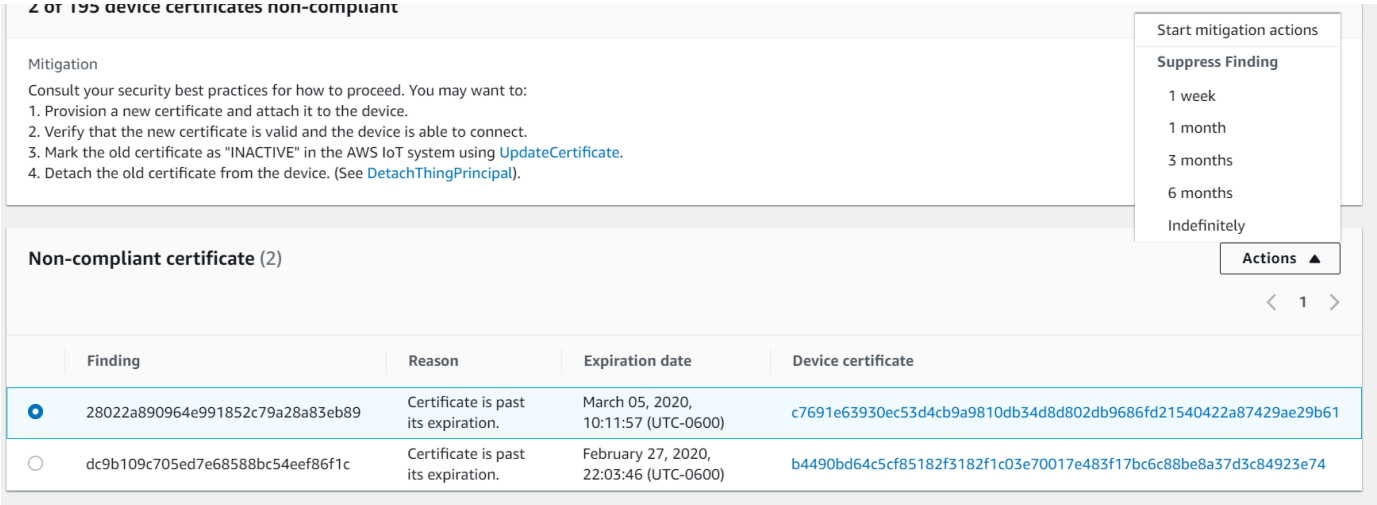


Dopo che abbiamo riempito i campi, scegli Create (Crea). Viene visualizzato un banner di successo dopo che è stata creata la soppressione del rilevamento di audit.

4. Abbiamo soppresso una ricerca di audit per uno dei certificati e ora abbiamo bisogno di sopprimere la ricerca di audit per il secondo certificato. Potremmo usare lo stesso metodo di soppressione che abbiamo usato nel passaggio 3, ma useremo un metodo diverso per scopi dimostrativi.

   Dalla barra laterale sinistra sotto Difender (Protezione), scegli Audit (Audit), quindi Results (Risultati). Sulla pagina Audit results (Risultati di audit) scegli l'audit con la risorsa non conforme. Quindi, seleziona la risorsa in Non-compliant checks (Controlli non conformi). Nel nostro caso, selezioniamo "Certificato dispositivo in scadenza".

5. Sulla pagina Device certificate expiring (Certificato del dispositivo in scadenza), sotto Non-compliant policy (Policy non conforme) scegli il pulsante di opzione accanto al risultato da eliminare. Quindi, seleziona Actions (Operazioni) e scegli la durata per la quale desideri che venga soppressa. Nel nostro caso, scegliamo `1 week` come abbiamo fatto per l'altro certificato. Sulla finestra Confirm suppression (Conferma eliminazione), scegli Enable suppression (Abilitazione dell'eliminazione).



Viene visualizzato un banner di successo dopo che è stata creata la soppressione del rilevamento di audit. Ora, entrambi i risultati dell'audit sono stati soppressi per 1 settimana, mentre i nostri sviluppatori lavorano su una soluzione per risolvere l'avviso.

Personalizzare i risultati dell'audit nell'interfaccia a riga di comando

Nella procedura dettagliata seguente viene utilizzato un account con un certificato di dispositivo scaduto che attiva un controllo audit non conforme. In questo scenario, vogliamo disabilitare l'avviso perché i nostri sviluppatori stanno testando una nuova funzionalità che risolverà il problema. Creiamo una soppressione del rilevamento di audit per il certificato per impedire che il risultato dell'audit non sia conforme per la settimana successiva.

Utilizza i seguenti comandi dell'interfaccia a riga di comando.

- create-audit-suppression
- describe-audit-suppression
- update-audit-suppression
- delete-audit-suppression
- list-audit-suppressions

1. Utilizza il seguente comando per abilitare l'audit.

   ```
   aws iot update-account-audit-configuration \
      --audit-check-configurations "{\"DEVICE_CERTIFICATE_EXPIRING_CHECK\":{\"enabled
   \":true}}"
   ```

   Output:

   Nessuna.

2. Utilizza il comando seguente per eseguire l'audit on demand che sia destinato al controllo di audit `DEVICE_CERTIFICATE_EXPIRING_CHECK`.

   ```
   aws iot start-on-demand-audit-task \
       --target-check-names DEVICE_CERTIFICATE_EXPIRING_CHECK
   ```

   Output:

   ```
   {
       "taskId": "787ed873b69cb4d6cdbae6ddd06996c5"
   }
   ```

3. Utilizza il comando describe-account-audit-configuration per descrivere la configurazione dell'audit. Vogliamo confermare che abbiamo attivato il controllo di audit per `DEVICE_CERTIFICATE_EXPIRING_CHECK`.

```
aws iot describe-account-audit-configuration
```

Output:

```
{
    "roleArn": "arn:aws:iam::<accountid>:role/service-role/project",
    "auditNotificationTargetConfigurations": {
        "SNS": {
            "targetArn": "arn:aws:sns:us-east-1:<accountid>:project_sns",
            "roleArn": "arn:aws:iam::<accountid>:role/service-role/project",
            "enabled": true
        }
    },
    "auditCheckConfigurations": {
        "AUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK": {
            "enabled": false
        },
        "CA_CERTIFICATE_EXPIRING_CHECK": {
            "enabled": false
        },
        "CA_CERTIFICATE_KEY_QUALITY_CHECK": {
            "enabled": false
        },
        "CONFLICTING_CLIENT_IDS_CHECK": {
            "enabled": false
        },
        "DEVICE_CERTIFICATE_EXPIRING_CHECK": {
            "enabled": true
        },
        "DEVICE_CERTIFICATE_KEY_QUALITY_CHECK": {
            "enabled": false
        },
        "DEVICE_CERTIFICATE_SHARED_CHECK": {
            "enabled": false
        },
        "IOT_POLICY_OVERLY_PERMISSIVE_CHECK": {
            "enabled": true
```

```
        },
        "IOT_ROLE_ALIAS_ALLOWS_ACCESS_TO_UNUSED_SERVICES_CHECK": {
            "enabled": false
        },
        "IOT_ROLE_ALIAS_OVERLY_PERMISSIVE_CHECK": {
            "enabled": false
        },
        "LOGGING_DISABLED_CHECK": {
            "enabled": false
        },
        "REVOKED_CA_CERTIFICATE_STILL_ACTIVE_CHECK": {
            "enabled": false
        },
        "REVOKED_DEVICE_CERTIFICATE_STILL_ACTIVE_CHECK": {
            "enabled": false
        },
        "UNAUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK": {
            "enabled": false
        }
    }
}
```

`DEVICE_CERTIFICATE_EXPIRING_CHECK` dovrebbe avere un valore di `true`.

4. Utilizza il comando list-audit-task per identificare le attività di audit completate.

```
aws iot list-audit-tasks \
    --task-status "COMPLETED" \
    --start-time 2020-07-31 \
    --end-time 2020-08-01
```

Output:

```
{
    "tasks": [
        {
            "taskId": "787ed873b69cb4d6cdbae6ddd06996c5",
            "taskStatus": "COMPLETED",
            "taskType": "SCHEDULED_AUDIT_TASK"
        }
    ]
}
```

Il `taskId` dell'audit eseguito nel passaggio 1 dovrebbe avere un `taskStatus` di `COMPLETED`.

5. Utilizza il comando describe-audit-task per ottenere informazioni dettagliate sull'audit completato tramite l'output `taskId` dal passaggio precedente. Questo comando elenca i dettagli relativi all'audit.

```
aws iot describe-audit-task \
    --task-id "787ed873b69cb4d6cdbae6ddd06996c5"
```

Output:

```
{
    "taskStatus": "COMPLETED",
    "taskType": "SCHEDULED_AUDIT_TASK",
    "taskStartTime": 1596168096.157,
    "taskStatistics": {
        "totalChecks": 1,
        "inProgressChecks": 0,
        "waitingForDataCollectionChecks": 0,
        "compliantChecks": 0,
        "nonCompliantChecks": 1,
        "failedChecks": 0,
        "canceledChecks": 0
    },
    "scheduledAuditName": "AWSIoTDeviceDefenderDailyAudit",
    "auditDetails": {
        "DEVICE_CERTIFICATE_EXPIRING_CHECK": {
            "checkRunStatus": "COMPLETED_NON_COMPLIANT",
            "checkCompliant": false,
            "totalResourcesCount": 195,
            "nonCompliantResourcesCount": 2
        }
    }
}
```

6. Utilizza il comando list-audit-findings per trovare l'ID certificato non conforme in modo da poter sospendere gli avvisi di audit per questa risorsa.

```
aws iot list-audit-findings \
    --start-time 2020-07-31 \
    --end-time 2020-08-01
```

Output:


```
{
    "findings": [
        {
            "findingId": "296ccd39f806bf9d8f8de20d0ceb33a1",
            "taskId": "787ed873b69cb4d6cdbae6ddd06996c5",
            "checkName": "DEVICE_CERTIFICATE_EXPIRING_CHECK",
            "taskStartTime": 1596168096.157,
            "findingTime": 1596168096.651,
            "severity": "MEDIUM",
            "nonCompliantResource": {
                "resourceType": "DEVICE_CERTIFICATE",
                "resourceIdentifier": {
                    "deviceCertificateId": "b4490<shortened>"
                },
                "additionalInfo": {
                "EXPIRATION_TIME": "1582862626000"
                }
            },
            "reasonForNonCompliance": "Certificate is past its expiration.",
            "reasonForNonComplianceCode": "CERTIFICATE_PAST_EXPIRATION",
            "isSuppressed": false
        },
        {
            "findingId": "37ecb79b7afb53deb328ec78e647631c",
            "taskId": "787ed873b69cb4d6cdbae6ddd06996c5",
            "checkName": "DEVICE_CERTIFICATE_EXPIRING_CHECK",
            "taskStartTime": 1596168096.157,
            "findingTime": 1596168096.651,
            "severity": "MEDIUM",
            "nonCompliantResource": {
                "resourceType": "DEVICE_CERTIFICATE",
                "resourceIdentifier": {
                    "deviceCertificateId": "c7691<shortened>"
                },
                "additionalInfo": {
                "EXPIRATION_TIME": "1583424717000"
                }
            },
            "reasonForNonCompliance": "Certificate is past its expiration.",
            "reasonForNonComplianceCode": "CERTIFICATE_PAST_EXPIRATION",
            "isSuppressed": false
```

```
        }
    ]
}
```

7. Utilizza il comando create-audit-suppression per sopprimere le notifiche per il controllo di audit `DEVICE_CERTIFICATE_EXPIRING_CHECK` per un certificato di dispositivo con l'id *c7691e<shortened>* fino al *20-08-2020*.

```
aws iot create-audit-suppression \
    --check-name DEVICE_CERTIFICATE_EXPIRING_CHECK \
    --resource-identifier deviceCertificateId="c7691e<shortened>" \
    --no-suppress-indefinitely \
    --expiration-date 2020-08-20
```

8. Utilizza il comando list-audit-suppression per confermare l'impostazione di soppressione del controllo e ottenere dettagli sulla soppressione.

```
aws iot list-audit-suppressions
```

Output:

```
{
    "suppressions": [
        {
        "checkName": "DEVICE_CERTIFICATE_EXPIRING_CHECK",
            "resourceIdentifier": {
                "deviceCertificateId": "c7691e<shortened>"
            },
        "expirationDate": 1597881600.0,
        "suppressIndefinitely": false
        }
    ]
}
```

9. Il comando update-audit-suppression può essere utilizzato per aggiornare la soppressione della ricerca di controllo. L'esempio seguente aggiorna `expiration-date` a `08/21/20`.

```
aws iot update-audit-suppression \
    --check-name DEVICE_CERTIFICATE_EXPIRING_CHECK \
    --resource-identifier deviceCertificateId=c7691e<shortened> \
    --no-suppress-indefinitely \
```

```
    --expiration-date 2020-08-21
```

10. Il comando delete-audit-suppression può essere utilizzato per rimuovere una soppressione della ricerca di audit.

```
aws iot delete-audit-suppression \
    --check-name DEVICE_CERTIFICATE_EXPIRING_CHECK \
    --resource-identifier deviceCertificateId="c7691e<shortened>"
```

Per confermare l'eliminazione, utilizza il comando list-audit-suppressions.

```
aws iot list-audit-suppressions
```

Output:

```
{
 "suppressions": []
}
```

In questo tutorial, ti abbiamo mostrato come sopprimere un controllo `Device certificate expiring` nella console e nell'interfaccia a riga di comando. Per ulteriori informazioni sul controllo per individuare le soppressioni, consulta Soppressioni della ricerca di audit

Audit

Un audit di AWS IoT Device Defender analizza le impostazioni e le policy correlate ad account e dispositivi per garantire l'applicazione delle misure di sicurezza. Un audit può aiutarti a individuare eventuali scostamenti dalle best practice di sicurezza o policy di accesso adeguate, come nel caso di più dispositivi che usano la stessa identità, o policy troppo permissive che consentono a un dispositivo di leggere e aggiornare i dati per molti altri dispositivi. È possibile eseguire audit in base alle necessità (audit on demand) oppure pianificarli per l'esecuzione periodica (audit pianificati).

Un audit di AWS IoT Device Defender esegue un set di controlli predefiniti relativi a vulnerabilità dei dispositivi e best practice di sicurezza IoT comuni. Tra i controlli predefiniti vi sono le policy che concedono l'autorizzazione per leggere o aggiornare i dati in più dispositivi, i dispositivi che condividono un'identità (certificato X.509) o i certificati in scadenza o che sono stati revocati ma sono ancora attivi.

Gravità del problema

La gravità del problema indica il livello di preoccupazione associato a ciascuna istanza identificata di non conformità e il tempo consigliato per la correzione.

Critico

I controlli di audit non conformi con questa gravità identificano i problemi che richiedono attenzione urgente. I problemi critici spesso consentono agli attori cattivi con poca sofisticazione e nessuna conoscenza privilegiata o credenziali speciali di ottenere facilmente l'accesso o il controllo delle tue risorse.

Elevata

I controlli di audit non conformi con questa gravità richiedono un'indagine urgente e una pianificazione delle correzioni a seguito della risoluzione di problemi critici. Come i problemi critici, i problemi di elevata gravità spesso forniscono agli attori cattivi l'accesso o il controllo delle risorse. Tuttavia, i problemi di elevata gravità sono spesso più difficili da sfruttare. Potrebbero richiedere strumenti speciali, conoscenze privilegiate o configurazioni specifiche.

Media

I controlli di audit non conformi con questa gravità presentano problemi che richiedono attenzione, sempre nell'ambito della manutenzione continua della posizione di sicurezza. Problemi di gravità

media potrebbero causare un impatto operativo negativo, ad esempio interruzioni non pianificate a causa di malfunzionamento dei controlli di sicurezza. Questi problemi potrebbero anche fornire agli attori cattivi l'accesso o il controllo limitato delle risorse o potrebbero facilitare parti delle loro azioni dannose.

Bassa

I controlli di audit non conformi con questo livello di gravità spesso indicano che le procedure di sicurezza consigliate sono state ignorate. Anche se potrebbero non causare un impatto immediato sulla sicurezza da soli, questi errori possono essere sfruttati da attori cattivi. Come i problemi di gravità media, i problemi di bassa gravità richiedono attenzione come parte della manutenzione continua della postura di sicurezza.

Passaggi successivi

Per comprendere i tipi di controlli di auditing che possono essere eseguiti, consultare Controlli di auditing. Per informazioni sulle quote di servizio applicabili agli audit, consulta la sezione Service Quotas.

Controlli di auditing

> **Note**
>
> Quando si attiva un controllo, la raccolta dei dati viene avviata immediatamente. Se nell'account è presente una quantità elevata di dati da raccogliere, i risultati del controllo potrebbero non essere disponibili per alcuni minuti dopo l'abilitazione.

Sono supportati i controlli di auditing seguenti:

- CA intermedia revocata per il controllo attivo dei certificati del dispositivo
- Certificato CA revocato ancora attivo
- Certificato del dispositivo condiviso
- Qualità della chiave del certificato del dispositivo
- Qualità della chiave del certificato emesso da una CA
- Ruolo Cognito non autenticato eccessivamente permissivo

- Ruolo Cognito autenticato eccessivamente permissivo
- Policy eccessivamente permissive di AWS IoT
- Policy AWS IoT potenzialmente configurata in modo errato
- Alias di ruolo eccessivamente permissivo
- L'alias del ruolo consente l'accesso a servizi inutilizzati
- Certificato emesso da una CA in scadenza
- ID client MQTT in conflitto
- Certificato del dispositivo in scadenza
- Un certificato del dispositivo revocato è ancora attivo
- Registrazione disabilitata

CA intermedia revocata per il controllo attivo dei certificati del dispositivo

Utilizzare questo controllo per identificare tutti i certificati dei dispositivi correlati che sono ancora attivi nonostante la revoca di una CA intermedia.

Questo controllo viene visualizzato come `INTERMEDIATE_CA_REVOKED_FOR_ACTIVE_DEVICE_CERTIFICATES_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Critico

Informazioni

Quando questo controllo trova una condizione di non conformità, vengono restituiti i codici motivo seguenti:

- INTERMEDIATE_CA_REVOKED_BY_ISSUER

Perché è importante

La CA intermedia revocata per il controllo dei certificati dei dispositivi attivi valuta l'identità e l'attendibilità del dispositivo, determinando se ci sono certificati dei dispositivi attivi in AWS IoT Core in cui le CA emittenti intermedie sono state revocate nella catena CA.

Una CA intermedia revocata non deve più essere utilizzata per firmare qualsiasi altra CA o certificati dei dispositivi nella catena CA. I nuovi dispositivi aggiunti con certificati firmati utilizzando questo

certificato CA dopo che la CA intermedia viene revocata rappresenteranno una minaccia per la sicurezza.

Come risolvere il problema

Esamina l'attività di registrazione del certificato del dispositivo nel periodo successivo alla revoca del certificato CA. Seguire le best practice di sicurezza per mitigare la situazione. È possibile:

1. Eseguire il provisioning di nuovi certificati, firmati da una CA diversa, per i dispositivi interessati.
2. Verificare che i nuovi certificati siano validi e che possano essere utilizzati dai dispositivi per connettersi.
3. Utilizza UpdateCertificate per contrassegnare il certificato precedente come REVOKED in AWS IoT. Puoi anche usare le operazioni di mitigazione per:
   - Applicare l'operazione di mitigazione `UPDATE_DEVICE_CERTIFICATE` sui risultati di audit per apportare questa modifica.
   - Applicare l'operazione di mitigazione `ADD_THINGS_TO_THING_GROUP` per aggiungere il dispositivo a un gruppo nel quale puoi agire su di esso.
   - Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.
   - Rivedere l'attività di registrazione del certificato del dispositivo nel periodo successivo alla revoca del certificato CA intermedio e prendere in considerazione la possibilità di revocare eventuali certificati del dispositivo che possono essere stati emessi durante tale periodo. È possibile utilizzare ListRelatedResourcesForAuditFinding per elencare i certificati dei dispositivi firmati dal certificato CA e UpdateCertificate per revocare un certificato del dispositivo.
   - Scollegare il vecchio certificato dal dispositivo. (Consultare DetachThingPrincipal).

   Per ulteriori informazioni, consultare Operazioni di mitigazione.

Certificato CA revocato ancora attivo

Un certificato CA è stato revocato, ma è ancora attivo in AWS IoT.

Questo controllo viene visualizzato come `REVOKED_CA_CERTIFICATE_STILL_ACTIVE_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Critico

Informazioni

Un certificato CA è contrassegnato come revocato nell'elenco di revoche di certificati gestito dall'autorità emittente, ma è ancora contrassegnato come "ACTIVE" o "PENDING_TRANSFER" in AWS IoT.

Quando questo controllo trova un certificato CA non conforme, vengono restituiti i codici motivo seguenti:

- CERTIFICATE_REVOKED_BY_ISSUER

Perché è importante

Un certificato CA revocato non deve più essere usato per firmare i certificati dei dispositivi. È possibile che sia stato revocato perché è compromesso. I nuovi dispositivi aggiunti con certificati firmati utilizzando questo certificato CA possono rappresentare una minaccia per la sicurezza.

Come risolvere il problema

1. Utilizza UpdateCACertificate per contrassegnare il certificato CA come INACTIVE in AWS IoT. Puoi anche usare le operazioni di mitigazione per:
   - Applicare l'operazione di mitigazione `UPDATE_CA_CERTIFICATE` sui risultati di audit per apportare questa modifica.
   - Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

   Per ulteriori informazioni, consultare Operazioni di mitigazione.
2. Rivedi l'attività di registrazione del certificato del dispositivo nel periodo successivo alla revoca del certificato CA e prendi in considerazione la possibilità di revocare eventuali certificati del dispositivo che possono essere stati emessi durante tale periodo. Puoi utilizzare ListCertificatesByCA per elencare i certificati del dispositivo firmati dal certificato CA e UpdateCertificate per revocare un certificato del dispositivo.

Certificato del dispositivo condiviso

Connessioni multiple e simultanee usano lo stesso certificato X.509 per l'autenticazione con AWS IoT.

Questo controllo viene visualizzato come `DEVICE_CERTIFICATE_SHARED_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Critico

Informazioni

Quando viene eseguito come parte di un audit on demand, questo controllo cerca i certificati e gli ID client usati dai dispositivi per connettersi durante i 31 giorni precedenti l'inizio dell'audit fino a 2 ore prima dell'esecuzione del controllo. Per i controlli pianificati, questo controllo analizza i dati da 2 ore prima dell'ultima esecuzione dell'audit fino a 2 ore prima dell'avvio di questa istanza dell'audit. Se hai eseguito operazioni per mitigare questa condizione nell'intervallo di tempo controllato, esamina quando sono state stabilite le connessioni simultanee per determinare se il problema persiste.

Quando questo controllo trova un certificato non conforme, vengono restituiti i codici motivo seguenti:

- CERTIFICATE_SHARED_BY_MULTIPLE_DEVICES

I risultati restituiti da questo controllo includono inoltre l'ID del certificato condiviso, gli ID dei client che usano il certificato per connettersi e gli orari di connessione/disconnessione. La maggior parte dei risultati recenti viene elencata per prima.

Perché è importante

Ogni dispositivo deve avere un certificato univoco per eseguire l'autenticazione con AWS IoT. Quando più dispositivi utilizzano lo stesso certificato, questo può indicare che un dispositivo è stato compromesso. L'identità potrebbe essere stata clonata per compromettere ulteriormente il sistema.

Come risolvere il problema

Verifica che il certificato del dispositivo non sia stato compromesso. In caso affermativo, segui le best practice di sicurezza per mitigare la situazione.

Se stai usando lo stesso certificato in più dispositivi, puoi eseguire queste operazioni:

1. Effettuare il provisioning di nuovi certificati univoci e collegarli a ciascun dispositivo.
2. Verificare che i nuovi certificati siano validi e che i dispositivi siano in grado di usarli per connettersi.
3. Utilizza UpdateCertificate per contrassegnare il certificato precedente come REVOKED in AWS IoT. È inoltre possibile utilizzare le azioni di mitigazione per effettuare le seguenti operazioni:

- Applicare l'operazione di mitigazione `UPDATE_DEVICE_CERTIFICATE` sui risultati di audit per apportare questa modifica.
- Applicare l'operazione di mitigazione `ADD_THINGS_TO_THING_GROUP` per aggiungere il dispositivo a un gruppo nel quale puoi agire su di esso.
- Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

Per ulteriori informazioni, consultare Operazioni di mitigazione.

4. Distaccare il vecchio certificato da ogni dispositivo.

Qualità della chiave del certificato del dispositivo

I clienti AWS IoT spesso si affidano all'autenticazione reciproca TLS utilizzando i certificati X.509 per l'autenticazione al broker di messaggi AWS IoT. Questi certificati e i relativi certificati dell'autorità di certificazione devono essere registrati nel proprio account AWS IoT prima di essere utilizzati. AWS IoT esegue controlli di integrità di base su questi certificati quando sono registrati. Tali controlli comprendono:

- Devono essere in un formato valido
- Devono essere firmati da un'autorità di certificazione registrata
- Devono essere ancora entro il loro periodo di validità (in altre parole, non devono essere scaduti)
- Le dimensioni delle chiavi crittografiche devono soddisfare una dimensione minima richiesta (per le chiavi RSA devono essere pari o superiori a 2048 bit).

Questo controllo di audit fornisce i seguenti test aggiuntivi della qualità della chiave crittografica:

- CVE-2008-0166 - Verifica se la chiave è stata generata utilizzando OpenSSL 0.9.8c-1 fino a versioni precedenti la 0.9.8g-9 su un sistema operativo basato su Debian. Queste versioni di OpenSSL utilizzano un generatore di numeri casuali che genera numeri prevedibili, rendendo più facili gli attacchi da remoto da parte degli utenti malintenzionati per impossessarsi delle chiavi crittografiche.
- CVE-2017-15361 - Verifica se la chiave è stata generata dalla libreria Infineon RSA 1.02.013 nel firmware Trusted Platform Module (TPM), ad esempio versioni precedenti la 0000000000000422 - 4.34, la 000000000000062b - 6.43 e la 0000000000008521 - 133.33. Questa libreria non fa altro che gestire male la generazione delle chiavi RSA e semplificare la violazione di alcuni meccanismi

di protezione crittografica agli utenti malintenzionati, i quali possono agire con attacchi mirati. Esempi di tecnologie interessate includono BitLocker con TPM 1.2, la generazione di chiavi PGP YubiKey 4 (prima della 4.3.5) e la funzionalità di crittografia dati utente nella cache in Chrome OS.

AWS IoT Device Defender segnala i certificati come non conformi se non superano questi test.

Questo controllo viene visualizzato come `DEVICE_CERTIFICATE_KEY_QUALITY_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Critico

Informazioni

Questo controllo si applica ai certificati dei dispositivi contrassegnati come "ACTIVE" o "PENDING_TRANSFER".

Quando questo controllo trova un certificato non conforme, vengono restituiti i codici motivo seguenti:

- CERTIFICATE_KEY_VULNERABILITY_CVE-2017-15361
- CERTIFICATE_KEY_VULNERABILITY_CVE-2008-0166

Perché è importante

Quando un dispositivo utilizza un certificato vulnerabile, gli aggressori possono facilmente compromettere tale dispositivo.

Come risolvere il problema

Aggiornare i certificati del dispositivo per sostituire quelli con vulnerabilità note.

Se stai usando lo stesso certificato in più dispositivi, puoi eseguire queste operazioni:

1. Effettuare il provisioning di nuovi certificati univoci e collegarli a ciascun dispositivo.
2. Verificare che i nuovi certificati siano validi e che i dispositivi siano in grado di usarli per connettersi.
3. Utilizza UpdateCertificate per contrassegnare il certificato precedente come REVOKED in AWS IoT. Puoi anche usare le operazioni di mitigazione per:
   - Applicare l'operazione di mitigazione `UPDATE_DEVICE_CERTIFICATE` sui risultati di audit per apportare questa modifica.

- Applicare l'operazione di mitigazione `ADD_THINGS_TO_THING_GROUP` per aggiungere il dispositivo a un gruppo nel quale puoi agire su di esso.
- Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

Per ulteriori informazioni, consultare Operazioni di mitigazione.

4. Distaccare il vecchio certificato da ogni dispositivo.

Qualità della chiave del certificato emesso da una CA

I clienti AWS IoT spesso si affidano all'autenticazione reciproca TLS utilizzando i certificati X.509 per l'autenticazione al broker di messaggi AWS IoT. Questi certificati e i relativi certificati dell'autorità di certificazione devono essere registrati nel proprio account AWS IoT prima di essere utilizzati. AWS IoT esegue controlli di integrità di base su questi certificati quando sono registrati, tra cui:

- I certificati sono in un formato valido.
- I certificati sono entro il loro periodo di validità (in altre parole, non scaduti).
- Le loro dimensioni delle chiavi crittografiche soddisfano una dimensione minima richiesta (per le chiavi RSA, devono essere pari o superiori a 2048 bit).

Questo controllo di audit fornisce i seguenti test aggiuntivi della qualità della chiave crittografica:

- CVE-2008-0166 - Verifica se la chiave è stata generata utilizzando OpenSSL 0.9.8c-1 fino a versioni precedenti la 0.9.8g-9 su un sistema operativo basato su Debian. Queste versioni di OpenSSL utilizzano un generatore di numeri casuali che genera numeri prevedibili, rendendo più facili gli attacchi da remoto da parte degli utenti malintenzionati per impossessarsi delle chiavi crittografiche.
- CVE-2017-15361 - Verifica se la chiave è stata generata dalla libreria Infineon RSA 1.02.013 nel firmware Trusted Platform Module (TPM), ad esempio versioni precedenti la 0000000000000422 - 4.34, la 000000000000062b - 6.43 e la 0000000000008521 - 133.33. Questa libreria non fa altro che gestire male la generazione delle chiavi RSA e semplificare la violazione di alcuni meccanismi di protezione crittografica agli utenti malintenzionati, i quali possono agire con attacchi mirati. Esempi di tecnologie interessate includono BitLocker con TPM 1.2, la generazione di chiavi PGP YubiKey 4 (prima della 4.3.5) e la funzionalità di crittografia dati utente nella cache in Chrome OS.

AWS IoT Device Defender segnala i certificati come non conformi se non superano questi test.

Questo controllo viene visualizzato come `CA_CERTIFICATE_KEY_QUALITY_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Critico

Informazioni

Questo controllo si applica ai certificati CA contrassegnati come "ACTIVE" o "PENDING_TRANSFER".

Quando questo controllo trova un certificato non conforme, vengono restituiti i codici motivo seguenti:

- CERTIFICATE_KEY_VULNERABILITY_CVE-2017-15361
- CERTIFICATE_KEY_VULNERABILITY_CVE-2008-0166

Perché è importante

I nuovi dispositivi aggiunti, firmati utilizzando questo certificato CA, possono rappresentare una minaccia per la sicurezza.

Come risolvere il problema

1. Utilizza UpdateCACertificate per contrassegnare il certificato CA come INACTIVE in AWS IoT. Puoi anche usare le operazioni di mitigazione per:
   - Applicare l'operazione di mitigazione `UPDATE_CA_CERTIFICATE` sui risultati di audit per apportare questa modifica.
   - Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

   Per ulteriori informazioni, consultare Operazioni di mitigazione.
2. Rivedi l'attività di registrazione del certificato del dispositivo nel periodo successivo alla revoca del certificato CA e prendi in considerazione la possibilità di revocare eventuali certificati del dispositivo che possono essere stati emessi durante tale periodo. Usa ListCertificatesByCA per elencare i certificati del dispositivo firmati dal certificato CA e UpdateCertificate per revocare un certificato del dispositivo.

Ruolo Cognito non autenticato eccessivamente permissivo

Una policy collegata a un ruolo di un pool di identità Amazon Cognito non autenticato è considerata troppo permissiva perché concede l'autorizzazione per eseguire le operazioni AWS IoT seguenti:

- gestire o modificare gli oggetti
- leggere i dati amministrativi degli oggetti
- gestire le risorse o i dati non correlati agli oggetti

Oppure, perché concede l'autorizzazione per eseguire le operazioni AWS IoT seguenti su un'ampia gamma di dispositivi:

- Utilizzare MQTT per connettersi a, pubblicare, sottoscrivere argomenti riservati (tra cui dati di esecuzione dei processi o copie shadow)
- usare comandi API per leggere o modificare dati di esecuzione dei processi o copie shadow

In generale, i dispositivi che si connettono utilizzando un ruolo di un pool di identità Amazon Cognito non autenticato devono avere solo autorizzazioni limitate per pubblicare/sottoscrivere argomenti MQTT specifici degli oggetti o usare comandi API per leggere/modificare dati specifici degli oggetti correlati a dati di esecuzione dei processi o copie shadow.

Questo controllo viene visualizzato come `UNAUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Critico

Informazioni

Per questo controllo, AWS IoT Device Defender esegue l'audit di tutti i pool di identità Amazon Cognito che sono stati usati per la connessione al broker di messaggi AWS IoT durante gli ultimi 31 giorni precedenti l'esecuzione dell'audit. Tutti i pool di identità Amazon Cognito da cui si è connessa un'identità Amazon Cognito autenticata o non autenticata vengono inclusi nell'audit.

Quando questo controllo trova un ruolo di un pool di identità Amazon Cognito non autenticato e non conforme, vengono restituiti i codici motivo seguenti:

- ALLOWS_ACCESS_TO_IOT_ADMIN_ACTIONS

- ALLOWS_BROAD_ACCESS_TO_IOT_DATA_PLANE_ACTIONS

Perché è importante

Poiché le identità non autenticate non vengono mai autenticate dall'utente, rappresentano un rischio molto maggiore rispetto alle identità Amazon Cognito autenticate. Se un'identità non autenticata viene compromessa, potrebbe usare le operazioni amministrative per modificare le impostazioni dell'account, eliminare le risorse o ottenere l'accesso a dati sensibili. Oppure, con un accesso alle impostazioni dei dispositivi più su vasta scala, potrebbe accedere alle copie shadow e ai processi per tutti i dispositivi nell'account e modificarli. Un utente guest potrebbe usare le autorizzazioni per compromettere l'intero parco istanze o sferrare un attacco DDOS con i messaggi.

Come risolvere il problema

Una policy collegata a un ruolo di un pool di identità Amazon Cognito non autenticato deve concedere solo le autorizzazioni di cui un dispositivo necessita. È consigliabile eseguire le operazioni seguenti:

1. Creare un nuovo ruolo conforme.
2. Creare un nuovo pool di identità Amazon Cognito e collegare a esso il ruolo conforme.
3. Verificare che le identità possano accedere a AWS IoT usando il nuovo pool.
4. Una volta completata la verifica, collegare il nuovo ruolo conforme al pool di identità Amazon Cognito contrassegnato come non conforme.

Puoi anche usare le operazioni di mitigazione per:

- Applicare l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

Per ulteriori informazioni, consultare Operazioni di mitigazione.

Gestire o modificare gli oggetti

Le seguenti operazioni API AWS IoT vengono utilizzate per gestire o modificare gli oggetti. L'autorizzazione per eseguire queste operazioni non deve essere concessa ai dispositivi che si connettono tramite un pool di identità Amazon Cognito non autenticato.

- `AddThingToThingGroup`

- `AttachThingPrincipal`
- `CreateThing`
- `DeleteThing`
- `DetachThingPrincipal`
- `ListThings`
- `ListThingsInThingGroup`
- `RegisterThing`
- `RemoveThingFromThingGroup`
- `UpdateThing`
- `UpdateThingGroupsForThing`

Qualsiasi ruolo che concede l'autorizzazione per eseguire queste operazioni anche su una singola risorsa è considerato non conforme.

Leggere i dati amministrativi degli oggetti

Le seguenti operazioni API AWS IoT vengono utilizzate per leggere o modificare i dati degli oggetti. I dispositivi che si connettono tramite un pool di identità Amazon Cognito non autenticato non devono essere autorizzati a eseguire queste operazioni.

- `DescribeThing`
- `ListJobExecutionsForThing`
- `ListThingGroupsForThing`
- `ListThingPrincipals`

Example

- noncompliant:

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

```
      "Action": [
          "iot:DescribeThing",
          "iot:ListJobExecutionsForThing",
          "iot:ListThingGroupsForThing",
          "iot:ListThingPrincipals"
      ],
      "Resource": [
        "arn:aws:iot:region:account-id:/thing/MyThing"
      ]
    }
  ]
}
```

In questo modo il dispositivo può eseguire le operazioni specificate anche se concesse solo per un oggetto.

Gestire non-oggetti

I dispositivi che si connettono tramite un pool di identità Amazon Cognito non autenticato non devono avere il permesso di eseguire azioni API AWS IoT diverse da quelle discusse in queste sezioni. È possibile gestire l'account con un'applicazione che si connette tramite un pool di identità Amazon Cognito non autenticato, creando un pool di identità separato, non usato dai dispositivi.

Sottoscrivere/pubblicare argomenti MQTT

I messaggi MQTT vengono inviati tramite il broker di messaggi AWS IoT e sono usati dai dispositivi per eseguire numerose operazioni diverse, tra cui l'accesso allo stato delle copie shadow e dell'esecuzione dei processi e la modifica di tali stati. Una policy che concede a un dispositivo l'autorizzazione di connessione, pubblicazione o sottoscrizione per i messaggi MQTT deve limitare queste operazioni a risorse specifiche, come illustrato di seguito:

Connessione

- noncompliant:

  ```
  arn:aws:iot:region:account-id:client/*
  ```

  Il carattere jolly * permette a qualsiasi dispositivo di connettersi a AWS IoT.

  ```
  arn:aws:iot:region:account-id:client/${iot:ClientId}
  ```

Se `iot:Connection.Thing.IsAttached` non è impostato su "true" nelle chiavi delle condizioni, questo equivale al carattere jolly* dell'esempio precedente.

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iot:Connect" ],
      "Resource": [
        "arn:aws:iot:region:account-id:client/${iot:Connection.Thing.ThingName}"
      ],
      "Condition": {
        "Bool": { "iot:Connection.Thing.IsAttached": "true" }
      }
    }
  ]
}
```

La risorsa specifica contiene una variabile che corrisponde al nome del dispositivo utilizzato per connettersi. L'istruzione condizionale limita ulteriormente il permesso controllando che il certificato utilizzato dal client MQTT corrisponda a quello associato all'oggetto con il nome utilizzato.

Pubblicare

- noncompliant:

```
arn:aws:iot:region:account-id:topic/$aws/things/*/shadow/update
```

Questo esempio permette al dispositivo di aggiornare la copia shadow di qualsiasi dispositivo (* = tutti i dispositivi).

```
arn:aws:iot:region:account-id:topic/$aws/things/*
```

Questo esempio permette al dispositivo di leggere, aggiornare o eliminare la copia shadow di qualsiasi dispositivo.

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iot:Publish" ],
      "Resource": [
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/*"
      ],
    }
  ]
}
```

La specifica della risorsa contiene un carattere jolly, che tuttavia corrisponde solo agli argomenti correlati alla copia shadow per il dispositivo il cui nome di oggetto viene usato per la connessione.

Subscribe

- noncompliant:

```
arn:aws:iot:region:account-id:topicfilter/$aws/things/*
```

Questo esempio permette al dispositivo di sottoscrivere le copie shadow riservate o gli argomenti dei processi per tutti i dispositivi.

```
arn:aws:iot:region:account-id:topicfilter/$aws/things/*
```

Equivale all'esempio precedente, ma con l'uso del carattere jolly #.

```
arn:aws:iot:region:account-id:topicfilter/$aws/things/+/shadow/update
```

Questo esempio permette al dispositivo di visualizzare gli aggiornamenti delle copie shadow di qualsiasi dispositivo (+ = tutti i dispositivi).

- conforme:

```
{
  "Version": "2012-10-17",
```

```
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iot:Subscribe" ],
      "Resource": [
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/*"
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/jobs/*"
      ],
    }
  ]
}
```

Le specifiche della risorsa contengono caratteri jolly, che tuttavia corrispondono solo agli argomenti correlati alla copia shadow e agli argomenti correlati ai processi per il dispositivo il cui nome di oggetto viene usato per la connessione.

Ricezione

- conforme:

```
arn:aws:iot:region:account-id:topicfilter/$aws/things/*
```

Questo è consentito perché il dispositivo può ricevere solo i messaggi dagli argomenti per i quali ha l'autorizzazione alla sottoscrizione.

Leggere/modificare i dati shadow o delle attività

Una policy che concede a un dispositivo l'autorizzazione per eseguire un'operazione API per l'accesso a o la modifica di copie shadow dei dispositivi o dati di esecuzione dei processi deve limitare queste operazioni a risorse specifiche. Di seguito sono riportate le operazioni API:

- `DeleteThingShadow`
- `GetThingShadow`
- `UpdateThingShadow`
- `DescribeJobExecution`
- `GetPendingJobExecutions`
- `StartNextPendingJobExecution`

- `UpdateJobExecution`

Example

- noncompliant:

```
arn:aws:iot:region:account-id:thing/*
```

  Questo esempio permette al dispositivo di eseguire l'operazione specificata su qualsiasi oggetto.

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iot:DeleteThingShadow",
          "iot:GetThingShadow",
          "iot:UpdateThingShadow",
          "iot:DescribeJobExecution",
          "iot:GetPendingJobExecutions",
          "iot:StartNextPendingJobExecution",
          "iot:UpdateJobExecution"
      ],
      "Resource": [
        "arn:aws:iot:region:account-id:/thing/MyThing1",
        "arn:aws:iot:region:account-id:/thing/MyThing2"
      ]
    }
  ]
}
```

  In questo modo il dispositivo può eseguire le operazioni specificate su due oggetti soltanto.

Ruolo Cognito autenticato eccessivamente permissivo

Una policy collegata a un ruolo di un pool di identità Amazon Cognito autenticato è considerata troppo permissiva perché concede l'autorizzazione per eseguire le operazioni AWS IoT seguenti:

- gestire o modificare gli oggetti
- gestire le risorse o i dati non correlati agli oggetti

Oppure, perché concede l'autorizzazione per eseguire le operazioni AWS IoT seguenti su un'ampia gamma di dispositivi:

- leggere i dati amministrativi degli oggetti
- usare MQTT per connettersi a/pubblicare/sottoscrivere argomenti riservati (tra cui dati di esecuzione dei processi o copie shadow)
- usare comandi API per leggere o modificare dati di esecuzione dei processi o copie shadow

In generale, i dispositivi che si connettono usando un ruolo di un pool di identità Amazon Cognito autenticato devono avere solo autorizzazioni limitate per leggere i dati amministrativi specifici degli oggetti, pubblicare/sottoscrivere argomenti MQTT specifici degli oggetti o usare comandi API per leggere/modificare dati specifici degli oggetti correlati a dati di esecuzione dei processi o copie shadow.

Questo controllo viene visualizzato come `AUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Critico

Informazioni

Per questo controllo, AWS IoT Device Defender esegue l'audit di tutti i pool di identità Amazon Cognito che sono stati usati per la connessione al broker di messaggi AWS IoT durante gli ultimi 31 giorni precedenti l'esecuzione dell'audit. Tutti i pool di identità Amazon Cognito da cui si è connessa un'identità Amazon Cognito autenticata o non autenticata vengono inclusi nell'audit.

Quando questo controllo trova un ruolo di un pool di identità Amazon Cognito autenticato non conforme, vengono restituiti i codici motivo seguenti:

- ALLOWS_BROAD_ACCESS_TO_IOT_THING_ADMIN_READ_ACTIONS
- ALLOWS_ACCESS_TO_IOT_NON_THING_ADMIN_ACTIONS
- ALLOWS_ACCESS_TO_IOT_THING_ADMIN_WRITE_ACTIONS

Perché è importante

Se un'identità autenticata viene compromessa, potrebbe usare le operazioni amministrative per modificare le impostazioni dell'account, eliminare le risorse o ottenere l'accesso a dati sensibili.

Come risolvere il problema

Una policy collegata a un ruolo di un pool di identità Amazon Cognito autenticato deve concedere solo le autorizzazioni di cui un dispositivo necessita. È consigliabile eseguire le operazioni seguenti:

1. Creare un nuovo ruolo conforme.
2. Creare un nuovo pool di identità Amazon Cognito e collegare a esso il ruolo conforme.
3. Verificare che le identità possano accedere a AWS IoT usando il nuovo pool.
4. Una volta completata la verifica, collegare il nuovo ruolo conforme al pool di identità Amazon Cognito contrassegnato come non conforme.

Puoi anche usare le operazioni di mitigazione per:

- Applicare l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

Per ulteriori informazioni, consultare Operazioni di mitigazione.

Gestire o modificare gli oggetti

Le operazioni API di AWS IoT seguenti vengono usate per gestire o modificare gli oggetti in modo che non sia necessario concedere le autorizzazioni per l'esecuzione di queste operazioni ai dispositivi che si connettono tramite un pool di identità Amazon Cognito autenticato:

- `AddThingToThingGroup`
- `AttachThingPrincipal`
- `CreateThing`
- `DeleteThing`
- `DetachThingPrincipal`
- `ListThings`
- `ListThingsInThingGroup`
- `RegisterThing`

- `RemoveThingFromThingGroup`
- `UpdateThing`
- `UpdateThingGroupsForThing`

Qualsiasi ruolo che concede l'autorizzazione per eseguire queste operazioni anche su una singola risorsa è considerato non conforme.

Gestire non-oggetti

I dispositivi che si connettono tramite un pool di identità Amazon Cognito autenticato non devono avere il permesso di eseguire operazioni API AWS IoT diverse da quelle discusse in queste sezioni. Per gestire l'account con un'applicazione che si connette tramite un pool di identità Amazon Cognito autenticato, crea un pool di identità separato non usato dai dispositivi.

Leggere i dati amministrativi degli oggetti

Le operazioni API di AWS IoT seguenti vengono usate per leggere i dati degli oggetti in modo che ai dispositivi che si connettono tramite un pool di identità Amazon Cognito autenticato vengano concesse le autorizzazioni per l'esecuzione di queste operazioni solo su un set limitato di oggetti:

- `DescribeThing`
- `ListJobExecutionsForThing`
- `ListThingGroupsForThing`
- `ListThingPrincipals`

- noncompliant:

```
arn:aws:iot:region:account-id:thing/*
```

  Questo esempio permette al dispositivo di eseguire l'operazione specificata su qualsiasi oggetto.

- conforme:

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

```
      "Action": [
          "iot:DescribeThing",
          "iot:ListJobExecutionsForThing",
          "iot:ListThingGroupsForThing",
          "iot:ListThingPrincipals"
      ],
      "Resource": [
        "arn:aws:iot:region:account-id:/thing/MyThing"
      ]
    }
  ]
}
```

Questo esempio permette al dispositivo di eseguire le operazioni specificate solo su un oggetto specifico.

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iot:DescribeThing",
          "iot:ListJobExecutionsForThing",
          "iot:ListThingGroupsForThing",
          "iot:ListThingPrincipals"
      ],
      "Resource": [
        "arn:aws:iot:region:account-id:/thing/MyThing*"
      ]
    }
  ]
}
```

Questo esempio è conforme perché, sebbene la risorsa sia specificata con un carattere jolly (*), il carattere è preceduto da una stringa specifica, che limita il set di oggetti accessibili a quelli con i nomi che hanno il prefisso specificato.

- noncompliant:

```
arn:aws:iot:region:account-id:thing/*
```

Questo esempio permette al dispositivo di eseguire l'operazione specificata su qualsiasi oggetto.

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iot:DescribeThing",
          "iot:ListJobExecutionsForThing",
          "iot:ListThingGroupsForThing",
          "iot:ListThingPrincipals"
      ],
      "Resource": [
        "arn:aws:iot:region:account-id:/thing/MyThing"
      ]
    }
  ]
}
```

Questo esempio permette al dispositivo di eseguire le operazioni specificate solo su un oggetto specifico.

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iot:DescribeThing",
          "iot:ListJobExecutionsForThing",
          "iot:ListThingGroupsForThing",
          "iot:ListThingPrincipals"
      ],
      "Resource": [
        "arn:aws:iot:region:account-id:/thing/MyThing*"
```

```
      ]
    }
  ]
}
```

Questo esempio è conforme perché, sebbene la risorsa sia specificata con un carattere jolly (*), il carattere è preceduto da una stringa specifica, che limita il set di oggetti accessibili a quelli con i nomi che hanno il prefisso specificato.

Sottoscrivere/pubblicare argomenti MQTT

I messaggi MQTT vengono inviati tramite il broker di messaggi AWS IoT e sono usati dai dispositivi per eseguire numerose operazioni, tra cui l'accesso allo stato delle copie shadow e dell'esecuzione dei processi e la modifica di tali stati. Una policy che concede a un dispositivo l'autorizzazione di connessione, pubblicazione o sottoscrizione per i messaggi MQTT deve limitare queste operazioni a risorse specifiche, come illustrato di seguito:

Connessione

- noncompliant:

  ```
  arn:aws:iot:region:account-id:client/*
  ```

  Il carattere jolly * permette a qualsiasi dispositivo di connettersi a AWS IoT.

  ```
  arn:aws:iot:region:account-id:client/${iot:ClientId}
  ```

  Se `iot:Connection.Thing.IsAttached` non è impostato su "true" nelle chiavi delle condizioni, questo equivale al carattere jolly* dell'esempio precedente.

- conforme:

  ```
  {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Effect": "Allow",
        "Action": [ "iot:Connect" ],
        "Resource": [
          "arn:aws:iot:region:account-id:client/${iot:Connection.Thing.ThingName}"
  ```

```
      ],
      "Condition": {
        "Bool": { "iot:Connection.Thing.IsAttached": "true" }
      }
    }
  ]
}
```

La specifica della risorsa contiene una variabile che corrisponde al nome del dispositivo usato per la connessione e l'istruzione di condizione limita ulteriormente l'autorizzazione controllando che il certificato usato dal client MQTT corrisponda a quello collegato all'oggetto con il nome usato.

Pubblicare

- noncompliant:

```
arn:aws:iot:region:account-id:topic/$aws/things/*/shadow/update
```

Questo esempio permette al dispositivo di aggiornare la copia shadow di qualsiasi dispositivo (* = tutti i dispositivi).

```
arn:aws:iot:region:account-id:topic/$aws/things/*
```

Questo esempio permette al dispositivo di leggere/aggiornare/eliminare la copia shadow di qualsiasi dispositivo.

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iot:Publish" ],
      "Resource": [
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/*"
      ],
    }
  ]
}
```

La specifica della risorsa contiene un carattere jolly, che tuttavia corrisponde solo agli argomenti correlati alla copia shadow per il dispositivo il cui nome di oggetto viene usato per la connessione.

Subscribe

- noncompliant:

```
arn:aws:iot:region:account-id:topicfilter/$aws/things/*
```

Questo esempio permette al dispositivo di sottoscrivere le copie shadow riservate o gli argomenti dei processi per tutti i dispositivi.

```
arn:aws:iot:region:account-id:topicfilter/$aws/things/#
```

Equivale all'esempio precedente, ma con l'uso del carattere jolly #.

```
arn:aws:iot:region:account-id:topicfilter/$aws/things/+/shadow/update
```

Questo esempio permette al dispositivo di visualizzare gli aggiornamenti delle copie shadow di qualsiasi dispositivo (+ = tutti i dispositivi).

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iot:Subscribe" ],
      "Resource": [
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/*"
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/jobs/*"
      ],
    }
  ]
}
```

Le specifiche della risorsa contengono caratteri jolly, che tuttavia corrispondono solo agli argomenti correlati alla copia shadow e agli argomenti correlati ai processi per il dispositivo il cui nome di oggetto viene usato per la connessione.

Ricezione

- conforme:

```
arn:aws:iot:region:account-id:topicfilter/$aws/things/*
```

si dice conforme perché il dispositivo può ricevere solo i messaggi dagli argomenti per i quali ha l'autorizzazione alla sottoscrizione.

Leggere o modificare i dati shadow o delle attività

Una policy che concede a un dispositivo l'autorizzazione per eseguire un'operazione API per l'accesso a o la modifica di copie shadow dei dispositivi o dati di esecuzione dei processi deve limitare queste operazioni a risorse specifiche. Di seguito sono riportate le operazioni API:

- `DeleteThingShadow`
- `GetThingShadow`
- `UpdateThingShadow`
- `DescribeJobExecution`
- `GetPendingJobExecutions`
- `StartNextPendingJobExecution`
- `UpdateJobExecution`

Examples (Esempi)

- noncompliant:

```
arn:aws:iot:region:account-id:thing/*
```

Questo esempio permette al dispositivo di eseguire l'operazione specificata su qualsiasi oggetto.

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iot:DeleteThingShadow",
          "iot:GetThingShadow",
          "iot:UpdateThingShadow",
          "iot:DescribeJobExecution",
          "iot:GetPendingJobExecutions",
          "iot:StartNextPendingJobExecution",
          "iot:UpdateJobExecution"
      ],
      "Resource": [
        "arn:aws:iot:region:account-id:/thing/MyThing1",
        "arn:aws:iot:region:account-id:/thing/MyThing2"
      ]
    }
  ]
}
```

Questo esempio permette al dispositivo di eseguire le operazioni specificate solo su due oggetti specifici.

Policy eccessivamente permissive di AWS IoT

Una policy AWS IoT concede autorizzazioni troppo ampie/illimitate. Concede l'autorizzazione per inviare o ricevere messaggi MQTT per un'ampia gamma di dispositivi oppure concede l'autorizzazione per accedere o modificare le copie shadow e i dati di processi di esecuzione per un'ampia gamma di dispositivi.

In generale, una policy per un dispositivo deve concedere l'accesso a risorse associate solo al dispositivo interessato e a nessun altro dispositivo oppure a pochi altri. Con alcune eccezioni, l'uso di un carattere jolly (ad esempio"*") per specificare le risorse in una policy è considerato troppo ampio/illimitato.

Questo controllo viene visualizzato come `IOT_POLICY_OVERLY_PERMISSIVE_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Critico

Informazioni

Quando questo controllo trova una policy AWS IoT non conforme, viene restituito il codice di motivo seguente:

- ALLOWS_BROAD_ACCESS_TO_IOT_DATA_PLANE_ACTIONS

Perché è importante

Un certificato, un'identità Amazon Cognito o un gruppo di oggetti con una policy eccessivamente permissiva possono, se compromessi, avere un impatto sulla sicurezza di tutto l'account. Un utente malintenzionato potrebbe sfruttare tale accesso ampio per leggere o modificare copie shadow, processi o esecuzioni dei processi per tutti i dispositivi. Oppure un utente malintenzionato potrebbe usare un certificato compromesso per connettere dispositivi dannosi o sferrare un attacco DDOS nella rete.

Come risolvere il problema

Segui queste fasi per correggere eventuali policy non conformi collegate a oggetti, gruppi di oggetti o altre entità:

1. Utilizza CreatePolicyVersion per creare una nuova versione conforme ai requisiti della policy. Imposta il flag `setAsDefault` su "true". (In questo modo questa nuova versione è operativa per tutte le entità che utilizzano la policy.)
2. Utilizza ListTargetsForPolicy per ottenere un elenco delle destinazioni (certificati, gruppi di oggetti) a cui è collegata la policy e stabilire quali dispositivi sono inclusi nei gruppi o quali utilizzano i certificati per connettersi.
3. Verificare che tutti i dispositivi associati possano connettersi a AWS IoT. Se un dispositivo non è in grado di connettersi, eseguire il rollback della policy predefinita alla versione precedente usando SetPolicyVersion, rivedere la policy e riprovare.

Puoi usare le operazioni di mitigazione per:

- Applicare l'operazione di mitigazione `REPLACE_DEFAULT_POLICY_VERSION` sui risultati di audit per apportare questa modifica.

- Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

Per ulteriori informazioni, consultare Operazioni di mitigazione.

Usare le variabili delle policy AWS IoT Core per fare riferimento in modo dinamico a risorse AWS IoT nelle policy.

Autorizzazioni MQTT

I messaggi MQTT vengono inviati tramite il broker di messaggi AWS IoT e sono usati dai dispositivi per eseguire numerose operazioni diverse, tra cui l'accesso allo stato delle copie shadow e dell'esecuzione dei processi e la modifica di tali stati. Una policy che concede a un dispositivo l'autorizzazione di connessione, pubblicazione o sottoscrizione per i messaggi MQTT deve limitare queste operazioni a risorse specifiche, come illustrato di seguito:

Connessione

- noncompliant:

```
arn:aws:iot:region:account-id:client/*
```

Il carattere jolly * permette a qualsiasi dispositivo di connettersi a AWS IoT.

```
arn:aws:iot:region:account-id:client/${iot:ClientId}
```

Se `iot:Connection.Thing.IsAttached` non è impostato su "true" nelle chiavi delle condizioni, questo equivale al carattere jolly * come nell'esempio precedente.

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iot:Connect" ],
      "Resource": [
        "arn:aws:iot:region:account-id:client/${iot:Connection.Thing.ThingName}"
      ],
      "Condition": {
```

```
        "Bool": { "iot:Connection.Thing.IsAttached": "true" }
      }
    }
  ]
}
```

La risorsa specifica contiene una variabile che corrisponde al nome del dispositivo utilizzato per connettersi. L'istruzione condizionale limita ulteriormente il permesso controllando che il certificato utilizzato dal client MQTT corrisponda a quello associato all'oggetto con il nome utilizzato.

Pubblicare

- noncompliant:

```
arn:aws:iot:region:account-id:topic/$aws/things/*/shadow/update
```

Questo esempio permette al dispositivo di aggiornare la copia shadow di qualsiasi dispositivo (* = tutti i dispositivi).

```
arn:aws:iot:region:account-id:topic/$aws/things/*
```

Questo esempio permette al dispositivo di leggere, aggiornare o eliminare la copia shadow di qualsiasi dispositivo.

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iot:Publish" ],
      "Resource": [
        "arn:aws:iot:region:account-id:topic/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/*"
      ],
    }
  ]
}
```

La specifica della risorsa contiene un carattere jolly, che tuttavia corrisponde solo agli argomenti correlati alla copia shadow per il dispositivo il cui nome di oggetto viene usato per la connessione.

Subscribe

- noncompliant:

```
arn:aws:iot:region:account-id:topicfilter/$aws/things/*
```

Questo esempio permette al dispositivo di sottoscrivere le copie shadow riservate o gli argomenti dei processi per tutti i dispositivi.

```
arn:aws:iot:region:account-id:topicfilter/$aws/things/*
```

Equivale all'esempio precedente, ma con l'uso del carattere jolly #.

```
arn:aws:iot:region:account-id:topicfilter/$aws/things/+/shadow/update
```

Questo esempio permette al dispositivo di visualizzare gli aggiornamenti delle copie shadow di qualsiasi dispositivo (+ = tutti i dispositivi).

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [ "iot:Subscribe" ],
      "Resource": [
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/shadow/*"
        "arn:aws:iot:region:account-id:topicfilter/$aws/things/
${iot:Connection.Thing.ThingName}/jobs/*"
      ],
    }
  ]
}
```

Le specifiche della risorsa contengono caratteri jolly, che tuttavia corrispondono solo agli argomenti correlati alla copia shadow e agli argomenti correlati ai processi per il dispositivo il cui nome di oggetto viene usato per la connessione.

Ricezione

- conforme:

```
arn:aws:iot:region:account-id:topic/$aws/things/*
```

Questo esempio è appropriato perché il dispositivo può ricevere solo i messaggi dagli argomenti per i quali ha l'autorizzazione di sottoscrizione.

Autorizzazioni shadow e di attività

Una policy che concede a un dispositivo l'autorizzazione per eseguire un'operazione API per l'accesso a o la modifica di copie shadow dei dispositivi o dati di esecuzione dei processi deve limitare queste operazioni a risorse specifiche. Di seguito sono riportate le operazioni API:

- `DeleteThingShadow`
- `GetThingShadow`
- `UpdateThingShadow`
- `DescribeJobExecution`
- `GetPendingJobExecutions`
- `StartNextPendingJobExecution`
- `UpdateJobExecution`

Examples (Esempi)

- noncompliant:

```
arn:aws:iot:region:account-id:thing/*
```

Questo esempio permette al dispositivo di eseguire l'operazione specificata su qualsiasi oggetto.

- conforme:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
          "iot:DeleteThingShadow",
          "iot:GetThingShadow",
          "iot:UpdateThingShadow",
          "iot:DescribeJobExecution",
          "iot:GetPendingJobExecutions",
          "iot:StartNextPendingJobExecution",
          "iot:UpdateJobExecution"
      ],
      "Resource": [
        "arn:aws:iot:region:account-id:/thing/MyThing1",
        "arn:aws:iot:region:account-id:/thing/MyThing2"
      ]
    }
  ]
}
```

Questo esempio permette al dispositivo di eseguire le operazioni specificate solo su due oggetti specifici.

Policy AWS IoT potenzialmente configurata in modo errato

Una policy AWS IoT è stata identificata come potenzialmente configurata in modo errato. Le policy configurate in modo errato, comprese quelle eccessivamente permissive, possono causare incidenti di sicurezza, ad esempio consentire ai dispositivi di accedere a risorse indesiderate.

Il controllo AWS IoT policy potentially misconfigured è un avviso per assicurarsi che siano consentite solo le azioni previste prima di aggiornare la policy.

Nella CLI e nell'API, questo controllo viene visualizzato come `IOT_POLICY_POTENTIAL_MISCONFIGURATION_CHECK`.

Gravità: Medium (media)

Informazioni

AWS IoT restituisce il seguente codice motivo quando questo controllo rileva una policy AWS IoT potenzialmente configurata in modo errato:

- POLICY_CONTAINS_MQTT_WILDCARDS_IN_DENY_STATEMENT
- TOPIC_FILTERS_INTENDED_TO_DENY_ALLOWED_USING_WILDCARDS

Perché è importante

Le policy configurate in modo errato possono portare a conseguenze indesiderate fornendo ai dispositivi più autorizzazioni di quelle necessarie. Si consiglia di valutare attentamente la policy per limitare l'accesso alle risorse e impedire le minacce alla sicurezza.

La policy contiene caratteri jolly MQTT nell'esempio di istruzione di rifiuto

Il controllo AWS IoT policy potentially misconfigured verifica la presenza di caratteri jolly MQTT (+ o #) nelle istruzioni di rifiuto. I caratteri jolly vengono trattati come stringhe letterali dalle policy AWS IoT e possono rendere la policy eccessivamente permissiva.

L'esempio seguente ha lo scopo di rifiutare la sottoscrizione ad argomenti correlati a `building/control_room` utilizzando il carattere jolly MQTT # nelle policy. Tuttavia, i caratteri jolly MQTT non hanno un significato di carattere jolly nelle policy AWS IoT e i dispositivi possono effettuare la sottoscrizione a `building/control_room/data1`.

Il controllo AWS IoT policy potentially misconfigured contrassegnerà questa policy con un codice motivo `POLICY_CONTAINS_MQTT_WILDCARDS_IN_DENY_STATEMENT`.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:Subscribe",
      "Resource": "arn:aws:iot:region:account-id:topicfilter/building/*"
    },
    {
      "Effect": "Deny",
      "Action": "iot:Subscribe",
      "Resource": "arn:aws:iot:region:account-id:topicfilter/building/control_room/#"
```

```
    },
    {
      "Effect": "Allow",
      "Action": "iot:Receive",
      "Resource": "arn:aws:iot:region:account-id:topic/building/*"
    }
  ]
}
```

Di seguito è riportato un esempio di policy configurata correttamente. I dispositivi non dispongono dell'autorizzazione per effettuare la sottoscrizione ad argomenti secondari di `building/control_room/` e non dispongono delle autorizzazioni per ricevere messaggi da argomenti secondari di `building/control_room/`.

```
{
"Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:Subscribe",
      "Resource": "arn:aws:region:account-id:topicfilter/building/*"
    },
    {
      "Effect": "Deny",
      "Action": "iot:Subscribe",
      "Resource": "arn:aws:iot:region:account-id:topicfilter/building/control_room/*"
    },
    {
      "Effect": "Allow",
      "Action": "iot:Receive",
      "Resource": "arn:aws:iot:region:account-id:topic/building/*"
    },
    {
      "Effect": "Deny",
      "Action": "iot:Receive",
      "Resource": "arn:aws:iot:region:account-id:topic/building/control_room/*"
    }
  ]
}
```

Esempio di filtri argomento concepiti per rifiutare consentiti utilizzando caratteri jolly

La policy di esempio seguente è concepita per rifiutare la sottoscrizione ad argomenti correlati a `building/control_room` rifiutando la risorsa `building/control_room/*`. Tuttavia, i dispositivi possono inviare richieste per effettuare la sottoscrizione a `building/#` e ricevere messaggi da tutti gli argomenti correlati a `building`, incluso `building/control_room/data1`.

Il controllo AWS IoT policy potentially misconfigured (Policy AWS IoT potenzialmente configurata in modo errato) contrassegnerà questa policy con un codice motivo `TOPIC_FILTERS_INTENDED_TO_DENY_ALLOWED_USING_WILDCARDS`.

La policy di esempio seguente dispone delle autorizzazioni per ricevere messaggi su `building/control_room topics`:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:Subscribe",
      "Resource": "arn:aws:iot:region:account-id:topicfilter/building/*"
    },
    {
      "Effect": "Deny",
      "Action": "iot:Subscribe",
      "Resource": "arn:aws:iot:region:account-id:topicfilter/building/control_room/*"
    },
    {
      "Effect": "Allow",
      "Action": "iot:Receive",
      "Resource": "arn:aws:iot:region:account-id:topic/building/*"
    }
  ]
}
```

Di seguito è riportato un esempio di policy configurata correttamente. I dispositivi non dispongono dell'autorizzazione per effettuare la sottoscrizione ad argomenti secondari di `building/control_room/` e non dispongono delle autorizzazioni per ricevere messaggi da argomenti secondari di `building/control_room/`.

```
{
```

```
"Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "iot:Subscribe",
      "Resource": "arn:aws:iot:region:account-id:topicfilter/building/*"
    },
    {
      "Effect": "Deny",
      "Action": "iot:Subscribe",
      "Resource": "arn:aws:iot:region:account-id:topicfilter/building/control_room/*"
    },
    {
      "Effect": "Allow",
      "Action": "iot:Receive",
      "Resource": "arn:aws:iot:region:account-id:topic/building/*"
    },
    {
      "Effect": "Deny",
      "Action": "iot:Receive",
      "Resource": "arn:aws:iot:region:account-id:topic/building/control_room/*"
    }
  ]
}
```

> **Note**
>
> Questo controllo potrebbe segnalare falsi positivi. Si consiglia di valutare tutte le eventuali policy contrassegnate ed evidenziare le risorse con falsi positivi utilizzando le soppressioni di audit.

Come risolvere il problema

Questo controllo contrassegna le policy potenzialmente configurate in modo errato, quindi potrebbero esserci falsi positivi. Evidenziare i falsi positivi utilizzando soppressioni della ricerca di audit in modo che non vengano contrassegnati in futuro.

È anche possibile seguire queste fasi per correggere eventuali policy non conformi collegate a oggetti, gruppi di oggetti o altre entità:

1. Utilizza CreatePolicyVersion per creare una nuova versione conforme ai requisiti della policy. Imposta il flag `setAsDefault` su "true". (In questo modo questa nuova versione è operativa per tutte le entità che utilizzano la policy.)

   Per esempi di creazione di policy AWS IoT per casi d'uso comuni, consulta Esempi di policy di pubblicazione/sottoscrizione nella Guida per sviluppatori di AWS IoT Core.
2. Verificare che tutti i dispositivi associati possano connettersi a AWS IoT. Se un dispositivo non è in grado di connettersi, eseguire il rollback della policy predefinita alla versione precedente usando SetPolicyVersion, rivedere la policy e riprovare.

Puoi usare le operazioni di mitigazione per:

- Applicare l'operazione di mitigazione `REPLACE_DEFAULT_POLICY_VERSION` sui risultati di audit per apportare questa modifica.
- Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

Per ulteriori informazioni, consultare Operazioni di mitigazione.

Usa le variabili delle policy IoT Core descritte nella Guida per gli sviluppatori di AWS IoT Core per fare riferimento in modo dinamico alle risorse AWS IoT nelle policy.

Alias di ruolo eccessivamente permissivo

L'alias del ruolo AWS IoT fornisce un meccanismo per i dispositivi connessi per l'autenticazione ad AWS IoT utilizzando i certificati X.509 e quindi ottenere credenziali AWS di breve durata da un ruolo IAM associato a un alias del ruolo AWS IoT. Le autorizzazioni per queste credenziali devono essere oggetto di policy di accesso con variabili di contesto di autenticazione. Se le policy non sono configurate correttamente, l'utente potrebbe essere esposto a un'escalation di attacco con privilegi. Questo controllo di audit garantisce che le policy temporanee fornite dagli alias del ruolo AWS IoT non siano eccessivamente permissive.

Questo controllo viene attivato in presenza di una delle seguenti condizioni:

- La policy fornisce autorizzazioni amministrative a tutti i servizi utilizzati nell'anno passato da questo alias di ruolo (ad esempio "iot:*", "dynamodb:*", "iam:*" e così via).
- La policy fornisce un ampio accesso alle operazioni dei metadati degli oggetti, l'accesso alle operazioni AWS IoT con restrizioni o un ampio accesso alle operazioni del piano dati AWS IoT.

- La policy fornisce l'accesso ai servizi di audit della sicurezza come "iam", "cloudtrail", "guardduty", "inspector" o "trustedadvisor".

Questo controllo viene visualizzato come `IOT_ROLE_ALIAS_OVERLY_PERMISSIVE_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Critico

Informazioni

Quando questo controllo trova una policy IoT non conforme, viene restituito il codice motivo seguente:

- ALLOWS_BROAD_ACCESS_TO_USED_SERVICES
- ALLOWS_ACCESS_TO_SECURITY_AUDITING_SERVICES
- ALLOWS_BROAD_ACCESS_TO_IOT_THING_ADMIN_READ_ACTIONS
- ALLOWS_ACCESS_TO_IOT_NON_THING_ADMIN_ACTIONS
- ALLOWS_ACCESS_TO_IOT_THING_ADMIN_WRITE_ACTIONS
- ALLOWS_BROAD_ACCESS_TO_IOT_DATA_PLANE_ACTIONS

Perché è importante

Limitando le autorizzazioni a quelle necessarie per consentire a un dispositivo di eseguire le normali operazioni, si riducono i rischi per l'account in caso di compromissione di un dispositivo.

Come risolvere il problema

Segui queste fasi per correggere eventuali policy non conformi collegate a oggetti, gruppi di oggetti o altre entità:

1. Segui i passaggi descritti in Autorizzazione di chiamate dirette ai servizi AWS utilizzando il provider di credenziali AWS IoT Core per applicare una policy più restrittiva all'alias del ruolo.

Puoi usare le operazioni di mitigazione per:

- Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

Per ulteriori informazioni, consultare Operazioni di mitigazione.

L'alias del ruolo consente l'accesso a servizi inutilizzati

L'alias del ruolo AWS IoT fornisce un meccanismo per i dispositivi connessi per l'autenticazione a AWS IoT utilizzando i certificati X.509 e quindi ottenere credenziali AWS di breve durata da un ruolo IAM associato a un alias del ruolo AWS IoT. Le autorizzazioni per queste credenziali devono essere oggetto di policy di accesso con variabili di contesto di autenticazione. Se le policy non sono configurate correttamente, l'utente potrebbe essere esposto a un'escalation di attacco con privilegi. Questo controllo di audit garantisce che le policy temporanee fornite dagli alias del ruolo AWS IoT non siano eccessivamente permissive.

Questo controllo viene attivato se l'alias del ruolo ha accesso a servizi che non sono stati utilizzati per il dispositivo AWS IoT nell'ultimo anno. Ad esempio, l'audit segnala se si dispone di un ruolo IAM collegato all'alias del ruolo che ha utilizzato solo AWS IoT nell'anno precedente, ma la policy allegata al ruolo concede anche l'autorizzazione a `"iam:getRole"` e `"dynamodb:PutItem"`.

Questo controllo viene visualizzato come `IOT_ROLE_ALIAS_ALLOWS_ACCESS_TO_UNUSED_SERVICES_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Medium (media)

Informazioni

Quando questo controllo trova una policy AWS IoT non conforme, vengono restituiti i codici motivo seguenti:

- ALLOWS_ACCESS_TO_UNUSED_SERVICES

Perché è importante

Limitando le autorizzazioni ai servizi necessari per consentire a un dispositivo per eseguire le normali operazioni, si riducono i rischi per l'account in caso di compromissione di un dispositivo.

Come risolvere il problema

Segui queste fasi per correggere eventuali policy non conformi collegate a oggetti, gruppi di oggetti o altre entità:

1. Segui i passaggi descritti in Autorizzazione di chiamate dirette ai servizi AWS utilizzando il provider di credenziali AWS IoT Core per applicare una policy più restrittiva all'alias del ruolo.

Puoi usare le operazioni di mitigazione per:

- Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

Per ulteriori informazioni, consultare Operazioni di mitigazione.

Certificato emesso da una CA in scadenza

Un certificato CA è in scadenza tra 30 giorni o è scaduto.

Questo controllo viene visualizzato come `CA_CERTIFICATE_EXPIRING_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Medium (media)

Informazioni

Questo controllo si applica ai certificati CA contrassegnati come "ACTIVE" o "PENDING_TRANSFER".

Quando questo controllo trova un certificato CA non conforme, vengono restituiti i codici motivo seguenti:

- CERTIFICATE_APPROACHING_EXPIRATION
- CERTIFICATE_PAST_EXPIRATION

Perché è importante

Un certificato CA scaduto non deve più essere usato per firmare i nuovi certificati dei dispositivi.

Come risolvere il problema

Consulta le best practice sulla sicurezza per sapere come procedere. È possibile:

1. Registrare un nuovo certificato CA con AWS IoT.
2. Verificare di poter accedere ai certificati del dispositivo utilizzando il nuovo certificato CA.

3. Utilizzare UpdateCACertificate per contrassegnare il certificato CA precedente come INACTIVE in AWS IoT. È inoltre possibile utilizzare le azioni di mitigazione per effettuare le seguenti operazioni:
   - Applicare l'operazione di mitigazione `UPDATE_CA_CERTIFICATE` sui risultati di audit per apportare questa modifica.
   - Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

   Per ulteriori informazioni, consultare Operazioni di mitigazione.

ID client MQTT in conflitto

Più dispositivi si connettono usando lo stesso ID client.

Questo controllo viene visualizzato come `CONFLICTING_CLIENT_IDS_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: High (alta)

Informazioni

Sono state stabilite diverse connessioni usando lo stesso ID client e di conseguenza un dispositivo già connesso è stato disconnesso. La specifica MQTT permette una sola connessione attiva per ID client, pertanto quando un altro dispositivo si connette usando lo stesso ID client, la connessione del dispositivo precedente viene interrotta.

Quando viene eseguito come parte di un audit on demand, questo controllo esamina come sono stati usati gli ID client per le connessioni durante i 31 giorni precedenti l'inizio dell'audit. Per gli audit pianificati, questo controllo analizza i dati dall'ultima esecuzione dell'audit fino all'avvio di questa istanza dell'audit. Se hai eseguito operazioni per mitigare questa condizione nell'intervallo di tempo controllato, esamina quando sono avvenute le connessioni/disconnessioni per determinare se il problema persiste.

Quando questo controllo trova una condizione di non conformità, vengono restituiti i codici motivo seguenti:

- DUPLICATE_CLIENT_ID_ACROSS_CONNECTIONS

I risultati restituiti da questo controllo includono inoltre l'ID client usato per connettersi, gli ID delle entità principali e gli orari di disconnessione. I risultati più recenti sono elencati per primi.

Perché è importante

I dispositivi con ID in conflitto sono costretti a riconnettersi continuamente e questo potrebbe causare la perdita di messaggi o l'impossibilità di connettersi da parte di un dispositivo.

Ciò può indicare che un dispositivo o le sue credenziali sono state compromesse e la causa potrebbe essere un attacco DDoS. È anche possibile che i dispositivi non siano configurati correttamente nell'account o che un dispositivo abbia una connessione malfunzionante e debba riconnettersi più volte al minuto.

Come risolvere il problema

Registra ogni dispositivo come oggetto univoco in AWS IoT e usa il nome dell'oggetto come ID client per la connessione. In alternativa, usa un UUID come ID client per la connessione del dispositivo tramite MQTT. Puoi anche usare le operazioni di mitigazione per:

- Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

Per ulteriori informazioni, consultare Operazioni di mitigazione.

Certificato del dispositivo in scadenza

Un certificato di un dispositivo è in scadenza tra 30 giorni o è scaduto.

Questo controllo viene visualizzato come `DEVICE_CERTIFICATE_EXPIRING_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Medium (media)

Informazioni

Questo controllo si applica ai certificati dei dispositivi contrassegnati come "ACTIVE" o "PENDING_TRANSFER".

Quando questo controllo trova un certificato di un dispositivo non conforme, vengono restituiti i codici motivo seguenti:

- CERTIFICATE_APPROACHING_EXPIRATION
- CERTIFICATE_PAST_EXPIRATION

Perché è importante

Un certificato di un dispositivo non deve essere usato dopo la scadenza.

Come risolvere il problema

Consulta le best practice sulla sicurezza per sapere come procedere. È possibile:

1. Effettuare il provisioning di un nuovo certificato e collegarlo al dispositivo.
2. Verificare che il nuovo certificato sia valido e che il dispositivo sia in grado di usarlo per connettersi.
3. Utilizzare UpdateCertificate per contrassegnare il certificato vecchio come INACTIVE in AWS IoT. Puoi anche usare le operazioni di mitigazione per:
   - Applicare l'operazione di mitigazione `UPDATE_DEVICE_CERTIFICATE` sui risultati di audit per apportare questa modifica.
   - Applicare l'operazione di mitigazione `ADD_THINGS_TO_THING_GROUP` per aggiungere il dispositivo a un gruppo nel quale puoi agire su di esso.
   - Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

   Per ulteriori informazioni, consultare Operazioni di mitigazione.
4. Scollegare il vecchio certificato dal dispositivo. (Consultare DetachThingPrincipal).

Un certificato del dispositivo revocato è ancora attivo

Un certificato del dispositivo revocato è ancora attivo.

Questo controllo viene visualizzato come `REVOKED_DEVICE_CERTIFICATE_STILL_ACTIVE_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Medium (media)

Informazioni

Un certificato del dispositivo si trova nell'elenco di revoche di certificati della CA, ma è ancora attivo in AWS IoT.

Questo controllo si applica ai certificati dei dispositivi contrassegnati come "ACTIVE" o "PENDING_TRANSFER".

Quando questo controllo trova una condizione di non conformità, vengono restituiti i codici motivo seguenti:

- CERTIFICATE_REVOKED_BY_ISSUER

Perché è importante

Un certificato di un dispositivo viene in genere revocato perché è stato compromesso. È possibile che non sia stato ancora revocato in AWS IoT a causa di un errore o di una svista.

Come risolvere il problema

Verifica che il certificato del dispositivo non sia stato compromesso. In caso affermativo, segui le best practice di sicurezza per mitigare la situazione. È possibile:

1. Effettuare il provisioning di un nuovo certificato per il dispositivo.
2. Verificare che il nuovo certificato sia valido e che il dispositivo sia in grado di usarlo per connettersi.
3. Utilizza UpdateCertificate per contrassegnare il certificato precedente come REVOKED in AWS IoT. Puoi anche usare le operazioni di mitigazione per:
   - Applicare l'operazione di mitigazione `UPDATE_DEVICE_CERTIFICATE` sui risultati di audit per apportare questa modifica.
   - Applicare l'operazione di mitigazione `ADD_THINGS_TO_THING_GROUP` per aggiungere il dispositivo a un gruppo nel quale puoi agire su di esso.
   - Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

   Per ulteriori informazioni, consultare Operazioni di mitigazione.
4. Scollegare il vecchio certificato dal dispositivo. (Consultare DetachThingPrincipal).

Registrazione disabilitata

I log di AWS IoT non sono stati abilitati in Amazon CloudWatch. Verifica registrazione V1 e V2.

Questo controllo viene visualizzato come `LOGGING_DISABLED_CHECK` nell'interfaccia a riga di comando e nell'API.

Gravità: Low (bassa)

Informazioni

Quando questo controllo trova una condizione di non conformità, vengono restituiti i codici motivo seguenti:

- LOGGING_DISABLED

Perché è importante

I log di AWS IoT in CloudWatch forniscono visibilità sui comportamenti in AWS IoT, inclusi errori di autenticazione e connessioni e disconnessioni inattese che potrebbero indicare che un dispositivo è stato compromesso.

Come risolvere il problema

Abilita i log di AWS IoT in CloudWatch. Consulta Logging and Monitoring nella Guida per gli sviluppatori di AWS IoT Core. Puoi anche usare le operazioni di mitigazione per:

- Applicare l'operazione di mitigazione `ENABLE_IOT_LOGGING` sui risultati di audit per apportare questa modifica.
- Applica l'operazione di mitigazione `PUBLISH_FINDINGS_TO_SNS` per implementare una risposta personalizzata al messaggio di Amazon SNS.

Per ulteriori informazioni, consultare Operazioni di mitigazione.

Comandi di auditing

Gestione delle impostazioni di auditing

Utilizzare `UpdateAccountAuditConfiguration` per configurare le impostazioni di audit per l'account. Questo comando permette di abilitare i controlli che desideri siano disponibili per gli audit, configurare le notifiche opzionali e configurare le autorizzazioni.

Controlla queste impostazioni con `DescribeAccountAuditConfiguration`.

Usa `DeleteAccountAuditConfiguration` per eliminare le impostazioni di auditing. In questo modo, vengono ripristinati tutti i valori predefiniti e vengono disabilitati in modo efficace tutti gli audit in quanto tutti i controlli sono disabilitati per impostazione predefinita.

UpdateAccountAuditConfiguration

Configura o riconfigura le impostazioni di auditing di Device Defender per l'account. Le impostazioni includono la modalità di invio delle notifiche degli audit e i controlli di auditing abilitati o disabilitati.

Riepilogo

```
aws iot  update-account-audit-configuration \
    [--role-arn <value>] \
    [--audit-notification-target-configurations <value>] \
    [--audit-check-configurations <value>]  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
  "roleArn": "string",
  "auditNotificationTargetConfigurations": {
    "string": {
      "targetArn": "string",
      "roleArn": "string",
      "enabled": "boolean"
    }
  },
  "auditCheckConfigurations": {
    "string": {
      "enabled": "boolean"
    }
  }
}
```

Campi **`cli-input-json`**

Nome	Type	Descrizione
roleArn	string	L’ARN del ruolo che concede a AWS IoT l'autorizzazione

Nome	Type	Descrizione
	Lunghezza max: 2048, min.: 20	per accedere alle informazioni su dispositivi, policy, certificati e altri elementi necessari per eseguire un audit.
auditNotificationTargetConfigurations	map	Informazioni sui target a cui vengono inviate le notifiche di auditing.
targetArn	string	ARN del target (argomento SNS) a cui vengono inviate le notifiche di auditing.
roleArn	string Lunghezza max: 2048, min.: 20	ARN del ruolo che concede l'autorizzazione per l'invio delle notifiche al target.
enabled	booleano	True se le notifiche per il target sono abilitate.

Nome	Type	Descrizione
auditCheckConfigurations	map	Specifica i controlli di auditing abilitati e disabilitati per l'account. Usa `DescribeAccountAuditConfiguration` per visualizzare l'elenco di tutti i controlli, inclusi quelli attualmente abilitati. Alcune raccolte di dati potrebbero iniziare subito quando alcuni controlli sono abilitati. Quando un controllo viene disabilitato, i dati raccolti fino a quel momento in relazione al controllo vengono eliminati. Non è possibile disabilitare un controllo se viene usato da un audit pianificato. È prima necessario eliminare il controllo dall'audit pianificato oppure eliminare l'audit pianificato stesso. Nella prima chiamata a `UpdateAccountAuditConfiguration` questo parametro è obbligatorio e deve specificare almeno un controllo abilitato.
enabled	booleano	True se il controllo di auditing è abilitato per l'account.

Output

Nessuno

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

DescribeAccountAuditConfiguration

Ottiene informazioni sulle impostazioni di Device Defender Audit per l'account. Le impostazioni includono la modalità di invio delle notifiche degli audit e i controlli di auditing abilitati o disabilitati.

Riepilogo

```
aws iot  describe-account-audit-configuration  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
}
```

Output

```
{
  "roleArn": "string",
  "auditNotificationTargetConfigurations": {
    "string": {
      "targetArn": "string",
      "roleArn": "string",
      "enabled": "boolean"
```

```
    }
  },
  "auditCheckConfigurations": {
    "string": {
      "enabled": "boolean"
    }
  }
}
```

Campi di output dell'interfaccia a riga di comando

Nome	Type	Descrizione
roleArn	string Lunghezza max: 2048, min.: 20	L'ARN del ruolo che concede a AWS IoT l'autorizzazione per accedere alle informazioni su dispositivi, policy, certificati e altri elementi necessari per eseguire un audit. Nella prima chiamata a `UpdateAccountAuditConfiguration` questo parametro è obbligatorio.
auditNotificationTargetConfigurations	map	Informazioni sui target a cui vengono inviate le notifiche di auditing per l'account.
targetArn	string	ARN del target (argomento SNS) a cui vengono inviate le notifiche di auditing.
roleArn	string Lunghezza max: 2048, min.: 20	ARN del ruolo che concede l'autorizzazione per l'invio delle notifiche al target.
enabled	booleano	True se le notifiche per il target sono abilitate.

Nome	Type	Descrizione
auditCheckConfigurations	map	Specifica i controlli di auditing abilitati e disabilitati per l'account.
enabled	booleano	True se il controllo di auditing è abilitato per l'account.

Errori

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

DeleteAccountAuditConfiguration

Ripristina le impostazioni predefinite per gli audit di Device Defender per l'account. I dati di configurazione immessi vengono eliminati e tutti i controlli di audit vengono reimpostati come disabilitati.

Riepilogo

```
aws iot  delete-account-audit-configuration \
    [--delete-scheduled-audits | --no-delete-scheduled-audits]  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
  "deleteScheduledAudits": "boolean"
}
```

Campi **`cli-input-json`**

Nome	Type	Descrizione
deleteScheduledAudits	booleano	Se true, tutti gli audit pianificati vengono eliminati.

Output

Nessuno

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceNotFoundException`

La risorsa specificata non esiste.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

Pianificazione di audit

Crea uno o più audit pianificati usando `CreateScheduledAudit`. Questo comando ti permette di specificare i controlli da eseguire durante un audit e la frequenza di esecuzione dell'audit.

Tieni traccia degli audit pianificati con `ListScheduledAudits` e `DescribeScheduledAudit`.

Cambia un audit pianificato esistente con `UpdateScheduledAudit` o eliminalo con `DeleteScheduledAudit`.

CreateScheduledAudit

Crea un audit pianificato che viene eseguito con un intervallo di tempo specificato.

Riepilogo

```
aws iot  create-scheduled-audit \
    --frequency <value> \
    [--day-of-month <value>] \
    [--day-of-week <value>] \
    --target-check-names <value> \
    [--tags <value>] \
    --scheduled-audit-name <value>  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
  "frequency": "string",
  "dayOfMonth": "string",
  "dayOfWeek": "string",
  "targetCheckNames": [
    "string"
  ],
  "tags": [
    {
      "Key": "string",
      "Value": "string"
    }
  ],
  "scheduledAuditName": "string"
}
```

Campi **`cli-input-json`**

Nome	Type	Descrizione
frequenza	string	Frequenza di esecuzione dell'audit. I valori possibili sono "DAILY", "WEEKLY", "BIWEEKLY" o "MONTHLY" . L'ora di inizio effettiva di ogni audit è determinata dal sistema.

Nome	Type	Descrizione
		enumerazione: DAILY | WEEKLY | BIWEEKLY | MONTHLY
dayOfMonth	string modello: ^([1-9]|[12][0-9]|3[01])$\|^LAST$	Giorno del mese in cui viene eseguito l'audit pianificato. Il valore può essere compreso tra "1" e "31" oppure può essere "LAST". Questo campo è obbligatorio se il parametro `frequency` è impostato su "MONTHLY". Se vengono specificati i giorni 29-31 e il mese non ha tali giorni, l'audit viene eseguito l'ultimo ("LAST") giorno del mese.
dayOfWeek	string	Giorno della settimana in cui viene eseguito l'audit pianificato. I valori possibili sono "SUN", "MON", "TUE", "WED", "THU", "FRI" o "SAT". Questo campo è obbligatorio se il parametro `frequency` è impostato su "WEEKLY" o "BIWEEKLY". enumerazione: SUN | MON | TUE | WED | THU | FRI | SAT

Nome	Type	Descrizione
targetCheckNames	elenco membro: AuditCheckName	Controlli eseguiti durante l'audit pianificato. I controlli devono essere abilitati per l'account. Usa `DescribeAccountAuditConfiguration` per visualizzare l'elenco di tutti i controlli, inclusi quelli abilitati, o `UpdateAccountAuditConfiguration` per selezionare i controlli abilitati.
tags	elenco member: Tag Classe Java: java.util.List	Metadati utilizzabili per la gestione dell'audit pianificato.
Chiave	string	La chiave del tag.
Valore	string	Il valore del tag.
scheduledAuditName	string Lunghezza max: 128, min.: 1 Modello: [a–z A–Z 0–9 _-]+	Nome da assegnare all'audit pianificato. (numero massimo pari a 128 caratteri)

Output

```
{
  "scheduledAuditArn": "string"
}
```

Campi di output dell'interfaccia a riga di comando

Nome	Type	Descrizione
scheduledAuditArn	string	ARN dell'audit pianificato.

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

`LimitExceededException`

È stato superato un limite.

ListScheduledAudits

Elenca tutti gli audit pianificati.

Riepilogo

```
aws iot  list-scheduled-audits \
    [--next-token <value>] \
    [--max-results <value>]  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
  "nextToken": "string",
  "maxResults": "integer"
```

```
}
```

Campi **`cli-input-json`**

Nome	Type	Descrizione
nextToken	string	Token per il set di risultati successivo.
maxResults	integer Intervallo – Max: 250, min.: 1	Numero massimo di risultati da restituire per volta. Il valore predefinito è 25.

Output

```
{
  "scheduledAudits": [
    {
      "scheduledAuditName": "string",
      "scheduledAuditArn": "string",
      "frequency": "string",
      "dayOfMonth": "string",
      "dayOfWeek": "string"
    }
  ],
  "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando

Nome	Type	Descrizione
scheduledAudits	elenco membro: ScheduledAuditMetadata Classe Java: java.util.List	Elenco di audit pianificati.
scheduledAuditName	string	Nome dell'audit pianificato.

Nome	Type	Descrizione
	Lunghezza max: 128, min.: 1 Modello: [a–z A–Z 0–9 _-]+	
scheduledAuditArn	string	ARN dell'audit pianificato.
frequenza	string	Frequenza di esecuzione dell'audit. enumerazione: DAILY | WEEKLY | BIWEEKLY | MONTHLY
dayOfMonth	string modello: ^([1-9]|[12][0-9]|3[01])$\|^LAST$	Giorno del mese in cui viene eseguito l'audit pianificato (se `frequency` è "MONTHLY"). Se vengono specificati i giorni 29-31 e il mese non ha tali giorni, l'audit viene eseguito l'ultimo ("LAST") giorno del mese.
dayOfWeek	string	Giorno della settimana in cui viene eseguito l'audit pianificato (se `frequency` è "WEEKLY" o "BIWEEKLY"). enumerazione: SUN | MON | TUE | WED | THU | FRI | SAT
nextToken	string	Token che è possibile usare per recuperare il set di risultati successivo oppure `null` se non ci sono altri risultati.

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

DescribeScheduledAudit

Ottiene le informazioni su un audit pianificato.

Riepilogo

```
aws iot  describe-scheduled-audit \
    --scheduled-audit-name <value>  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
  "scheduledAuditName": "string"
}
```

Campi **`cli-input-json`**

Nome	Type	Descrizione
scheduledAuditName	string Lunghezza max: 128, min.: 1 Modello: [a–z A–Z 0–9 _-]+	Nome dell'audit pianificato di cui ottenere le informazioni.

Output

```
{
  "frequency": "string",
  "dayOfMonth": "string",
  "dayOfWeek": "string",
  "targetCheckNames": [
    "string"
  ],
  "scheduledAuditName": "string",
  "scheduledAuditArn": "string"
}
```

Campi di output dell'interfaccia a riga di comando

Nome	Type	Descrizione
frequenza	string	Frequenza di esecuzione dell'audit. Un valore tra "DAILY", "WEEKLY", "BIWEEKLY" o "MONTHLY". L'ora di inizio effettiva di ogni audit è determinata dal sistema. enumerazione: DAILY | WEEKLY | BIWEEKLY | MONTHLY
dayOfMonth	string modello: ^([1-9]|[12][0-9]|3[01])$\|^LAST$	Giorno del mese in cui viene eseguito l'audit pianificato. Il valore può essere compreso tra "1" e "31" oppure può essere "LAST". Se vengono specificati i giorni 29-31 e il mese non ha tali giorni, l'audit viene eseguito l'ultimo ("LAST") giorno del mese.
dayOfWeek	string	Giorno della settimana in cui viene eseguito l'audit pianifica

Nome	Type	Descrizione
		to. Un valore tra "SUN", "MON", "TUE", "WED", "THU", "FRI" o "SAT". enumerazione: SUN | MON | TUE | WED | THU | FRI | SAT
targetCheckNames	elenco membro: AuditCheckName	Controlli eseguiti durante l'audit pianificato. I controlli devono essere abilitati per l'account. (Usa `DescribeAccountAuditConfiguration` per visualizzare l'elenco di tutti i controlli, inclusi quelli abilitati o `UpdateAccountAuditConfiguration` per selezionare i controlli abilitati).
scheduledAuditName	string Lunghezza max: 128, min.: 1 Modello: [a–z A–Z 0–9 _-]+	Nome dell'audit pianificato.
scheduledAuditArn	string	ARN dell'audit pianificato.

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceNotFoundException`

La risorsa specificata non esiste.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

UpdateScheduledAudit

Aggiorna un audit pianificato, inclusi i controlli eseguiti e la frequenza di esecuzione dell'audit.

Riepilogo

```
aws iot  update-scheduled-audit \
    [--frequency <value>] \
    [--day-of-month <value>] \
    [--day-of-week <value>] \
    [--target-check-names <value>] \
    --scheduled-audit-name <value>  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
  "frequency": "string",
  "dayOfMonth": "string",
  "dayOfWeek": "string",
  "targetCheckNames": [
    "string"
  ],
  "scheduledAuditName": "string"
}
```

Campi **`cli-input-json`**

Nome	Type	Descrizione
frequenza	string	Frequenza di esecuzione dell'audit. I valori possibili sono "DAILY", "WEEKLY",

Nome	Type	Descrizione
		"BIWEEKLY" o "MONTHLY" . L'ora di inizio effettiva di ogni audit è determinata dal sistema. enumerazione: DAILY | WEEKLY | BIWEEKLY | MONTHLY
dayOfMonth	string modello: ^([1-9]|[12][0-9]|3[01])$\|^LAST$	Giorno del mese in cui viene eseguito l'audit pianificato. Il valore può essere compreso tra "1" e "31" oppure può essere "LAST". Questo campo è obbligatorio se il parametro `frequency` è impostato su "MONTHLY". Se vengono specificati i giorni 29-31 e il mese non ha tali giorni, l'audit viene eseguito l'ultimo ("LAST") giorno del mese.
dayOfWeek	string	Giorno della settimana in cui viene eseguito l'audit pianificato. I valori possibili sono "SUN", "MON", "TUE", "WED", "THU", "FRI" o "SAT". Questo campo è obbligatorio se il parametro `frequency` è impostato su "WEEKLY" o "BIWEEKLY". enumerazione: SUN | MON | TUE | WED | THU | FRI | SAT

Nome	Type	Descrizione
targetCheckNames	elenco membro: AuditCheckName	Controlli eseguiti durante l'audit pianificato. I controlli devono essere abilitati per l'account. (Usa `DescribeAccountAuditConfiguration` per visualizzare l'elenco di tutti i controlli, inclusi quelli abilitati o `UpdateAccountAuditConfiguration` per selezionare i controlli abilitati).
scheduledAuditName	string Lunghezza max: 128, min.: 1 Modello: [a–z A–Z 0–9 _-]+	Nome dell'audit pianificato. (numero massimo pari a 128 caratteri)

Output

```
{
  "scheduledAuditArn": "string"
}
```

Campi di output dell'interfaccia a riga di comando

Nome	Type	Descrizione
scheduledAuditArn	string	ARN dell'audit pianificato.

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceNotFoundException`

La risorsa specificata non esiste.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

DeleteScheduledAudit

Elimina un audit pianificato.

Riepilogo

```
aws iot  delete-scheduled-audit \
    --scheduled-audit-name <value>  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
  "scheduledAuditName": "string"
}
```

Campi **`cli-input-json`**

Nome	Type	Descrizione
scheduledAuditName	string Lunghezza max: 128, min.: 1 Modello: [a–z A–Z 0–9 _-]+	Nome dell'audit pianificato da eliminare.

Output

Nessuno

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceNotFoundException`

La risorsa specificata non esiste.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

Esecuzione di un audit on demand

Usare `StartOnDemandAuditTask` per specificare i controlli da eseguire e avviare un audit immediatamente.

StartOnDemandAuditTask

Avvia un audit di Device Defender on demand.

Riepilogo

```
aws iot  start-on-demand-audit-task \
    --target-check-names <value>  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
  "targetCheckNames": [
    "string"
  ]
}
```

Campi **`cli-input-json`**

Nome	Type	Descrizione
targetCheckNames	elenco membro: AuditCheckName	Controlli eseguiti durante l'audit. I controlli specifica ti devono essere abilitati per l'account, altrimenti si verifica un'eccezione. Usa `DescribeAccountAud itConfiguration` per visualizzare l'elenco di tutti i controlli, inclusi quelli abilitati o `UpdateAccountAudit Configuration` per selezionare i controlli abilitati.

Output

```
{
  "taskId": "string"
}
```

Campi di output dell'interfaccia a riga di comando

Nome	Type	Descrizione
taskId	string Lunghezza max: 40, min.: 1 Modello: [a–z A–Z 0–9 -]+	ID dell'audit on demand avviato.

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

`LimitExceededException`

È stato superato un limite.

Gestione di istanze di audit

Usa `DescribeAuditTask` per ottenere informazioni su un'istanza di audit specifica. Se l'esecuzione è già avvenuta, i risultati includono i controlli con esito negativo e quelli con esito positivo, quelli che il sistema non è stato in grado di completare e, se l'audit è ancora in corso, quelli ancora in fase di elaborazione.

Usa `ListAuditTasks` per trovare gli audit eseguiti durante un intervallo di tempo specifico.

Usa `CancelAuditTask` per arrestare un audit in corso.

DescribeAuditTask

Ottiene le informazioni su un audit di Device Defender.

Riepilogo

```
aws iot  describe-audit-task \
    --task-id <value>  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
  "taskId": "string"
}
```

Campi **cli-input-json**

Nome	Type	Descrizione
taskId	string Lunghezza max: 40, min.: 1 Modello: [a–z A–Z 0–9 -]+	ID dell'audit di cui ottenere le informazioni.

Output

```
{
  "taskStatus": "string",
  "taskType": "string",
  "taskStartTime": "timestamp",
  "taskStatistics": {
    "totalChecks": "integer",
    "inProgressChecks": "integer",
    "waitingForDataCollectionChecks": "integer",
    "compliantChecks": "integer",
    "nonCompliantChecks": "integer",
    "failedChecks": "integer",
    "canceledChecks": "integer"
  },
  "scheduledAuditName": "string",
  "auditDetails": {
    "string": {
      "checkRunStatus": "string",
      "checkCompliant": "boolean",
      "totalResourcesCount": "long",
      "nonCompliantResourcesCount": "long",
      "errorCode": "string",
      "message": "string"
    }
  }
}
```

Campi di output dell'interfaccia a riga di comando

Nome	Type	Descrizione
taskStatus	string	Stato dell'audit: un valore tra "IN_PROGRESS", "COMPLETED", "FAILED" o "CANCELED". enumerazione: IN_PROGRESS | COMPLETED | FAILED | CANCELED
taskType	string	Tipo di audit: "ON_DEMAND_AUDIT_TASK" o "SCHEDULED_AUDIT_TASK". enumerazione: ON_DEMAND_AUDIT_TASK | SCHEDULED_AUDIT_TASK
taskStartTime	timestamp	Ora di inizio dell'audit.
taskStatistics	TaskStatistics	Informazioni statistiche sull'audit.
totalChecks	integer	Numero di controlli nell'audit.
inProgressChecks	integer	Numero di controlli in corso.
waitingForDataCollectionChecks	integer	Numero di controlli in attesa della raccolta dei dati.
compliantChecks	integer	Numero di controlli che hanno trovato risorse conformi.
nonCompliantChecks	integer	Numero di controlli che hanno trovato risorse non conformi.

Nome	Type	Descrizione
failedChecks	integer	Numero di controlli.
canceledChecks	integer	Numero di controlli non eseguiti perché l'audit è stato annullato.
scheduledAuditName	string Lunghezza max: 128, min.: 1 Modello: [a–z A–Z 0–9 _-]+	Nome dell'audit pianificato (solo se l'audit è di tipo pianificato).
auditDetails	map	Informazioni dettagliate su ogni controllo eseguito durante l'audit.
checkRunStatus	string	Stato di completamento del controllo. Un valore tra "IN_PROGRESS", "WAITING_FOR_DATA_COLLECTION", "CANCELED", "COMPLETED_COMPLIANT", "COMPLETED_NON_COMPLIANT" o "FAILED". enumerazione: IN_PROGRESS | WAITING_FOR_DATA_COLLECTION | CANCELED | COMPLETED_COMPLIANT | COMPLETED_NON_COMPLIANT | FAILED
checkCompliant	booleano	True se il controllo è stato completato e ha trovato tutte le risorse conformi.

Nome	Type	Descrizione
totalResourcesCount	Long	Numero di risorse su cui è stato eseguito il controllo.
nonCompliantResourcesCount	Long	Numero di risorse che dal controllo sono risultate non conformi.
errorCode	string	Codice degli errori rilevati durante l'esecuzione del controllo nel corso dell'audit. Un valore tra "INSUFFICIENT_PERMISSIONS" o "AUDIT_CHECK_DISABLED".
message	string Lunghezza max: 2048	Messaggio associato agli errori rilevati durante l'esecuzione del controllo nel corso dell'audit.

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ResourceNotFoundException`

La risorsa specificata non esiste.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

ListAuditTasks

Elenca gli audit di Device Defender eseguiti durante un determinato periodo di tempo.

Riepilogo

```
aws iot  list-audit-tasks \
    --start-time <value> \
    --end-time <value> \
    [--task-type <value>] \
    [--task-status <value>] \
    [--next-token <value>] \
    [--max-results <value>]  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
  "startTime": "timestamp",
  "endTime": "timestamp",
  "taskType": "string",
  "taskStatus": "string",
  "nextToken": "string",
  "maxResults": "integer"
}
```

Campi **`cli-input-json`**

Nome	Type	Descrizione
startTime	timestamp	Inizio del periodo di tempo. Le informazioni sull'audit vengono conservate per un periodo di tempo limitato (180 giorni). Richiesta di un orario di inizio precedente a ciò che viene conservato comporta un `InvalidRequestException` .

Nome	Type	Descrizione
endTime	timestamp	Fine del periodo di tempo.
taskType	string	Filtro che limita l'output al tipo di audit specificato: può essere un valore tra "ON_DEMAND_AUDIT_TASK" o "SCHEDULED__AUDIT_TASK". enumerazione: ON_DEMAND_AUDIT_TASK | SCHEDULED_AUDIT_TASK
taskStatus	string	Filtro che limita l'output agli audit con lo stato di completamento specifica to: può essere un valore tra "IN_PROGRESS", "COMPLETED", "FAILED" o "CANCELED". enumerazione: IN_PROGRESS | COMPLETED | FAILED | CANCELED
nextToken	string	Token per il set di risultati successivo.
maxResults	integer Intervallo – Max: 250, min.: 1	Numero massimo di risultati da restituire per volta. Il valore predefinito è 25.

Output

```
{
  "tasks": [
```

```
    {
      "taskId": "string",
      "taskStatus": "string",
      "taskType": "string"
    }
  ],
  "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando

Nome	Type	Descrizione
attività	elenco membro: AuditTaskMetadata Classe Java: java.util.List	Audit eseguiti durante il periodo di tempo specificato.
taskId	string Lunghezza max: 40, min.: 1 Modello: [a–z A–Z 0–9 -]+	ID dell'audit.
taskStatus	string	Stato dell'audit: un valore tra "IN_PROGRESS", "COMPLETED", "FAILED" o "CANCELED". enumerazione: IN_PROGRESS | COMPLETED | FAILED | CANCELED
taskType	string	Tipo di audit: un valore tra "ON_DEMAND_AUDIT_TASK" o "SCHEDULED_AUDIT_TASK".

Nome	Type	Descrizione
		enumerazione: ON_DEMAND _AUDIT_TASK | SCHEDULED _AUDIT_TASK
nextToken	string	Token che è possibile usare per recuperare il set di risultati successivo oppure `null` se non ci sono risultati aggiuntivi.

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

CancelAuditTask

Annulla un audit in corso. L'audit può essere pianificato o on demand. Se l'audit non è in corso, si verifica `InvalidRequestException`.

Riepilogo

```
aws iot  cancel-audit-task \
    --task-id <value>  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
  "taskId": "string"
```

```
}
```

Campi **`cli-input-json`**

Nome	Type	Descrizione
taskId	string Lunghezza max: 40, min.: 1 Modello: [a–z A–Z 0–9 -]+	ID dell'audit da annullare. È possibile annullare solo un audit con stato "IN_PROGRESS".

Output

Nessuno

Errori

`ResourceNotFoundException`

La risorsa specificata non esiste.

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

Controllo dei risultati dell'audit

Usa `ListAuditFindings` per visualizzare i risultati di un audit. Puoi filtrare i risultati in base al tipo di controllo, a una risorsa specifica o a quando è stato eseguito l'audit. È possibile utilizzare queste informazioni per mitigare gli eventuali problemi rilevati.

È possibile definire operazioni di mitigazione e applicarle ai risultati dell'audit. Per ulteriori informazioni, consultare Operazioni di mitigazione.

ListAuditFindings

Elenca i risultati di un audit di Device Defender o degli audit eseguiti durante un periodo di tempo specificato. I risultati vengono conservati per 180 giorni.

Riepilogo

```
aws iot  list-audit-findings \
    [--task-id <value>] \
    [--check-name <value>] \
    [--resource-identifier <value>] \
    [--max-results <value>] \
    [--next-token <value>] \
    [--start-time <value>] \
    [--end-time <value>]  \
    [--cli-input-json <value>] \
    [--generate-cli-skeleton]
```

`cli-input-json` formato

```
{
  "taskId": "string",
  "checkName": "string",
  "resourceIdentifier": {
    "deviceCertificateId": "string",
    "caCertificateId": "string",
    "cognitoIdentityPoolId": "string",
    "clientId": "string",
    "policyVersionIdentifier": {
      "policyName": "string",
      "policyVersionId": "string"
    },

    "roleAliasArn": "string",
    "account": "string"
  },
  "maxResults": "integer",
  "nextToken": "string",
  "startTime": "timestamp",
  "endTime": "timestamp"
}
```

Campi **`cli-input-json`**

Nome	Type	Descrizione
taskId	string Lunghezza max: 40, min.: 1 Modello: [a–z A–Z 0–9 -]+	Filtro che limita i risultati all'audit con l'ID specificato. Devi specificare il valore di taskId oppure di startTime ed endTime, ma non entrambi.
checkName	string	Filtro che limita i risultati al controllo di auditing specifica to.
resourceIdentifier	ResourceIdentifier	Informazioni che identificano le risorse non conformi.
deviceCertificateId	string Lunghezza max: 64, min.: 64 Modello: (0x)?[a–f A–F 0–9]+	ID del certificato collegato alla risorsa.
caCertificateId	string Lunghezza max: 64, min.: 64 Modello: (0x)?[a–f A–F 0–9]+	ID del certificato CA usato per autorizzare il certificato.
cognitoIdentityPoolId	string	ID del pool di identità Amazon Cognito.
clientId	string	ID client.
policyVersionIdentifier	PolicyVersionIdentifier	Versione della policy associata alla risorsa.
policyName	string Lunghezza max: 128, min.: 1	Il nome della policy .

Nome	Type	Descrizione
	modello: [w+=,.@-]+	
policyVersionId	string Modello: [0–9]+	ID della versione della policy associata alla risorsa.
roleAliasArn	string	L'ARN dell'alias ruolo con azioni eccessivamente permissive. Lunghezza max: 2048, min.: 1
account	string Lunghezza max: 12, min.: 12 Modello: [0–9]+	Account a cui è associata la risorsa.
maxResults	integer Intervallo – Max: 250, min.: 1	Numero massimo di risultati da restituire per volta. Il valore predefinito è 25.
nextToken	string	Token per il set di risultati successivo.
startTime	timestamp	Filtro che limita i risultati a quelli trovati dopo l'ora specificata. Devi specifica re il valore di startTime ed endTime oppure di taskId, ma non entrambi.
endTime	timestamp	Filtro che limita i risultati a quelli trovati prima dell'ora specificata. Devi specifica re il valore di startTime ed endTime oppure di taskId, ma non entrambi.

Output

```
{
  "findings": [
    {
      "taskId": "string",
      "checkName": "string",
      "taskStartTime": "timestamp",
      "findingTime": "timestamp",
      "severity": "string",
      "nonCompliantResource": {
        "resourceType": "string",
        "resourceIdentifier": {
          "deviceCertificateId": "string",
          "caCertificateId": "string",
          "cognitoIdentityPoolId": "string",
          "clientId": "string",
          "policyVersionIdentifier": {
            "policyName": "string",
            "policyVersionId": "string"
          },
          "account": "string"
        },
        "additionalInfo": {
          "string": "string"
        }
      },
      "relatedResources": [
        {
          "resourceType": "string",
          "resourceIdentifier": {
            "deviceCertificateId": "string",
            "caCertificateId": "string",
            "cognitoIdentityPoolId": "string",
            "clientId": "string",

            "iamRoleArn": "string",

            "policyVersionIdentifier": {
              "policyName": "string",
              "policyVersionId": "string"
            },
            "account": "string"
          },
```

```
          "roleAliasArn": "string",

          "additionalInfo": {
            "string": "string"
          }
        }
      ],
      "reasonForNonCompliance": "string",
      "reasonForNonComplianceCode": "string"
    }
  ],
  "nextToken": "string"
}
```

Campi di output dell'interfaccia a riga di comando

Nome	Type	Descrizione
risultati	elenco membro: AuditFinding	Risultati dell'audit.
taskId	string Lunghezza max: 40, min.: 1 Modello: [a–z A–Z 0–9 -]+	ID dell'audit che ha generato il risultato (ricerca)
checkName	string	Controllo di auditing che ha generato il risultato.
taskStartTime	timestamp	Ora di inizio dell'audit.
findingTime	timestamp	Ora in cui è stato trovato il risultato.
severity	string	Gravità del risultato. enumerazione: CRITICAL | HIGH | MEDIUM | LOW

Nome	Type	Descrizione
nonCompliantResource	NonCompliantResource	Risorsa risultata non conforme dal controllo di auditing.
resourceType	string	Tipo della risorsa non conforme. enumerazione: DEVICE_CERTIFICATE | CA_CERTIFICATE | IOT_POLICY | COGNITO_IDENTITY_POOL | CLIENT_ID | ACCOUNT_SETTINGS
resourceIdentifier	ResourceIdentifier	Informazioni che identificano le risorse non conformi.
deviceCertificateId	string Lunghezza max: 64, min.: 64 Modello: (0x)?[a–f A–F 0–9]+	ID del certificato collegato alla risorsa.
caCertificateId	string Lunghezza max: 64, min.: 64 Modello: (0x)?[a–f A–F 0–9]+	ID del certificato CA usato per autorizzare il certificato.
cognitoIdentityPoolId	string	ID del pool di identità Amazon Cognito.
clientId	string	ID client.
policyVersionIdentifier	PolicyVersionIdentifier	Versione della policy associata alla risorsa.

Nome	Type	Descrizione
policyName	string Lunghezza max: 128, min.: 1 modello: [w+=,.@-]+	Il nome della policy .
policyVersionId	string Modello: [0–9]+	ID della versione della policy associata alla risorsa.
account	string Lunghezza max: 12, min.: 12 Modello: [0–9]+	Account a cui è associata la risorsa.
additionalInfo	map	Altre informazioni sulla risorsa non conforme.
relatedResources	elenco membro: RelatedResource	Elenco delle risorse correlate.
resourceType	string	Il tipo di risorsa. enumerazione: DEVICE_CERTIFICATE | CA_CERTIFICATE | IOT_POLICY | COGNITO_IDENTITY_POOL | CLIENT_ID | ACCOUNT_SETTINGS
resourceIdentifier	ResourceIdentifier	Informazioni che identificano la risorsa.

Nome	Type	Descrizione
deviceCertificateId	string Lunghezza max: 64, min.: 64 Modello: (0x)?[a–f A–F 0–9]+	ID del certificato collegato alla risorsa.
caCertificateId	string Lunghezza max: 64, min.: 64 Modello: (0x)?[a–f A–F 0–9]+	ID del certificato CA usato per autorizzare il certificato.
cognitoIdentityPoolId	string	ID del pool di identità Amazon Cognito.
clientId	string	ID client.
policyVersionIdentifier	PolicyVersionIdentifier	Versione della policy associata alla risorsa.
iamRoleArn	string Lunghezza max: 2048, min.: 20	L'ARN del ruolo IAM che ha azioni eccessivamente permissive.
policyName	string Lunghezza max: 128, min.: 1 modello: [w+=,.@-]+	Il nome della policy .
policyVersionId	string Modello: [0–9]+	ID della versione della policy associata alla risorsa.
roleAliasArn	string Lunghezza max: 2048, min.: 1	L'ARN dell'alias ruolo con azioni eccessivamente permissive.

Nome	Type	Descrizione
account	string Lunghezza max: 12, min.: 12 Modello: [0–9]+	Account a cui è associata la risorsa.
additionalInfo	map	Altre informazioni sulla risorsa.
reasonForNonCompliance	string	Motivo per cui la risorsa è risultata non conforme.
reasonForNonComplianceCode	string	Codice che indica il motivo per cui la risorsa è risultata non conforme.
nextToken	string	Token che è possibile usare per recuperare il set di risultati successivo oppure `null` se non ci sono risultati aggiuntivi.

Errori

`InvalidRequestException`

I contenuti della richiesta non sono validi.

`ThrottlingException`

La velocità supera il limite.

`InternalFailureException`

Si è verificato un errore imprevisto.

Soppressioni della ricerca di audit

Quando si esegue un audit, vengono riportati i risultati per tutte le risorse non conformi. Ciò significa che i rapporti di audit includono risultati per le risorse a cui stai lavorando per mitigare i

problemi e anche per le risorse che sono notoriamente non conformi, ad esempio dispositivi di test o danneggiati. Il controllo continua a segnalare i risultati per le risorse che rimangono non conformi nelle successive esecuzioni di audit e che potrebbero aggiungere informazioni indesiderate ai report. Le soppressioni di ricerca di audit consentono di sopprimere o filtrare i risultati per un periodo di tempo definito fino a quando la risorsa non viene sistemata oppure fino a tempo indeterminato per una risorsa associata a un dispositivo di prova o danneggiato.

> **Note**
>
> Le operazioni di attenuazione non saranno disponibili per i risultati di audit soppressi. Per ulteriori informazioni sulle operazioni di mitigazione, consulta Operazioni di mitigazione.

Per informazioni sull'audit per individuare le quote di soppressione, consulta Endpoint e quote di AWS IoT Device Defender.

Come funzionano le soppressioni dei risultati di audit

Quando si crea una soppressione della ricerca di audit per una risorsa non conforme, i rapporti di audit e le notifiche si comportano in modo diverso.

I rapporti di audit includeranno una nuova sezione che elenca tutti i risultati eliminati associati al report. I risultati eliminati non verranno presi in considerazione quando valutiamo se un controllo di audit è conforme o meno. Viene inoltre restituito un conteggio delle risorse soppresse per ogni controllo di audit quando si utilizza il comando describe-audit-task nell'interfaccia a riga di comando (CLI).

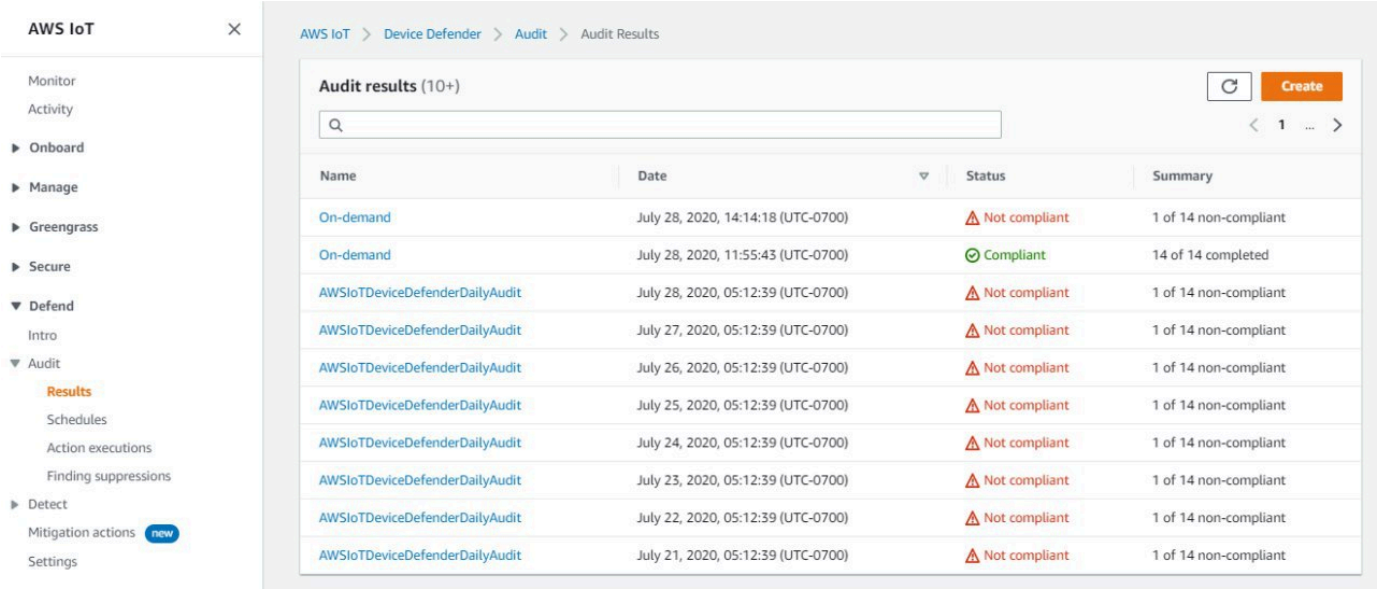
Per le notifiche di audit, i risultati eliminati non vengono presi in considerazione quando si valuta se un controllo di audit è conforme o meno. Un conteggio delle risorse soppresse è incluso in ogni notifica di controllo audit che AWS IoT Device Defender pubblica su Amazon CloudWatch e Amazon Simple Notification Service (Amazon SNS).

Come utilizzare le soppressioni della ricerca di audit nella console

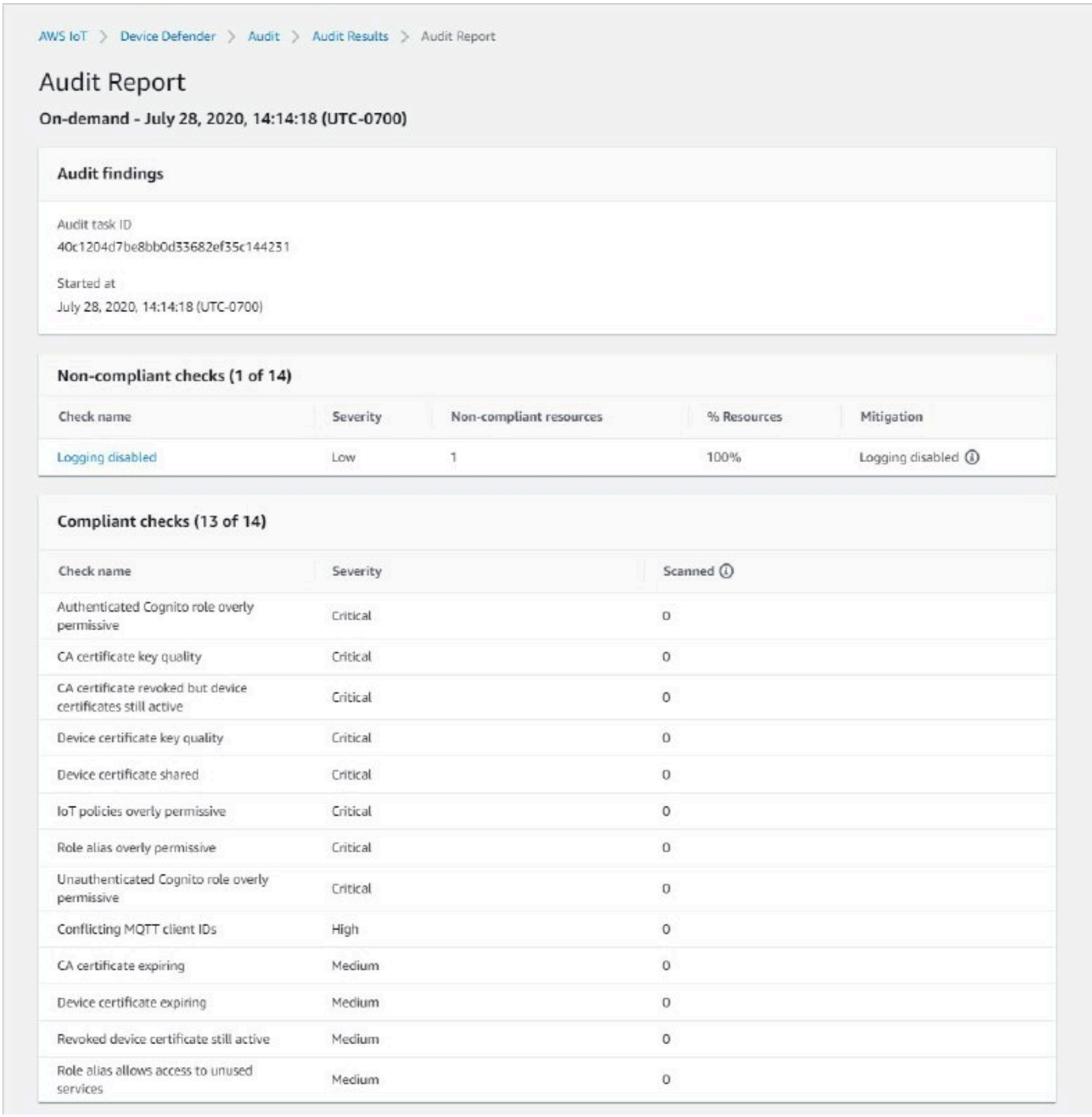
Per sopprimere un risultato da un rapporto di audit

La procedura seguente mostra come creare una soppressione della ricerca di audit nell’AWS IoT console.

1. Nell'AWS IoT console, nel riquadro di navigazione, espandi Defend (Protezione) e scegli Audit (Audit), quindi Results (Risultati).
2. Seleziona un rapporto di audit che desideri esaminare.

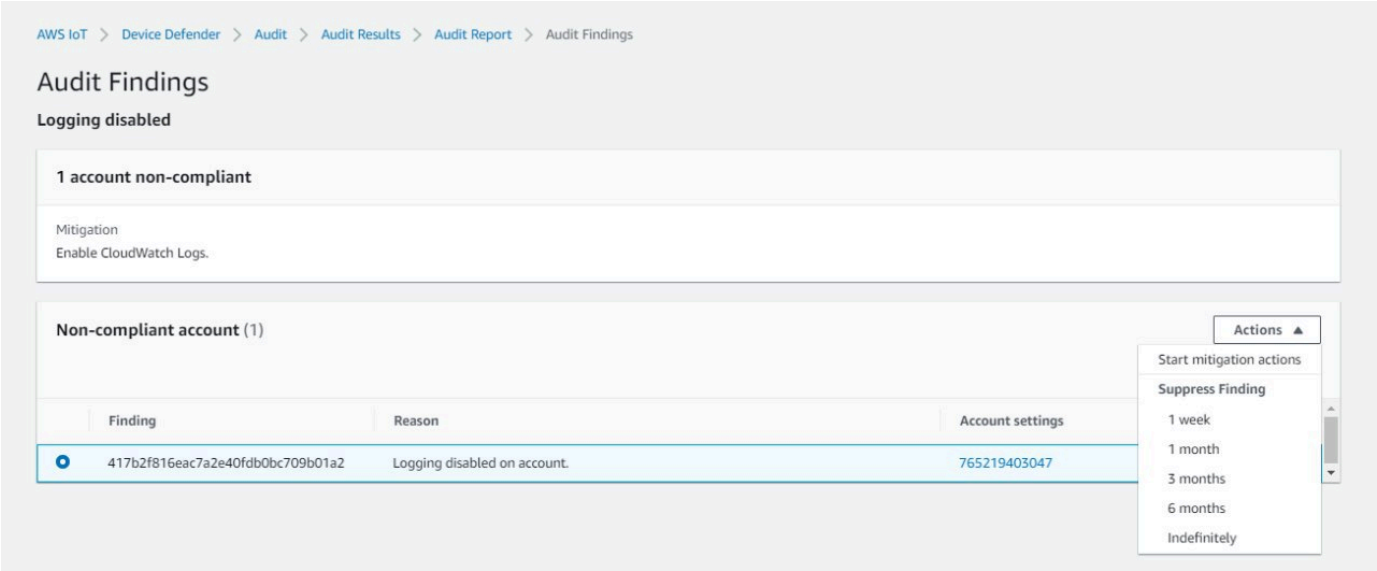


3. Nella sezione Non-compliant checks (Controlli non conformi), in Check name (Controlla il nome) scegli il controllo di audit che ti interessa.

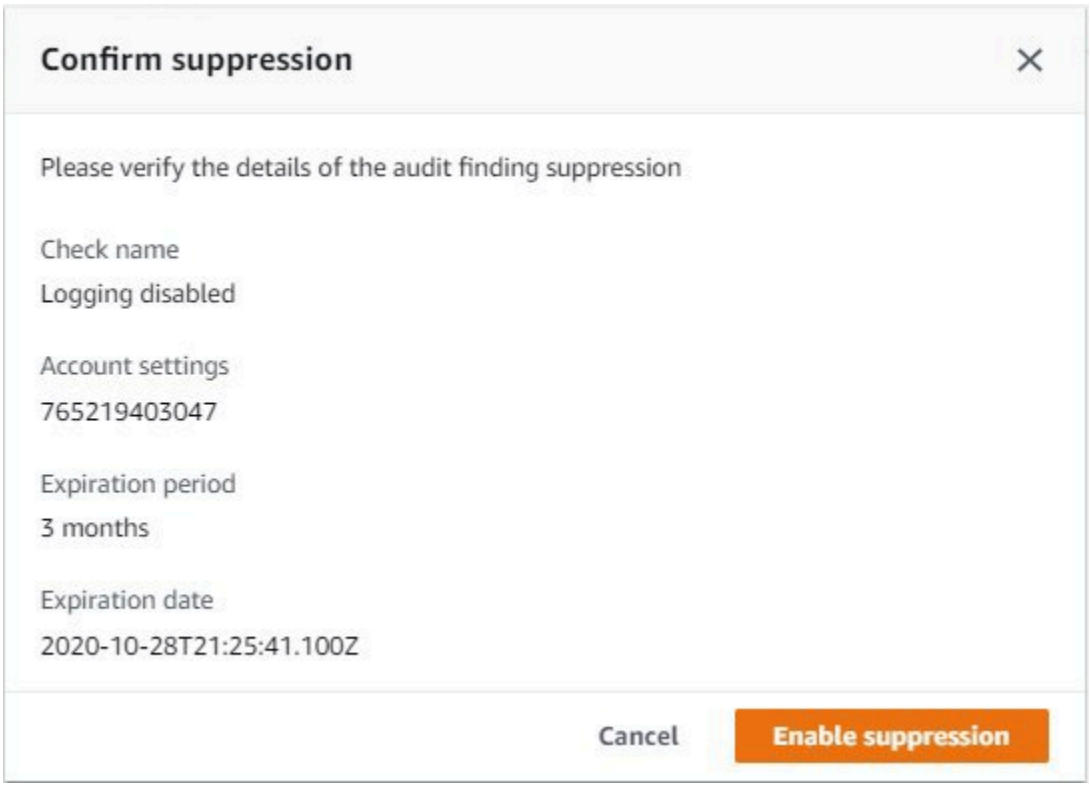


4. Nella schermata dei dettagli del controllo di audit, se ci sono risultati che non desideri visualizzare, seleziona il pulsante di opzione accanto al risultato. Quindi, seleziona Actions (Operazioni) e scegli il periodo di tempo in cui desideri che la soppressione del rilevamento di audit venga mantenuta.

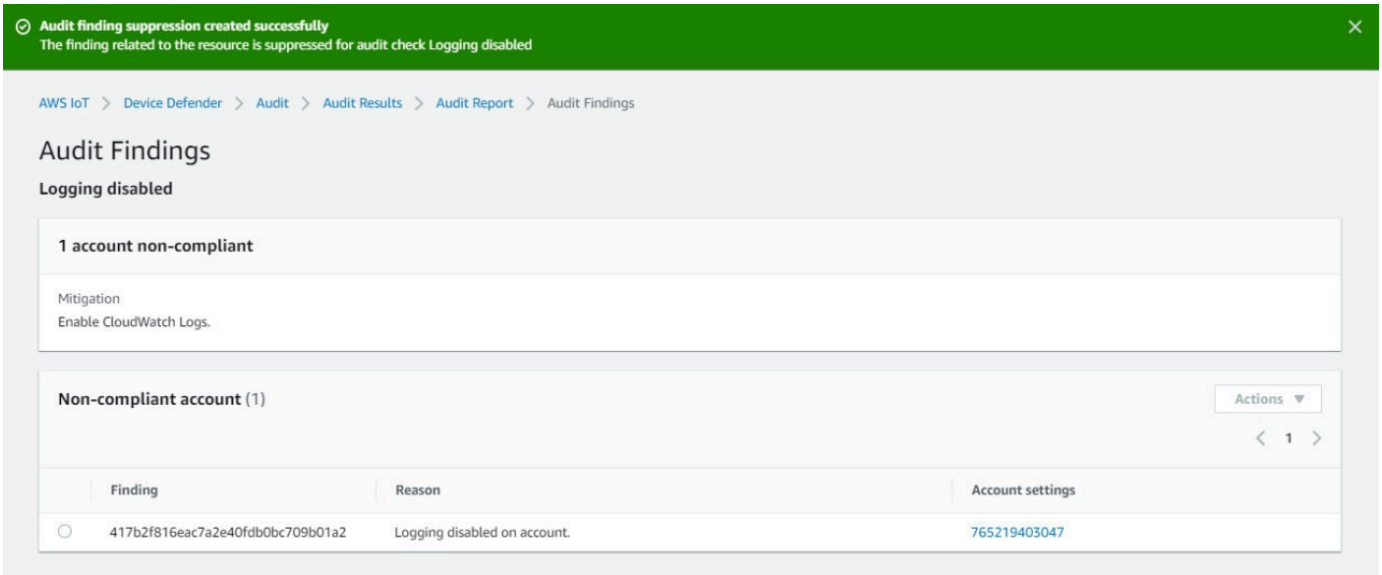
> **Note**
>
> Nella console, puoi selezionare 1 week (1 settimana), 1 month (1 mese), 3 months (3 mesi), 6 months (6 mesi) oppure Indefinitely (A tempo indeterminato) come date di scadenza per l'eliminazione dei risultati di verifica. Se desideri impostare una data di scadenza specifica, puoi farlo solo nell'interfaccia della riga di comando o nell'API. Le soppressioni della ricerca di audit possono anche essere annullate in qualsiasi momento, indipendentemente dalla data di scadenza.



5. Conferma i dettagli di soppressione e scegli Enable suppression (Abilita la soppressione).



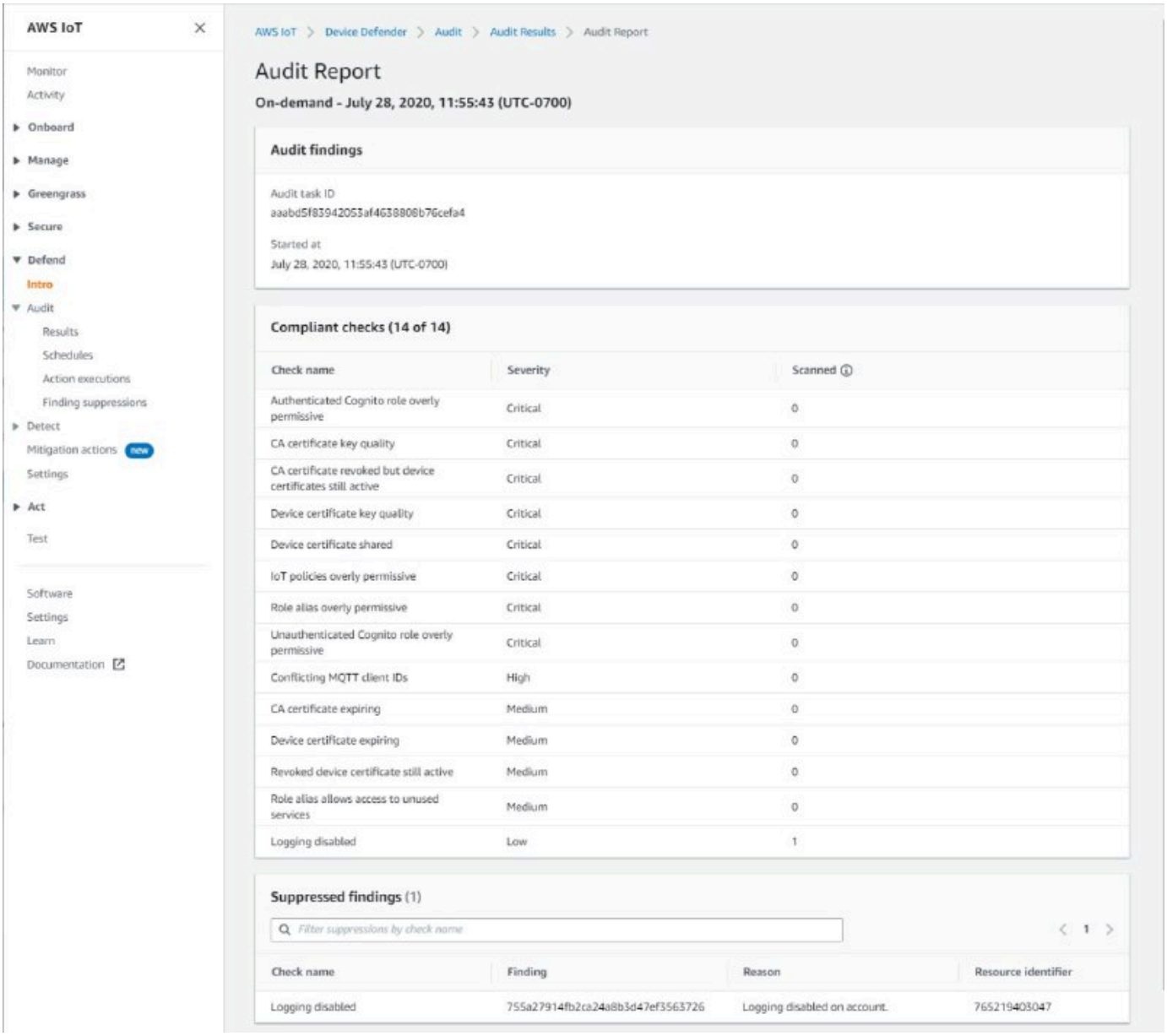
6. Dopo aver creato la soppressione della ricerca di audit, viene visualizzato un banner che lo conferma.



Per visualizzare i risultati soppressi in un report di audit

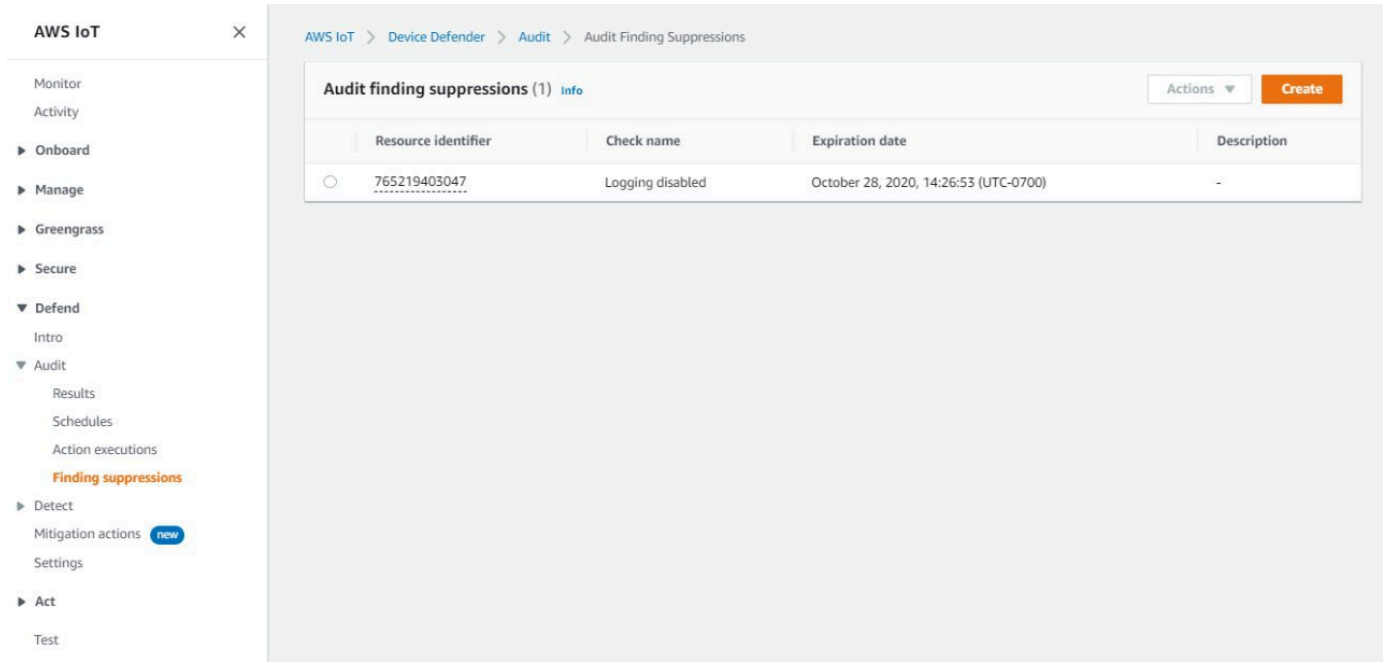
1. Nell'AWS IoT console, nel riquadro di navigazione, espandi Defend (Protezione) e scegli Audit (Audit), quindi Results (Risultati).

2. Seleziona un rapporto di audit che desideri esaminare.
3. Nella sezione Suppressed findings (Risultati eliminati), visualizza quali risultati di audit sono stati eliminati per il report di audit scelto.



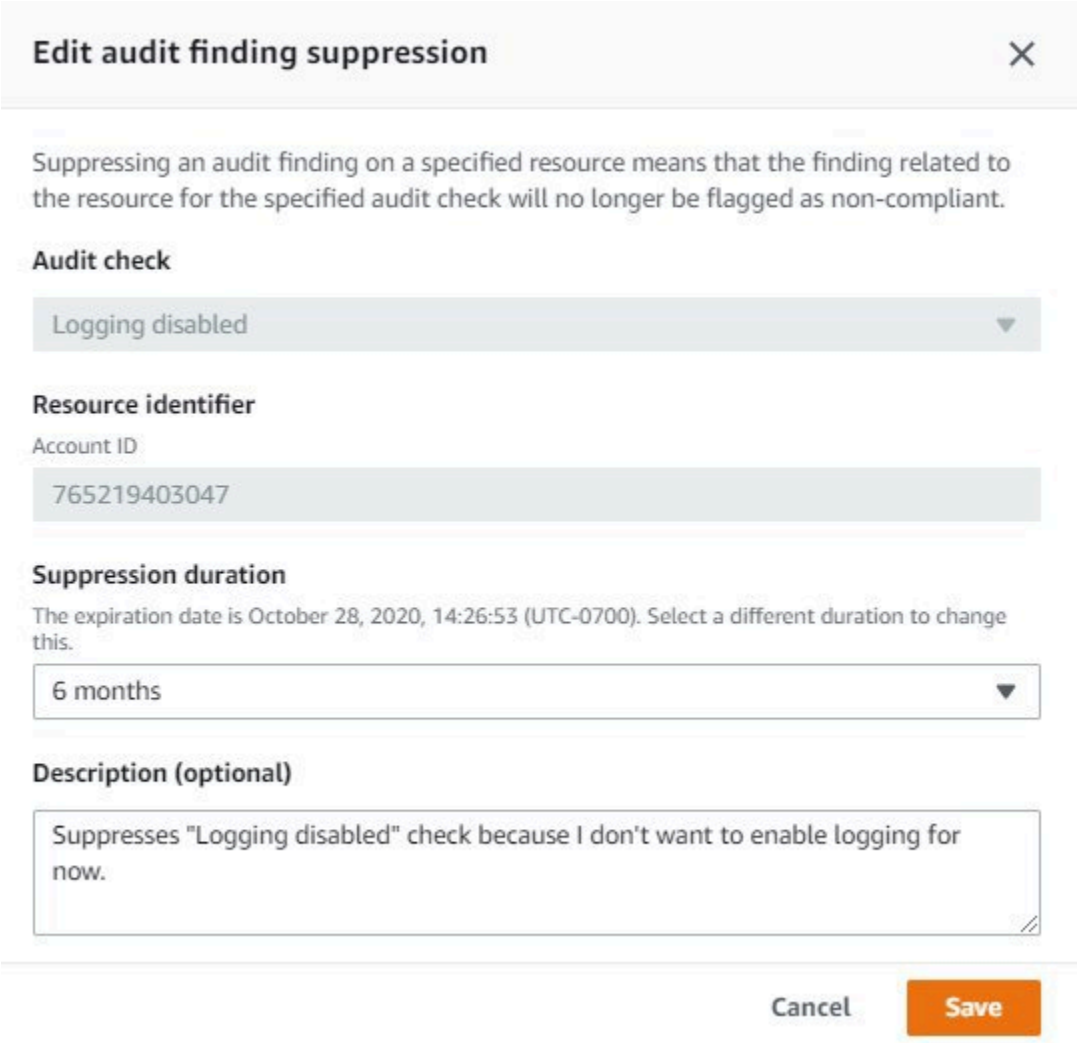
Per elencare le soppressioni della ricerca di audit

- Nell'AWS IoT console, nel riquadro di navigazione, espandi Defend (Protezione) e scegli Audit (Audit), Finding suppressions (Ricerca di eliminazione).



Per modificare la soppressione della ricerca di audit

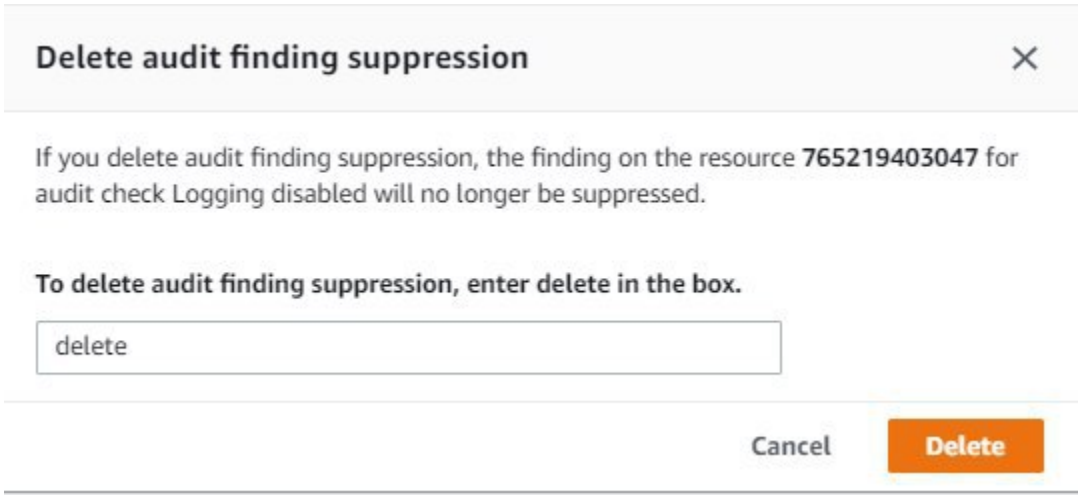
1. Nell'AWS IoT console, nel riquadro di navigazione, espandi Defend (Protezione) e scegli Audit (Audit), Finding suppressions (Ricerca di eliminazione).
2. Seleziona il pulsante di opzione accanto al tipo di soppressione dei risultati di audit che desideri modificare. Quindi, seleziona Actions (Operazioni), Edit (Modifica).
3. Sulla finestra Edit audit finding suppression (Modifica la soppressione della ricerca di audit) è possibile modificare Suppression duration (Durata della eliminazione) o Description (Descrizione) (facoltativa).



4. Dopo avere effettuato le modifiche, scegli Save (Salva). Si apre la finestra Finding suppressions (Ricerca di soppressioni).

Per eliminare una soppressione della ricerca di audit

1. Nell'AWS IoT console, nel riquadro di navigazione, espandi Defend (Protezione) e scegli Audit (Audit), Finding suppressions (Ricerca di eliminazione).
2. Seleziona il pulsante di opzione accanto alla soppressione della ricerca di audit da eliminare e quindi scegli Actions (Operazioni), Delete (Elimina).
3. Sulla finestra Delete audit finding suppression (Elimina la soppressione della ricerca di audit), immetti `delete` nella casella di testo per confermare l'eliminazione, quindi seleziona Delete (Elimina). Si apre la finestra Finding suppressions (Ricerca di soppressioni).



Come utilizzare le soppressioni della ricerca di audit nell'interfaccia della riga di comando

È possibile utilizzare i seguenti comandi CLI per creare e gestire le soppressioni dei risultati di audit.

- create-audit-suppression
- describe-audit-suppression
- update-audit-suppression
- delete-audit-suppression
- list-audit-suppressions

Il `resource-identifier` che immetti dipende dal `check-name` per cui stai sopprimendo i risultati. Nella tabella seguente sono riportati i dettagli che richiedono i controlli, quali i `resource-identifier` per la creazione e la modifica delle soppressioni.

> **Note**
>
> I comandi di soppressione non indicano la disattivazione di un audit. Gli audit continueranno a essere eseguiti sui tuoi dispositivi AWS IoT. Le soppressioni sono applicabili solo ai risultati dell'audit.

check-name	resource-identifier
AUTHENTICATE_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK	cognitoIdentityPoolId
CA_CERT_APPROACHING_EXPIRATION_CHECK	caCertificateId
CA_CERTIFICATE_KEY_QUALITY_CHECK	caCertificateId
CONFLICTING_CLIENT_IDS_CHECK	clientId
DEVICE_CERT_APPROACHING_EXPIRATION_CHECK	deviceCertificateId
DEVICE_CERTIFICATE_KEY_QUALITY_CHECK	deviceCertificateId
DEVICE_CERTIFICATE_SHARED_CHECK	deviceCertificateId
IOT_POLICY_OVERLY_PERMISSIVE_CHECK	policyVersionIdentifier
IOT_ROLE_ALIAS_ALLOWS_ACCESS_TO_UNUSED_SERVICES_CHECK	roleAliasArn
IOT_ROLE_ALIAS_OVERLY_PERMISSIVE_CHECK	roleAliasArn
LOGGING_DISABLED_CHECK	account
REVOKED_CA_CERT_CHECK	caCertificateId
REVOKED_DEVICE_CERT_CHECK	deviceCertificateId
UNAUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK	cognitoIdentityPoolId

Per creare e applicare una soppressione di ricerca di audit

La procedura seguente mostra come creare una soppressione della ricerca di audit nella CLI dei servizi AWS.

- Utilizza il comando `create-audit-suppression` per creare una soppressione della ricerca di audit. Nell'esempio seguente viene creata una soppressione della ricerca di audit per l'account Account AWS *123456789012* sulla base del controllo Registrazione disattivata.

  ```
  aws iot create-audit-suppression \
      --check-name LOGGING_DISABLED_CHECK \
      --resource-identifier account=123456789012 \
      --client-request-token 28ac32c3-384c-487a-a368-c7bbd481f554 \
      --suppress-indefinitely \
      --description "Suppresses logging disabled check because I don't want to enable
   logging for now."
  ```

  Non esiste un output per questo comando.

Ricerca di audit delle soppressioni delle API

Le seguenti API possono essere utilizzate per creare e gestire le soppressioni della ricerca di audit.

- CreateAuditSuppression
- DescribeAuditSuppression
- UpdateAuditSuppression
- DeleteAuditSuppression
- ListAuditSuppressions

Per filtrare per risultati specifici di audit, è possibile utilizzare l'API ListAuditFindings.

Rilevamento

AWS IoT Device Defender Detect consente di identificare un comportamento insolito che può indicare un dispositivo compromesso monitorando il comportamento dei dispositivi. Utilizzando una combinazione di parametri sul lato cloud (da AWS IoT) e metriche sul lato dispositivo (dagli agenti installati sui dispositivi) è possibile rilevare:

- Cambiamenti nei modelli di connessione.
- Dispositivi che comunicano a endpoint non autorizzati o non riconosciuti.
- Modifiche nei modelli di traffico del dispositivo in entrata e in uscita.

È possibile creare profili di sicurezza, che contengono definizioni dei comportamenti dei dispositivi previsti, e assegnarli a un gruppo di dispositivi o a tutti i dispositivi del parco istanze. AWS IoT Device Defender Detect utilizza questi profili di sicurezza per rilevare le anomalie e inviare allarmi tramite i parametri di Amazon CloudWatch e le notifiche di Amazon Simple Notification Service.

AWS IoT Device Defender Detect può rilevare problemi di sicurezza riscontrati frequentemente nei dispositivi connessi:

- Traffico da un dispositivo verso un indirizzo IP dannoso noto o verso un endpoint non autorizzato, che indica un canale di controllo e un comando potenzialmente dannosi.
- Traffico anomalo, ad esempio un picco del traffico in uscita, che indica che un dispositivo sta prendendo parte a un attacco DDoS.
- Dispositivi con interfacce di gestione remote e porte accessibili in remoto.
- Un picco nella frequenza dei messaggi inviati all'account, ad esempio da un dispositivo non autorizzato, che può comportare spese eccessive legate ai messaggi.

Casi d'uso:

Misurazione della superficie di attacco

Puoi usare AWS IoT Device Defender Detect per misurare la superficie di attacco dei dispositivi. Puoi ad esempio identificare i dispositivi con porte di servizio che sono spesso l'obiettivo di campagne di attacchi (servizio telnet in esecuzione sulle porte 23/2323, servizio SSH in esecuzione sulla porta 22, servizi HTTP/S in esecuzione sulle porte 80/443/8080/8081). Sebbene ci possano essere motivi legittimi per usare queste porte di servizio nei dispositivi, spesso tali

porte fanno parte della superficie di attacco per gli avversari e comportano rischi. Quando AWS IoT Device Defender Detect segnala una superficie di attacco, puoi scegliere di ridurla al minimo (eliminando i servizi di rete inutilizzati) oppure, puoi scegliere di eseguire ulteriori valutazioni per identificare le vulnerabilità della sicurezza (ad esempio, telnet configurato con password comuni, predefinite o poco sicure).

Rilevamento di anomalie nel comportamento dei dispositivi con le possibili cause principali legate alla sicurezza

Puoi usare AWS IoT Device Defender Detect per ricevere avvisi in caso di metriche impreviste relativi al comportamento dei dispositivi (numero di porte aperte, numero di connessioni, presenza di una porta aperta non prevista, connessioni a indirizzi IP non previsti) che potrebbero indicare una violazione della sicurezza. Un numero di connessioni TCP maggiore del previsto può ad esempio indicare un dispositivo usato per un attacco DDoS. Un processo in ascolto su una porta diversa da quella prevista può indicare una backdoor installata in un dispositivo per il controllo remoto. Puoi usare AWS IoT Device Defender Detect per esaminare lo stato del parco istanze di dispositivi e verificare i presupposti di sicurezza (ad esempio, nessun dispositivo deve essere in ascolto sulla porta 23 o 2323).

È possibile abilitare il rilevamento delle minacce basato su machine learning (ML) per identificare automaticamente le potenziali minacce.

Rileva un dispositivo non configurato correttamente

Un picco nel numero o nelle dimensioni dei messaggi inviati da un dispositivo all'account può indicare un'errata configurazione del dispositivo. Tale dispositivo potrebbe causare un aumento dei costi per i messaggi. Analogamente, un dispositivo con numerosi errori di autorizzazione potrebbe richiedere una nuova configurazione della policy.

Monitoraggio del comportamento dei dispositivi non registrati

AWS IoT Device Defender Detect consente di identificare comportamenti insoliti per i dispositivi che non vengono registrati nel registro AWS IoT. È possibile definire i profili di sicurezza specifici per uno dei seguenti tipi di destinazione:

- Tutti i dispositivi
- Tutti i dispositivi registrati (oggetti nel registro AWS IoT)
- Tutti i dispositivi non registrati
- Dispositivi in un gruppo di oggetti

Un profilo di sicurezza definisce una serie di comportamenti attesi per i dispositivi nel tuo account e specifica le azioni da eseguire quando viene rilevata un'anomalia. I profili di sicurezza devono essere collegati ai target più specifici per conferirti il controllo granulare su quali dispositivi sono valutati rispetto a tale profilo.

I dispositivi non registrati devono fornire un identificatore client MQTT coerente o un nome oggetto (per dispositivi che segnalano i parametri di dispositivo) per la durata di vita del dispositivo, in modo che tutte le violazioni e i parametri siano attribuiti allo stesso dispositivo.

> **Important**
>
> I messaggi riportati dai dispositivi sono rifiutati se il nome dell'oggetto contiene caratteri di controllo oppure se il nome dell'oggetto è più lungo di 128 byte di caratteri di codifica UTF-8.

Casi d'uso della sicurezza

In questa sezione vengono descritti i diversi tipi di attacchi che minacciano il parco istanze del tuo dispositivo e i parametri consigliati che è possibile utilizzare per monitorare tali attacchi. Ti consigliamo di utilizzare le anomalie dei parametri come punto di partenza per analizzare i problemi di sicurezza, ma non devi basare la tua determinazione di eventuali minacce alla sicurezza esclusivamente su un'anomalia metrica.

Per analizzare un allarme di anomalia, correla i dettagli dell'allarme con altre informazioni contestuali, ad esempio attributi del dispositivo, tendenze cronologiche dei parametri del dispositivo, tendenze cronologiche dei parametri del profilo di sicurezza, parametri personalizzati e registri per determinare se è presente una minaccia per la sicurezza.

Casi d'uso lato cloud

Device Defender è in grado di monitorare i seguenti casi d'uso nel lato cloud di AWS IoT.

Furto di proprietà intellettuale:

Il furto di proprietà intellettuale comporta il furto delle proprietà intellettuali di una persona o azienda, tra cui segreti commerciali, hardware o software. Spesso si verifica durante la fase di produzione dei dispositivi. Il furto di proprietà intellettuale può presentarsi sotto forma di pirateria, furto di dispositivi o furto di certificati di dispositivo. Il furto della proprietà intellettuale basata sul

cloud può verificarsi a causa della presenza di policy che consentono l'accesso non intenzionale alle risorse IoT. È necessario rivedere le Policy IoT e attivare Audit eccessivamente permissivi per identificare policy eccessivamente permissive.

Parametri correlati:

Parametro	Rationale
IP di origine	Se il dispositivo viene rubato, il suo indirizzo IP di origine non rientrerebbe nell'intervallo di indirizzi IP normalmente previsto per i dispositivi circolati in una normale catena di fornitura.
Numero di messaggi ricevuti	Poiché un utente malintenzionato può utilizzare un dispositivo rubato basato su IP cloud, le metriche relative al conteggio dei messaggi o alle dimensioni dei messaggi inviati al dispositivo da AWS IoT cloud possono aumentare, indicando un possibile problema di sicurezza.
Dimensione dei messaggi	

Esfiltrazione dei dati basata su MQTT:

L'esfiltrazione dei dati avviene quando un utente malintenzionato effettua un trasferimento di dati non autorizzato da una distribuzione IoT o da un dispositivo. L'aggressore lancia questo tipo di attacchi tramite MQTT contro origini dati sul cloud.

Parametri correlati:

Parametro	Rationale
IP di origine	Se un dispositivo viene rubato, l'indirizzo IP di origine non rientra nell'intervallo di indirizzi IP normalmente previsto per i dispositivi circolati in una catena di fornitura standard.
Numero di messaggi ricevuti	Poiché un utente malintenzionato può utilizzare un dispositivo rubato basato su IP cloud, i

Parametro	Rationale
Dimensione dei messaggi	parametri relativi al conteggio dei messaggi o alle dimensioni dei messaggi inviati al dispositivo da AWS IoT cloud possono aumentare, indicando un possibile problema di sicurezza.

Rappresentazione:

Un attacco di rappresentazione è il luogo in cui gli attaccanti si pongono come entità note o attendibili nel tentativo di accedere ai servizi AWS IoT sul cloud, applicazioni, dati o impegnarsi nel comando e nel controllo dei dispositivi IoT.

Parametri correlati:

Parametro	Rationale
Errori di autorizzazione	Quando gli utenti malintenzionati si pongono come entità attendibili utilizzando identità rubate, i parametri relativi alla connettività spesso aumentano, poiché le credenziali potrebbero non essere più valide o potrebber o essere già utilizzate da un dispositivo attendibile. I comportamenti anomali in caso di errori di autorizzazione, tentativi di connessione o disconnessione, indicano un potenziale scenario di rappresentazione.
Tentativi di connessione	
Disconnessioni	

Uso illecito dell'infrastruttura cloud:

Un abuso dei servizi AWS IoT cloud si verifica quando si pubblicano o si sottoscrivono argomenti con un volume elevato di messaggi o con messaggi di grandi dimensioni. Anche criteri eccessivamente permissivi o exploit di vulnerabilità dei dispositivi per comando e controllo possono causare abusi dell'infrastruttura cloud. Uno degli obiettivi principali di questo attacco è quello di aumentare il tuo conto dei servizi AWS. È necessario rivedere le Policy IoT e attivare Controlli eccessivamente permissivi per identificare policy eccessivamente permissive.

Parametri correlati:

Parametro	Rationale
Numero di messaggi ricevuti	L'obiettivo di questo attacco è quello di aumentare il tuo conto dei servizi AWS. Le metriche che monitorano attività come il conteggio dei messaggi, i messaggi ricevuti e le dimensioni dei messaggi verranno aumentate.
Numero di messaggi inviati	
Dimensione dei messaggi	
IP di origine	Possono essere visualizzati elenchi IP di origine sospetta, da cui gli utenti malintenz ionati generano il loro volume di messaggis tica.

Casi d'uso lato dispositivo

Device Defender è in grado di monitorare i seguenti casi d'uso su lato dispositivo.

Denial-of-Service attack (Attacco Denial of Service (DoS)):

Un attacco DoS (Denial of Service) mira ad arrestare un dispositivo o una rete, rendendo il dispositivo o la rete inaccessibile agli utenti previsti. Gli attacchi DoS bloccano l'accesso inondando la destinazione di traffico, o inviando richieste che avviano un sistema e rallentano o provocano un guasto del sistema. I dispositivi IoT possono essere sfruttati durante gli attacchi DoS.

Parametri correlati:

Parametro	Rationale
Pacchetti in uscita	Gli attacchi DoS in genere comportano tassi più elevati di comunicazione in uscita da un determinato dispositivo e, a seconda del tipo di attacco DoS, potrebbe esserci un aumento di uno o entrambi i numeri di pacchetti e byte in uscita.
Byte in uscita	

Parametro	Rationale
IP di destinazione	Se si definiscono gli indirizzi IP/intervalli CIDR con cui i dispositivi devono comunicare, un'anomalia nell'IP di destinazione può indicare una comunicazione IP non autorizzata dai dispositivi.
Porte TCP in ascolto	Un attacco DoS richiede solitamente un'infrastruttura di comando e controllo più ampia, in cui il malware installato sui dispositivi riceve comandi e informazioni su chi attaccare e quando attaccare. Pertanto, per ricevere tali informazioni, il malware in genere ascolta su porte che normalmente non vengono utilizzate dai dispositivi.
Conteggio porte TCP in ascolto	
Porte UDP in ascolto	
Conteggio porte UDP in ascolto	

Escalation delle minacce laterali:

L'escalation delle minacce laterali di solito inizia con un utente malintenzionato che accede a un punto di una rete, ad esempio un dispositivo connesso. L'utente malintenzionato tenta quindi di aumentare il proprio livello di privilegi, o l'accesso ad altri dispositivi, attraverso metodi come un furto di credenziali o exploit di vulnerabilità.

Parametri correlati:

Parametro	Rationale
Pacchetti in uscita	In situazioni tipiche, l'utente malintenzionato dovrebbe eseguire una scansione sulla rete locale al fine di eseguire la ricognizione e identificare i dispositivi disponibili al fine di restringere la selezione del bersaglio di attacco. Questo tipo di scansione potrebbe comportare un picco nei conteggi di byte e di pacchetti in uscita.
Byte in uscita	

Parametro	Rationale
IP di destinazione	Se supponiamo che un dispositivo comunichi con un insieme noto di indirizzi IP o CIDR, sarà possibile identificare i tentativi di comunicazione con un indirizzo IP anomalo, solitamente rappresentato da un indirizzo IP privato sulla rete locale in un caso d'uso di escalation di minacce laterali.
Errori di autorizzazione	Poiché l'utente malintenzionato tenta di aumentare il proprio livello di privilegi su una rete IoT, può utilizzare credenziali rubate che sono state revocate o scadute, provocando un incremento degli errori di autorizzazione.

Esfiltrazione o sorveglianza dei dati:

L'esfiltrazione dei dati avviene quando malware o un attore malintenzionato effettua un trasferimento di dati non autorizzato da un dispositivo o da un endpoint di rete. L'esfiltrazione dei dati serve normalmente a due scopi per l'autore dell'attacco: ottenere dati o proprietà intellettuale o condurre la ricognizione di una rete. Per sorveglianza si intende l'utilizzo di un codice dannoso per monitorare le attività degli utenti, allo scopo di rubare credenziali e raccogliere informazioni. I parametri riportate di seguito possono fornire un punto di partenza per indagare su entrambi i tipi di attacchi.

Parametri correlati:

Parametro	Rationale
Pacchetti in uscita	Quando si verificano attacchi di esfiltrazione dei dati o sorveglianza, l'utente malintenz ionato spesso rispecchia i dati inviati dal dispositivo piuttosto che semplicemente reindirizzarli, in modo da non essere identific ato dal difensore quando non vede arrivare i dati previsti. Questo mirroring dei dati aumenterebbe significativamente la quantità
Byte in uscita	

Parametro	Rationale
	totale di dati inviati dal dispositivo, con conseguente picco nei conteggi di pacchetti e byte in uscita.
IP di destinazione	Quando un utente malintenzionato utilizza un dispositivo per attacchi di esfiltrazione o sorveglianza, i dati devono essere inviati a un indirizzo IP anormale controllato dall'utente malintenzionato. Il monitoraggio dell'IP di destinazione può aiutare a identificare tale attacco.

Mining di criptovalute

Gli aggressori sfruttano la potenza di elaborazione dei dispositivi per estrarre criptovaluta. Il crypto-mining è un processo computazionale intensivo, che richiede in genere una comunicazione di rete con altri peer e pool mining.

Parametri correlati:

Parametro	Rationale
IP di destinazione	La comunicazione di rete è in genere un requisito necessario per il cryptomining. Avere un elenco strettamente controllato di indirizzi IP con cui il dispositivo deve comunicare può aiutare a identificare le comunicazioni non intenzionali su un dispositivo, come nel caso del mining di criptovalute.
Utilizzo CPU Parametri personalizzati	Il mining delle criptovalute richiede un calcolo intensivo con conseguente utilizzo elevato della CPU del dispositivo. Se si sceglie di raccogliere e monitorare questo parametro, un utilizzo della CPU superiore al normale

Parametro	Rationale
	potrebbe essere un indicatore delle attività di crypto-mining.

Comando e controllo, malware e ransomware

Il malware o il ransomware limitano il controllo dell'utente sui dispositivi e limitano le funzionalità del dispositivo. Nel caso di un attacco ransomware, l'utente perderebbe l'accesso ai dati andrebbe a causa della crittografia utilizzata dal ransomware.

Parametri correlati:

Parametro	Rationale
IP di destinazione	Gli attacchi di rete o remoti rappresentano una gran parte degli attacchi sui dispositi vi IoT. Un elenco strettamente controlla to di indirizzi IP con cui il dispositivo deve comunicare può aiutare a identificare IP di destinazione anomali derivanti da un attacco malware o ransomware.
Porte TCP in ascolto	Diversi attacchi malware prevedono l'avvio di un server di comando e controllo, che invia una serie di comandi da eseguire su un dispositivo. Questo tipo di server è fondamentale per un'operazione di malware o ransomware, e può essere identificato monitorando strettamente le porte TCP/UDP aperte e il conteggio delle porte.
Conteggio porte TCP in ascolto	
Porte UDP in ascolto	
Conteggio porte UDP in ascolto	

Concetti

parametro

AWS IoT Device Defender Detect usa i parametri per rilevare un comportamento anomalo. AWS IoT Device Defender Detect confronta il valore segnalato per un parametro con il valore previsto

fornito. Questi parametri possono essere ricavati da due origini: parametri lato cloud e parametri lato dispositivo. ML Detect supporta 6 metriche lato cloud e 7 metriche lato dispositivo. Per un elenco delle metriche supportate per ML Detect, consulta Parametri supportati.

Un comportamento anomalo nella rete AWS IoT viene rilevato usando i parametri lato cloud, come il numero di errori di autorizzazione oppure il numero o la dimensione dei messaggi inviati o ricevuti da un dispositivo mediante AWS IoT.

AWS IoT Device Defender Detect, inoltre, è in grado di raccogliere, aggregare e monitorare i dati delle metriche generate dai dispositivi AWS IoT (ad esempio le porte su cui un dispositivo è in ascolto, il numero di byte o di pacchetti inviati o le connessioni TCP del dispositivo).

Puoi usare AWS IoT Device Defender Detect solo con i parametri lato cloud. Per usare i parametri lato dispositivo, devi prima distribuire un SDK AWS IoT nei gateway dei dispositivi o nei dispositivi connessi a AWS IoT per raccogliere i parametri e inviarli a AWS IoT. Per informazioni, consulta Invio di parametri dai dispositivi.

Profilo di sicurezza

Un profilo di sicurezza definisce i comportamenti anomali per un gruppo di dispositivi (un gruppo di oggetti statici) o per tutti i dispositivi nell'account e specifica le operazioni da eseguire quando viene rilevata un'anomalia. È possibile utilizzare l'AWS IoT console o i comandi API per creare un profilo di sicurezza e associarlo a un gruppo di dispositivi. AWS IoT Device Defender Detect avvia la registrazione dei dati correlati alla sicurezza e usa i comportamenti definiti nel profilo di sicurezza per rilevare le anomalie nel comportamento dei dispositivi.

comportamento

Un comportamento indica a AWS IoT Device Defender Detect come riconoscere un comportamento anomalo di un dispositivo. Qualsiasi operazione del dispositivo che non corrisponde a un comportamento, attiva un avviso. Un comportamento Rules Detect è costituito da un parametro e da una soglia di valore assoluto o statistica con un operatore (ad esempio, minore o uguale a, maggiore o uguale a), che descrivono il comportamento previsto del dispositivo. Un comportamento ML Detector consiste in un parametro e una configurazione che definisce un modello ML per apprendere il normale comportamento dei dispositivi.

modello di ML

Un modello ML è un modello di machine learning creato per monitorare ogni comportamento configurato dal cliente. Il modello si allena su modelli di dati di parametri provenienti da gruppi di dispositivi mirati e genera tre soglie di confidenza delle anomalie (alta, media e bassa) per il comportamento basato sui parametri. Induce anomalie in base ai dati di parametri ingeriti a

livello di dispositivo. Nel contesto di ML Detect, viene creato un modello ML per valutare un comportamento basato sui parametri. Per ulteriori informazioni, consultare Rilevamento ML.

livello di confidenza

ML Detect supporta tre livelli di confidenza: `High`, `Medium`, e `Low`. `High` fiducia significa bassa sensibilità nella valutazione del comportamento anomalo e spesso un numero inferiore di allarmi. `Medium` fiducia significa sensibilità media e `Low` fiducia significa alta sensibilità e frequentemente un maggior numero di allarmi.

dimensione

È possibile definire una dimensione per regolare l'ambito di un comportamento. Ad esempio, è possibile definire una dimensione del filtro argomento che applica un comportamento agli argomenti MQTT corrispondenti a un modello. Per informazioni sulla definizione di una dimensione da utilizzare in un profilo di sicurezza, consulta CreateDimension.

allarme

Quando viene rilevata un'anomalia, è possibile inviare una notifica di allarme tramite un parametro CloudWatch (consulta Monitorare allarmi e metriche di AWS IoT utilizzando Amazon CloudWatch nella Guida per gli sviluppatori di AWS IoT Core) o una notifica SNS. Una notifica di allarme viene visualizzata anche nell'AWS IoT console insieme a informazioni aggiuntive sull'allarme e a una cronologia degli allarmi per il dispositivo. Viene inviato un allarme anche quando un dispositivo monitorato smette di presentare un comportamento anomalo oppure quando ha provocato la generazione di un allarme ma la segnalazione non avviene più per un lungo periodo di tempo.

stato di verifica dell'allarme

Dopo aver creato un allarme, è possibile classificarlo come True positive (Vero positivo), Benign positive (Benigno positivo), False positive (Falso positivo) o Unknown (Sconosciuto). Puoi anche aggiungere una descrizione allo stato di verifica dell'allarme. È possibile visualizzare, organizzare e filtrare gli allarmi AWS IoT Device Defender utilizzando uno dei quattro stati di verifica. Puoi utilizzare gli stati di verifica degli allarmi e le relative descrizioni per informare i membri del tuo team. Questo aiuta il tuo team a intraprendere azioni di follow-up, ad esempio eseguire azioni di mitigazione su allarmi veri positivi, ignorare allarmi positivi benigni o continuare le verifiche su allarmi sconosciuti. Lo stato di verifica di default per tutti gli allarmi è Unknown (Sconosciuto).

Soppressione degli allarmi

Gestisci Rileva notifiche SNS di allarme impostando la notifica di comportamento su on o `suppressed`. La soppressione degli allarmi non impedisce a Detect di eseguire valutazioni sul comportamento dei dispositivi; Detect continua a contrassegnare i comportamenti anomali come

allarmi di violazione. Tuttavia, gli allarmi soppressi non verranno inoltrati per la notifica SNS. Sono accessibili solo tramite l'AWS IoT console o API.

Comportamenti

Un profilo di sicurezza contiene un set di comportamenti. Ciascun comportamento contiene un parametro che specifica il comportamento normale per un gruppo di dispositivi o per tutti i dispositivi nell'account. I comportamenti rientrano in due categorie: comportamenti Rules Detect e ML Detect. Con Rules Detect comportamenti è possibile definire il comportamento dei dispositivi mentre ML Detect utilizza modelli ML basati su dati cronologici dei dispositivi per valutarne il comportamento.

Un profilo di sicurezza può avere uno dei due tipi di soglia: ML o Basato su regole. I profili di sicurezza ML rilevano automaticamente le anomalie operative e di sicurezza a livello di dispositivo nel parco istanze, imparando dai dati passati. I profili di sicurezza basati su regole richiedono l'impostazione manuale di regole statiche, utili a monitorare i comportamenti del dispositivo.

Di seguito sono descritti alcuni dei campi utilizzati nella definizione di `behavior`:

Comune a Rules Detect e ML Detect

`name`

Il nome per il comportamento.

`metric`

Il nome del parametro utilizzato (ovvero, ciò che è misurato dal comportamento).

`consecutiveDatapointsToAlarm`

Se un dispositivo viola un comportamento per un numero specificato di datapoint consecutivi, viene attivato un allarme. Se il valore non viene specificato, viene usato il valore predefinito 1.

`consecutiveDatapointsToClear`

Se si è verificato un allarme e il dispositivo in questione non viola più il comportamento per il numero specificato di datapoint consecutivi, l'allarme viene cancellato. Se il valore non viene specificato, viene usato il valore predefinito 1.

`threshold type`

Un profilo di sicurezza può avere uno tra questi due tipi di soglia: ML (Machine Learning) o Rules based (Basato su regole). I profili di sicurezza ML rilevano automaticamente le anomalie operative

e di sicurezza a livello di dispositivo nel parco istanze imparando dai dati passati. I profili di sicurezza basati su regole richiedono l'impostazione manuale di regole statiche, utili a monitorare i comportamenti del dispositivo.

`alarm suppressions`

Puoi gestire Rileva notifiche SNS di allarme impostando la notifica di comportamento su on o `suppressed`. La soppressione degli allarmi non impedisce a Detect di eseguire valutazioni sul comportamento dei dispositivi; Detect continua a contrassegnare i comportamenti anomali come allarmi di violazione. Tuttavia, gli allarmi soppressi non vengono inoltrati per la notifica Amazon SNS. È possibile accedervi solo attraverso l'AWS IoT console o API.

Rules Detect

`dimension`

È possibile definire una dimensione per regolare l'ambito di un comportamento. Ad esempio, è possibile definire una dimensione del filtro argomento che applica un comportamento agli argomenti MQTT corrispondenti a un modello. Per definire una dimensione da utilizzare in un profilo di sicurezza, consulta CreateDimension. Si applica solo a Rules Detect.

`criteria`

Criteri che determinano se un dispositivo presenta un comportamento normale in relazione a `metric`.

> **Note**
>
> Nella console AWS IoT, puoi scegliere Avvisami per ricevere una notifica tramite Amazon SNS quando AWS IoT Device Defender rileva che un dispositivo si comporta in modo anomalo.

`comparisonOperator`

Operatore che mette in correlazione l'oggetto misurato (`metric`) e i criteri (`value` o `statisticalThreshold`).

I possibili valori sono: "less-than", "less-than-equals", "greater-than", "greater-than-equals", "in-cidr-set", "not-in-cidr-set", "in-port-set", and "not-in-port-set". Non tutti gli operatori sono validi

per ogni parametro. Operatori per set di CIDR e porte sono solo per l'uso con i parametri che riguardano tali entità.

`value`

Valore da confrontare con `metric`. A seconda del tipo di parametro, questo dovrebbe contenere un `count` (un valore), `cidrs` (un elenco di CIDR) o `ports` (un elenco di porte).

`statisticalThreshold`

La soglia statistica in base alla quale viene determinata una violazione del comportamento. Il campo contiene un campo `statistic` che dispone dei seguenti valori possibili: "p0", "p0.1", "p0.01", "p1", "p10", "p50", "p90", "p99", "p99.9", "p99.99" o "p100".

`statistic` indica un percentile. Restituisce un valore in base al quale viene determinata la conformità con il comportamento. I parametri vengono raccolti una o più volte nell'arco della durata specificata (`durationSeconds`) da tutti i dispositivi di segnalazione associati a questo profilo di sicurezza e le percentuali vengono calcolate in base a tali dati. Dopodiché, le misure vengono raccolte per un dispositivo e accumulate nell'arco della stessa durata. Se il valore risultante per il dispositivo è sopra o sotto (`comparisonOperator`) il valore associato al percentile specificato, il dispositivo è considerato conforme al comportamento. In caso contrario, il dispositivo è considerato in violazione del comportamento.

Un percentile indica la percentuale di tutte le misurazioni considerate che sono inferiori al valore associato. Ad esempio, se il valore associato a "p90" (il novantesimo percentile) è 123, il 90% di tutte le misurazioni è inferiore a 123.

`durationSeconds`

Usa questo parametro per specificare il periodo di tempo durante cui viene valutato il comportamento, per i criteri che hanno una dimensione temporale (ad esempio, `NUM_MESSAGES_SENT`). Per un confronto di parametri `statisticalThreshhold`, questo è il periodo di tempo durante il quale le misurazioni vengono raccolte per tutti i dispositivi per determinare i valori `statisticalThreshold` e quindi per ogni dispositivo per determinare come si posiziona il comportamento nel confronto.

ML Detect

`ML Detect confidence`

ML Detect supporta tre livelli di confidenza: `High`, `Medium`, e `Low`. `High` fiducia significa bassa sensibilità nella valutazione del comportamento anomalo e spesso un numero inferiore di allarmi,

`Medium` fiducia significa sensibilità media, e `Low` fiducia significa alta sensibilità e frequentemente un maggior numero di allarmi.

Rilevamento ML

Con il rilevamento di Machine Learning (ML Detect), puoi creare profili di sicurezza che utilizzano l'apprendimento automatico per apprendere i comportamenti previsti dei dispositivi creando automaticamente modelli basati sui dati cronologici dei dispositivi e assegnare questi profili a un gruppo di dispositivi o a tutti i dispositivi del tuo parco istanze. AWS IoT Device Defender identificherà quindi le anomalie e attiverà gli allarmi utilizzando i modelli ML.

Per ulteriori informazioni su come iniziare a utilizzare ML Detect, consulta Guida a ML Detect.

Questo capitolo contiene le sezioni seguenti:

- Casi d'uso di ML Detect
- Come funziona ML Detect
- Requisiti minimi
- Limitazioni
- Contrassegno di falsi positivi e altri stati di verifica degli allarmi
- Parametri supportati
- Quote del servizio
- Comandi dell'interfaccia a riga di comando di ML Detect
- API di ML Detect
- Sospendere o eliminare un profilo di sicurezza ML Detect

Casi d'uso di ML Detect

È possibile utilizzare ML Detect per monitorare i dispositivi del parco istanze nel caso in cui sia difficile impostare i comportamenti previsti dei dispositivi. Ad esempio, per monitorare i parametri del numero di disconnessioni, potrebbe non essere chiaro quale sia considerata una soglia accettabile. In questo caso, è possibile abilitare ML Detect per identificare i datapoint dei parametri di disconnessione anomala in base ai dati cronologici segnalati dai dispositivi.

Un altro caso d'uso di ML Detect consiste nel monitorare i comportamenti dei dispositivi che cambiano dinamicamente nel tempo. ML Detect apprende in modo periodico i comportamenti

dinamici attesi del dispositivo, in base alle modifiche dei modelli di dati forniti dai dispositivi. Ad esempio, se il volume di messaggi inviati dal dispositivo registra variazioni tra i giorni feriali e i fine settimana, ML Detect apprenderà questo comportamento dinamico.

Come funziona ML Detect

Utilizzando ML Detect, è possibile creare comportamenti per identificare anomalie operative e di sicurezza in 6 parametri sul lato cloud e 7 parametri lato dispositivo. Dopo il periodo iniziale di formazione del modello, ML Detect aggiorna i modelli ogni giorno in base ai dati degli ultimi 14 giorni. Monitora i datapoint per questi parametri con i modelli ML e attiva un allarme se viene rilevata un'anomalia.

Il funzionamento di ML Detect può essere migliorato se si collega un profilo di sicurezza a una raccolta di dispositivi con comportamenti attesi simili. Ad esempio, se alcuni dei tuoi dispositivi vengono utilizzati nelle case dei clienti e altri dispositivi negli uffici aziendali, i modelli di comportamento del dispositivo potrebbero differire significativamente tra i due gruppi. È possibile organizzare i dispositivi in un gruppo di oggetti dispositivo home e un gruppo di oggetti dispositivo da ufficio. Per una migliore efficacia del rilevamento delle anomalie, collega ogni gruppo di elementi a un profilo di sicurezza ML Detect separato.

Per costruire il modello iniziale, ML Detect richiede 14 giorni e un minimo di 25.000 datapoint per parametro nel periodo dei 14 giorni per generare un modello. Successivamente, aggiorna il modello ogni giorno in cui è presente un numero minimo di datapoint dei parametri. Se il requisito minimo non viene soddisfatto, ML Detect tenta di creare il modello il giorno successivo. Il tentativo sarà ripetuto ogni giorno per i successivi 30 giorni, dopodiché il modello verrà interrotto per le opportune valutazioni.

Requisiti minimi

Per la formazione e la creazione del modello ML iniziale, ML Detect possiede i seguenti requisiti minimi.

Periodo di formazione minimo

Occorrono 14 giorni prima che i modelli iniziali vengano creati. Successivamente, il modello viene aggiornato ogni giorno con i dati dei parametri di un periodo finale di 14 giorni.

Totale minimo di datapoint

I datapoint minimi necessari per creare un modello ML sono 25.000 per metrica per gli ultimi 14 giorni. Per la formazione continua e l'aggiornamento del modello, ML Detect richiede

che i dispositivi monitorati soddisfino i dati minimi. È all'incirca l'equivalente delle seguenti configurazioni:

- 60 dispositivi che si connettono e hanno attività su AWS IoT ad intervalli di 45 minuti.
- 40 dispositivi a intervalli di 30 minuti.
- 15 dispositivi a intervalli di 10 minuti.
- 7 dispositivi a intervalli di 5 minuti.

Obiettivi del gruppo di dispositivi

Per raccogliere i dati, è necessario disporre di oggetti nei gruppi di oggetti di destinazione per il profilo di sicurezza.

Dopo la creazione del modello iniziale, i modelli ML si aggiornano ogni giorno e richiedono almeno 25.000 datapoint per un periodo di 14 giorni.

Limitazioni

È possibile utilizzare ML Detect con le dimensioni sui seguenti parametri lato cloud:

- Errori di autorizzazione (aws:num-authorization-failures)
- Messaggi ricevuti (aws:num-messages-received)
- Messaggi inviati (aws:num-messages-sent)
- Dimensioni del messaggio (aws:message-byte-size)

I seguenti parametri non sono supportati con ML Detect.

Parametri sul lato cloud non supportati con ML Detect:

- IP di origine (aws:source-ip-address)

Parametri sul lato dispositivo non supportati con ML Detect:

- IP di destinazione (`aws:destination-ip-addresses`)
- Porte TCP in ascolto (`aws:listening-tcp-ports`)
- Porte UDP in ascolto (`aws:listening-udp-ports`)

I parametri personalizzati supportano solo il tipo numero.

Contrassegno di falsi positivi e altri stati di verifica degli allarmi

Se durante l'indagine risulta che un allarme ML Detect in realtà è un falso positivo, è possibile impostare lo stato di verifica dell'allarme su False positive (Falso positivo). Questo aiuta te e il tuo team a identificare gli allarmi da ignorare. È inoltre possibile contrassegnare gli allarmi come True positive (Vero positivo), Benign positive (Benigno positivo) o Unknown (Sconosciuto).

È possibile contrassegnare gli allarmi tramite la console AWS IoT Device Defender o attraverso l'operazione API PutVerificationStateOnViolation.

Parametri supportati

Puoi utilizzare i seguenti parametri sul lato cloud con ML Detect:

- Errori di autorizzazione (aws:num-authorization-failures)
- Tentativi di connessione (aws:num-connection-attempts)
- Disconnessioni (aws:num-disconnects)
- Dimensioni del messaggio (aws:message-byte-size)
- Messaggi inviati (aws:num-messages-sent)
- Messaggi ricevuti (aws:num-messages-received)

Puoi utilizzare i seguenti parametri sul lato dispositivo con ML Detect:

- Byte in uscita (`aws:all-bytes-out`)
- Byte in entrata (`aws:all-bytes-in`)
- Conteggio di porte TCP in ascolto (`aws:num-listening-tcp-ports`)
- Conteggio porte UDP in ascolto (`aws:num-listening-udp-ports`)
- Pacchetti in uscita (`aws:all-packets-out`)
- Pacchetti in entrata (`aws:all-packets-in`)
- Conteggio delle connessioni TCP stabilite (`aws:num-established-tcp-connections`)

Quote del servizio

Per informazioni su ML Detect quote e limiti di servizio, consulta AWS IoT Device Defender endpoint e quote.

Comandi dell'interfaccia a riga di comando di ML Detect

Puoi utilizzare i comandi CLI; seguenti per creare e gestire ML Detect.

- create-security-profile
- attach-security-profile
- list-security-profiles
- describe-security-profile
- update-security-profile
- delete-security-profile
- get-behavior-model-training-summaries
- list-active-violations
- list-violation-events

API di ML Detect

Le seguenti API possono essere utilizzate per creare e gestire profili di sicurezza di ML Detect.

- CreateSecurityProfile
- AttachSecurityProfile
- ListSecurityProfiles
- DescribeSecurityProfile
- UpdateSecurityProfile
- DeleteSecurityProfile
- GetBehaviorModelTrainingSummaries
- ListActiveViolations
- ListViolationEvents
- PutVerificationStateOnViolation

Sospendere o eliminare un profilo di sicurezza ML Detect

È possibile sospendere il profilo di sicurezza ML Detect per interrompere temporaneamente il monitoraggio dei comportamenti dei dispositivi oppure eliminare il profilo di sicurezza ML Detect per interrompere il monitoraggio dei comportamenti dei dispositivi per un periodo di tempo prolungato.

Sospensione del profilo di sicurezza ML Detect utilizzando la console

Per mettere in pausa un profilo di sicurezza ML Detect utilizzando la console, è necessario disporre di un gruppo di oggetti vuoto. Per creare un gruppo di oggetti vuoto, consulta Gruppi di oggetti statici nella Guida per gli sviluppatori di AWS IoT Core. Se è stato creato un gruppo di oggetti vuoto, impostalo come destinazione del profilo di sicurezza ML Detect.

> **Note**
>
> Devi impostare la destinazione del tuo profilo di sicurezza su un gruppo di dispositivi entro 30 giorni o, altrimenti, non sarà possibile riattivare il profilo di sicurezza.

Eliminazione del profilo di sicurezza ML Detect utilizzando la console

Per eliminare un profilo di sicurezza, attieniti alla seguente procedura:

1. Nella console di navigazione AWS IoT sulla barra laterale, scegli la sezione Defend (Protezione).
2. In Defend (Protezione), scegli Detect (Rilevamento) e poi Security Profiles (Profili di sicurezza).
3. Scegli il profilo di sicurezza ML Detect da eliminare.
4. Scegli Actions (Operazioni) e poi Delete (Elimina) dalle opzioni.

> **Note**
>
> Dopo aver eliminato un profilo di sicurezza ML Detect, non sarà possibile riattivarlo.

Sospensione del profilo di sicurezza ML Detect utilizzando l'interfaccia a riga di comando

Per mettere in pausa un profilo di sicurezza ML Detect utilizzando l'interfaccia della riga di comando, utilizza il comando `detach-security-security-profile`:

```
$aws iot detach-security-profile --security-profile-name SecurityProfileName --
security-profile-target-arn arn:aws:iot:us-east-1:123456789012:all/registered-things
```

> **Note**
>
> Questa caratteristica è disponibile solo nella versione CLI dei servizi AWS. In modo analogo rispetto al flusso di lavoro della console, è necessario impostare la destinazione del profilo di sicurezza su un gruppo di dispositivi entro 30 giorni, altrimenti non sarà possibile riattivare il profilo di sicurezza. Per collegare un profilo di sicurezza a un gruppo di dispositivi, utilizza il comando `attach-security-profile`.

Eliminazione del profilo di sicurezza ML Detect utilizzando l'interfaccia a riga di comando

È possibile eliminare un profilo di sicurezza utilizzando il seguente comando `delete-security-profile`:

```
delete-security-profile --security-profile-name SecurityProfileName
```

> **Note**
>
> Dopo aver eliminato un profilo di sicurezza ML Detect, non sarà possibile riattivare il profilo di sicurezza.

Parametri personalizzati

Con i parametri personalizzati AWS IoT Device Defender puoi definire e monitorare parametri specifici per il tuo parco istanze o caso d'uso, ad esempio il numero di dispositivi collegati ai gateway Wi-Fi, i livelli di carica per le batterie o il numero di cicli di alimentazione per le prese intelligenti. I comportamenti dei parametri personalizzati sono definiti nei profili di sicurezza, che specificano i comportamenti previsti per un gruppo di dispositivi (un gruppo di oggetti) o per tutti i dispositivi. È

possibile monitorare i comportamenti impostando allarmi che puoi utilizzare per rilevare e rispondere a problemi specifici dei dispositivi.

Questo capitolo contiene le sezioni seguenti:

- Come utilizzare i parametri personalizzati nella console
- Come utilizzare i parametri personalizzati da CLI
- Parametri personalizzati dell'interfaccia a riga di comando
- API di parametri personalizzati

Come utilizzare i parametri personalizzati nella console

Tutorial

- AWS IoT Device Defender Agent SDK (Python)
- Creare un parametro personalizzato e aggiungilo a un profilo di sicurezza
- Visualizza dettagli personalizzati dei parametri
- Per creare un parametro personalizzato
- Eliminare un parametro personalizzato

AWS IoT Device Defender Agent SDK (Python)

Per iniziare, scarica l'agente di esempio AWS IoT Device Defender Agent SDK (Python). L'agente raccoglie i parametri e pubblica i report. Dopo la pubblicazione dei parametri sul dispositivo, è possibile visualizzare i parametri raccolti e determinare le soglie per l'impostazione degli allarmi. Le istruzioni per la configurazione dell'agente dispositivo sono disponibili su AWS IoT Readme Device Defender Agent SDK (Python). Per ulteriori informazioni, consulta AWS IoT Device Defender SDK Agent (Python).

Creare un parametro personalizzato e aggiungilo a un profilo di sicurezza

La procedura seguente mostra come creare un gruppo di parametri tramite la console.

1. Nell'AWS IoT console, nel pannello di navigazione, espandi Defend (Protezione), poi Detect (Rileva), e Metrics (Parametri).
2. Sulla pagina Custom metrics (Parametri personalizzati), scegli Create (Crea).

3. Nella pagina Create custom metric (Crea parametri personalizzati), esegui le seguenti operazioni.

   1. In Name (Nome) immetti un nome per il parametro personalizzato. Non è possibile modificare questo nome dopo aver creato il parametro personalizzato.
   2. In Display name (Visualizza nome) (opzionale) puoi immettere un nome facilmente identificabile per il parametro personalizzato. Non deve essere univoco e può essere modificato dopo la creazione.
   3. In Type (Tipo), scegli il tipo di parametro che desideri monitorare. I tipi di parametri includono string-list, ip-address-list, number-list e number. Il tipo di parametro non può essere modificato dopo la creazione.

      > **Note**
      >
      > ML Detect consente solo il tipo numero.

   4. In Tag è possibile selezionare i tag da associare alla risorsa.

   Al termine, scegli Confirm (Conferma).
4. Dopo aver creato il parametro personalizzato, appare la pagina Custom metrics (Parametri personalizzati) in cui è possibile visualizzare il parametro personalizzato appena creato.
5. A questo punto, aggiungi il parametro personalizzato a un profilo di sicurezza. Nell'AWS IoT console, nel pannello di navigazione, espandi Defend (Protezione), poi scegli Detect (Rileva), e seleziona Security profiles (Profili di sicurezza).
6. Scegli il profilo di sicurezza a cui desideri aggiungere il parametro personalizzato.
7. Scegli Actions (Operazioni), Edit (Modifica).
8. Scegli Additional Metrics to retain (Parametri aggiuntivi da conservare), quindi scegli il parametro personalizzato. Scegli Next (Successivo) nelle seguenti schermate fino a raggiungere la pagina Confirm (Conferma). Seleziona Save (Salva) e Continue (Continua). Dopo aver aggiunto correttamente il parametro personalizzato, viene visualizzata la pagina dei dettagli del profilo di sicurezza.

> **Note**
>
> Le statistiche di percentile non sono disponibili per i parametri quando uno qualsiasi dei valori dei parametri è un numero negativo.

Visualizza dettagli personalizzati dei parametri

La procedura seguente mostra come visualizzare i dettagli di un parametro personalizzato nella console.

1. Nell'AWS IoT console, nel pannello di navigazione, espandi Defend (Protezione), poi scegli Detect (Rileva), e Metrics (Parametri).
2. Seleziona Metric name (Nome parametro) del parametro personalizzato di cui desideri visualizzare i dettagli.

Per creare un parametro personalizzato

La procedura seguente illustra come aggiornare un parametro personalizzato nella console.

1. Nell'AWS IoT console, nel pannello di navigazione, espandi Defend (Protezione), poi scegli Detect (Rileva), e Metrics (Parametri).
2. Scegli il pulsante di opzione accanto al parametro personalizzato che desideri aggiornare. Quindi, per Actions (Operazioni), scegli Edit (Modifica).
3. Sulla pagina Update custom metric (Aggiorna parametro personalizzato), è possibile modificare il nome visualizzato e rimuovere o aggiungere tag.
4. Al termine, scegli Update (Aggiorna). La pagina Custom metric (Parametri personalizzati).

Eliminare un parametro personalizzato

La procedura seguente mostra come eliminare un parametro personalizzato tramite la console.

1. Innanzitutto, rimuovi il parametro personalizzato da qualsiasi profilo di sicurezza a cui fa riferimento. È possibile visualizzare quali profili di sicurezza contengono il parametro personalizzato nella pagina dei dettagli dei parametri personalizzati. Nell'AWS IoT console,

nel pannello di navigazione, espandi Defend (Protezione), poi scegli Detect (Rileva), e Metrics (Parametri).

2. Scegli il parametro personalizzato che desideri rimuovere. Rimuovi il parametro personalizzato da qualsiasi profilo di sicurezza elencato in Security Profiles (Profili di sicurezza) nella pagina dei dettagli dei parametri personalizzati.
3. Nell'AWS IoT console, nel pannello di navigazione, espandi Defend (Protezione), poi scegli Detect (Rileva), e Metrics (Parametri).
4. Scegli il pulsante di opzione accanto al parametro personalizzato da eliminare. Per Actions (Operazioni), scegli Delete (Elimina).
5. Sul messaggio Are you sure you want to delete custom metric? (Sei sicuro di voler cancellare il parametro personalizzato?), scegli Delete custom metric (Elimina parametro personalizzato).

> **Warning**
>
> Dopo aver eliminato un parametro personalizzato, si perdono tutti i dati associati al parametro. Questa operazione non può essere annullata.

Come utilizzare i parametri personalizzati da CLI

Tutorial

- AWS IoT Device Defender Agent SDK (Python)
- Creare un parametro personalizzato e aggiungerlo a un profilo di sicurezza
- Visualizzare dettagli personalizzati dei parametri
- Aggiornare un parametro personalizzato
- Eliminare un parametro personalizzato

AWS IoT Device Defender Agent SDK (Python)

Per iniziare, scarica l'agente di esempio AWS IoT Device Defender Agent SDK (Python). L'agente raccoglie i parametri e pubblica i report. Dopo la pubblicazione dei parametri sul dispositivo, è possibile visualizzare i parametri raccolti e determinare le soglie per l'impostazione degli allarmi. Le istruzioni per la configurazione dell'agente dispositivo sono disponibili su Readme AWS IoT Device Defender Agent SDK (Python). Per ulteriori informazioni, consulta AWS IoT Device Defender SDK Agent (Python).

Creare un parametro personalizzato e aggiungerlo a un profilo di sicurezza

La procedura seguente mostra come creare un parametro personalizzato e aggiungerlo a un profilo di sicurezza dall'interfaccia della riga di comando.

1. Utilizzo dell'`create-custom-metric` per creare il parametro personalizzato. Nell'esempio seguente viene creato un parametro personalizzato che misura la percentuale della batteria.

```
aws iot create-custom-metric \
    --metric-name "batteryPercentage" \
    --metric-type "number" \
    --display-name "Remaining battery percentage." \
    --region us-east-1
    --client-request-token "02ccb92b-33e8-4dfa-a0c1-35b181ed26b0" \
```

   Output:

```
{
    "metricName": "batteryPercentage",
    "metricArn": "arn:aws:iot:us-
east-1:1234564789012:custommetric/batteryPercentage"
}
```

2. Dopo aver creato il parametro personalizzato, è possibile aggiungerlo a un profilo esistente utilizzando `update-security-profile`, oppure creare un nuovo profilo di sicurezza per aggiungere il parametro personalizzato tramite `create-security-profile`. In questo modo, viene creato un nuovo profilo di sicurezza chiamato *batteryUsage* per aggiungere il nuovo parametro personalizzato *batteryPercentage*. Aggiungiamo anche un parametro Rules Detect chiamato *cellularBandwidth*.

```
aws iot create-security-profile \
    --security-profile-name batteryUsage \
    --security-profile-description "Shows how much battery is left in percentile."
 \
    --behaviors "[{\"name\":\"great-than-75\",\"metric\":\"batteryPercentage\",
\"criteria\":{\"comparisonOperator\":\"greater-than\",\"value\":{\"number
\":75},\"consecutiveDatapointsToAlarm\":5,\"consecutiveDatapointsToClear
\":1}},{\"name\":\"cellularBandwidth\",\"metric\":\"aws:message-byte-size\",
\"criteria\":{\"comparisonOperator\":\"less-than\",\"value\":{\"count\":128},
\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}}]" \
```

```
    --region us-east-1
```

Output:

```
{
    "securityProfileArn": "arn:aws:iot:us-east-1:1234564789012:securityprofile/
batteryUsage",
    "securityProfileName": "batteryUsage"
}
```

> **Note**
>
> Le statistiche di percentile non sono disponibili per i parametri quando uno qualsiasi dei valori dei parametri è un numero negativo.

Visualizzare dettagli personalizzati dei parametri

La procedura seguente mostra come visualizzare i dettagli per un parametro personalizzato dall'interfaccia della riga di comando.

- Utilizzo del comando `list-custom-metrics` per visualizzare tutti i parametri personalizzati.

  ```
  aws iot list-custom-metrics \
      --region us-east-1
  ```

  L'output di questo comando è simile al seguente.

  ```
  {
      "metricNames": [
          "batteryPercentage"
      ]
  }
  ```

Aggiornare un parametro personalizzato

La procedura seguente mostra come aggiornare un parametro personalizzato dall'interfaccia a riga di comando.

- Utilizzo del comando `update-custom-metric` per aggiornare un parametro personalizzato. Nell'esempio seguente viene aggiornato il `display-name`.

```
aws iot update-custom-metric \
    --metric-name batteryPercentage \
    --display-name 'remaining battery percentage on device' \
    --region us-east-1
```

L'output di questo comando è simile al seguente.

```
{
    "metricName": "batteryPercentage",
    "metricArn": "arn:aws:iot:us-
east-1:1234564789012:custommetric/batteryPercentage",
    "metricType": "number",
    "displayName": "remaining battery percentage on device",
    "creationDate": "2020-11-17T23:01:35.110000-08:00",
    "lastModifiedDate": "2020-11-17T23:02:12.879000-08:00"
}
```

Eliminare un parametro personalizzato

La procedura seguente mostra come eliminare un parametro personalizzato dall'interfaccia a riga di comando.

1. Per eliminare un parametro personalizzato, scollegalo prima da tutti i profili di sicurezza a cui è collegato. Utilizzo del comando `list-security-profiles` per visualizzare i profili di sicurezza con un determinato parametro personalizzato.
2. Per rimuovere un parametro personalizzato da un profilo di sicurezza, utilizza il comando `update-security-profiles`. Immetti tutte le informazioni che desideri conservare, ma escludi il parametro personalizzato.

```
aws iot update-security-profile \
  --security-profile-name batteryUsage \
  --behaviors "[{\"name\":\"cellularBandwidth\",\"metric\":\"aws:message-byte-size
\",\"criteria\":{\"comparisonOperator\":\"less-than\",\"value\":{\"count\":128},
\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}}]"
```

L'output di questo comando è simile al seguente.

```
{
  "behaviors": [{\"name\":\"cellularBandwidth\",\"metric\":\"aws:message-byte-size
\",\"criteria\":{\"comparisonOperator\":\"less-than\",\"value\":{\"count\":128},
\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}}],
  "securityProfileName": "batteryUsage",
  "lastModifiedDate": 2020-11-17T23:02:12.879000-09:00,
  "securityProfileDescription": "Shows how much battery is left in percentile.",
  "version": 2,
  "securityProfileArn": "arn:aws:iot:us-east-1:1234564789012:securityprofile/
batteryUsage",
  "creationDate": 2020-11-17T23:02:12.879000-09:00
}
```

3. Dopo che il parametro personalizzato è stato scollegato, utilizza il comando `delete-custom-metric` per eliminare il parametro personalizzato.

```
aws iot delete-custom-metric  \
  --metric-name batteryPercentage \
  --region us-east-1
```

L'output di questo comando è simile al seguente

```
HTTP 200
```

Parametri personalizzati dell'interfaccia a riga di comando

Puoi utilizzare i comandi CLI seguenti per creare e gestire parametri personalizzati.

- create-custom-metric
- describe-custom-metric
- list-custom-metrics
- update-custom-metric
- delete-custom-metric
- list-security-profiles

API di parametri personalizzati

Per creare e gestire parametri personalizzati, è possibile utilizzare le seguenti API.

- CreateCustomMetric
- DescribeCustomMetric
- ListCustomMetrics
- UpdateCustomMetric
- DeleteCustomMetric
- ListSecurityProfiles

Device-side metrics

Quando si crea un profilo di sicurezza, è possibile specificare il comportamento previsto del dispositivo IoT configurando comportamenti e soglie per i parametri generati dai dispositivi IoT. Di seguito sono riportati i parametri sul lato dispositivo, ovvero i parametri degli agenti installati sui dispositivi.

Byte in uscita (**`aws:all-bytes-out`**)

Numero di byte in uscita da un dispositivo durante un determinato periodo di tempo.

Usa questo parametro per specificare la quantità massima o minima di traffico in uscita che un dispositivo può inviare, misurata in byte, in un determinato periodo di tempo.

Compatibile con: Rule Detect | ML Detect

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: byte

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Example

```
{
  "name": "TCP outbound traffic",
```

```
  "metric": "aws:all-bytes-out",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 4096
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio utilizzando un **`statisticalThreshold`**

```
{
  "name": "TCP outbound traffic",
  "metric": "aws:all-bytes-out",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
      "statistic": "p50"
    },
    "durationSeconds": 900,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio con ML Detect

```
{
  "name": "Outbound traffic ML behavior",
  "metric": "aws:all-bytes-out",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
```

```
}
```

Byte in entrata (**aws:all-bytes-in**)

Numero di byte in entrata in un dispositivo durante un determinato periodo di tempo.

Usa questo parametro per specificare la quantità massima o minima di traffico in entrata che un dispositivo può ricevere, misurata in byte, in un determinato periodo di tempo.

Compatibile con: Rule Detect | ML Detect

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: byte

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Example

```
{
  "name": "TCP inbound traffic",
  "metric": "aws:all-bytes-in",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 4096
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio utilizzando un **statisticalThreshold**

```
{
  "name": "TCP inbound traffic",
  "metric": "aws:all-bytes-in",
  "criteria": {
    "comparisonOperator": "less-than-equals",
```

```
    "statisticalThreshold": {
      "statistic": "p90"
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio con ML Detect

```
{
  "name": "Inbound traffic ML behavior",
  "metric": "aws:all-bytes-in",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Conteggio di porte TCP in ascolto (**`aws:num-listening-tcp-ports`**)

Numero delle porte TCP su cui il dispositivo è in ascolto.

Usa questo parametro per specificare il numero massimo o minimo di porte TCP che ogni dispositivo dovrebbe monitorare.

Compatibile con: Rule Detect | ML Detect

Unità: errori

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: errori

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Example

```
{
  "name": "Max TCP Ports",
  "metric": "aws:num-listening-tcp-ports",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 5
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio utilizzando un **`statisticalThreshold`**

```
{
  "name": "Max TCP Ports",
  "metric": "aws:num-listening-tcp-ports",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
      "statistic": "p50"
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio di utilizzo di ML Detect

```
{
  "name": "Max TCP Port ML behavior",
  "metric": "aws:num-listening-tcp-ports",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
```

```
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Conteggio porte UDP in ascolto (**`aws:num-listening-udp-ports`**)

Numero delle porte UDP su cui il dispositivo è in ascolto.

Usa questo parametro per specificare il numero massimo o minimo di porte UDP che ogni dispositivo dovrebbe monitorare.

Compatibile con: Rule Detect | ML Detect

Unità: errori

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: errori

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Example

```
{
  "name": "Max UDP Ports",
  "metric": "aws:num-listening-udp-ports",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 5
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio utilizzando un **`statisticalThreshold`**

```
{
  "name": "Max UDP Ports",
  "metric": "aws:num-listening-udp-ports",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
      "statistic": "p50"
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio con ML Detect

```
{
  "name": "Max UPD Port ML behavior",
  "metric": "aws:num-listening-tcp-ports",
  "criteria": {
  "consecutiveDatapointsToAlarm": 1,
  "consecutiveDatapointsToClear": 1,
  "mlDetectionConfig": {
    "confidenceLevel": "HIGH"
   }
 },
  "suppressAlerts": true
}
```

Pacchetti in uscita (**`aws:all-packets-out`**)

Numero di pacchetti in uscita da un dispositivo durante un determinato periodo di tempo.

Usa questo parametro per specificare la quantità massima o minima di traffico in uscita totale che un dispositivo può inviare in un determinato periodo di tempo.

Compatibile con: Rule Detect | ML Detect

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: pacchetti

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Example

```
{
  "name": "TCP outbound traffic",
  "metric": "aws:all-packets-out",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 100
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio utilizzando un **`statisticalThreshold`**

```
{
  "name": "TCP outbound traffic",
  "metric": "aws:all-packets-out",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
      "statistic": "p90"
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio con ML Detect

```
{
```

```
  "name": "Outbound sent ML behavior",
  "metric": "aws:all-packets-out",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Pacchetti in entrata (**aws:all-packets-in**)

Numero di pacchetti in entrata in un dispositivo durante un determinato periodo di tempo.

Usa questo parametro per specificare la quantità massima o minima di traffico in entrata totale che un dispositivo può ricevere in un determinato periodo di tempo.

Compatibile con: Rule Detect | ML Detect

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: pacchetti

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Example

```
{
  "name": "TCP inbound traffic",
  "metric": "aws:all-packets-in",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 100
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
```

```
  },
  "suppressAlerts": true
}
```

Example

Esempio utilizzando un `statisticalThreshold`

```
{
  "name": "TCP inbound traffic",
  "metric": "aws:all-packets-in",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
      "statistic": "p90"
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio con ML Detect

```
{
  "name": "Inbound sent ML behavior",
  "metric": "aws:all-packets-in",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

IP di destinazione (**`aws:destination-ip-addresses`**)

Set di destinazioni IP.

Usa questo parametro per specificare un set di CIDR (Classless Inter-Domain Routings) consentiti (precedentemente chiamati whitelist) o non consentiti (precedentemente chiamati blacklist) da cui ciascun dispositivo deve o non deve connettersi a AWS IoT.

Compatibile con: Rules Detect

Operatori: in-cidr-set | not-in-cidr-set

Valori: elenco di CIDR

Unità: n/d

Example

```
{
  "name": "Denied source IPs",
  "metric": "aws:destination-ip-address",
  "criteria": {
    "comparisonOperator": "not-in-cidr-set",
    "value": {
      "cidrs": [ "12.8.0.0/16", "15.102.16.0/24" ]
    }
  },
  "suppressAlerts": true
}
```

Porte TCP in ascolto (**`aws:listening-tcp-ports`**)

Porte TCP su cui il dispositivo è in ascolto.

Usa questo parametro per specificare un set di porte TCP consentite (precedentemente chiamate whitelist) o non consentite (precedentemente chiamate blacklist) su cui ciascun dispositivo deve o non deve restare in ascolto.

Compatibile con: Rules Detect

Operatori: in-port-set | not-in-port-set

Valori: elenco di porte

Unità: n/d

Example

```
{
  "name": "Listening TCP Ports",
  "metric": "aws:listening-tcp-ports",
  "criteria": {
    "comparisonOperator": "in-port-set",
    "value": {
      "ports": [ 443, 80 ]
    }
  },
  "suppressAlerts": true
}
```

Porte UDP in ascolto (**`aws:listening-udp-ports`**)

Porte UDP su cui il dispositivo è in ascolto.

Usa questo parametro per specificare un set di porte UDP consentite (precedentemente chiamate whitelist) o non consentite (precedentemente chiamate blacklist) su cui ciascun dispositivo deve o non deve restare in ascolto.

Compatibile con: Rules Detect

Operatori: in-port-set | not-in-port-set

Valori: elenco di porte

Unità: n/d

Example

```
{
  "name": "Listening UDP Ports",
  "metric": "aws:listening-udp-ports",
  "criteria": {
    "comparisonOperator": "in-port-set",
    "value": {
      "ports": [ 1025, 2000 ]
    }
  }
}
```

Conteggio delle connessioni TCP stabilite (**aws:num-established-tcp-connections**)

Numero di connessioni TCP per un dispositivo.

Usa questo parametro per specificare il numero massimo o minimo di connessioni TCP attive che ciascun dispositivo può avere (Tutte le TCP con stati).

Compatibile con: Rule Detect | ML Detect

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: connessioni

Example

```
{
  "name": "TCP Connection Count",
  "metric": "aws:num-established-tcp-connections",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 3
    },
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio utilizzando un **statisticalThreshold**

```
{
  "name": "TCP Connection Count",
  "metric": "aws:num-established-tcp-connections",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
      "statistic": "p90"
    },
```

```
    "durationSeconds": 900,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio con ML Detect

```
{
  "name": "Connection count ML behavior",
  "metric": "aws:num-established-tcp-connections",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Specifica del documento di parametri dei dispositivi

Struttura generale

Nome lungo	Nome breve	Richiesto	Type	Vincoli	Note
header	hed	Y	Oggetto		Blocco completo necessario per un report in formato corretto.
parametri	met	Y	Oggetto		Un report può avere entrambi o almeno un `metrics` o un blocco

Nome lungo	Nome breve	Richiesto	Type	Vincoli	Note
					`custom_metrics` .
custom_metrics	cmet	Y	Oggetto		Un report può avere entrambi o almeno un `metrics` o un blocco `custom_metrics` .

Blocco di intestazione

Nome lungo	Nome breve	Richiesto	Type	Vincoli	Note
report_id	rid	Y	Numero intero		Valore crescente in maniera monotona. Timestamp epoch consigliato.
version	v	Y	Stringa	Major.Minor	Incrementi minori con aggiunta di campo. Incrementi maggiori se i parametri vengono rimossi.

Blocco dei parametri:

Connessioni TCP

Nome lungo	Nome breve	Elemento padre	Richiesto	Type	Vincoli	Note
tcp_connections	tc	parametri	N	Oggetto		
established_connections	ec	tcp_connections	N	Oggetto		Stato connessione TCP stabilita
connections	cs	established_connections	N	Elenco<Oggetto>		
remote_addr	rad	connections	Y	Numero	ip:porta	IP può essere ipv6 o ipv4
local_port	lp	connections	N	Numero	>= 0	
local_interface	li	connections	N	Stringa		Nome interfaccia
total	t	established_connections	N	Numero	>= 0	Numero di connessioni stabilite.

Porte TCP in ascolto

Nome lungo	Nome breve	Elemento padre	Richiesto	Type	Vincoli	Note
listening_tcp_ports	tp	parametri	N	Oggetto		

Nome lungo	Nome breve	Elemento padre	Richiesto	Type	Vincoli	Note
ports	pts	listening_tcp_ports	N	Elenco<Oggetto>	> 0	
port	pt	ports	N	Numero	> 0	I numeri di porta devono essere maggiori di 0
interface	if	ports	N	Stringa		Nome interfaccia
total	t	listening_tcp_ports	N	Numero	>= 0	

Porte UDP in ascolto

Nome lungo	Nome breve	Elemento padre	Richiesto	Type	Vincoli	Note
listening_udp_ports	up	parametri	N	Oggetto		
ports	pts	listening_udp_ports	N	Elenco<Porta>	> 0	
port	pt	ports	N	Numero	> 0	I numeri di porta devono essere maggiori di 0

Nome lungo	Nome breve	Elemento padre	Richiesto	Type	Vincoli	Note
interface	if	ports	N	Stringa		Nome interfaccia
total	t	listening_udp_ports	N	Numero	>= 0	

Statistiche di rete

Nome lungo	Nome breve	Elemento padre	Richiesto	Type	Vincoli	Note
network_stats	ns	metrics	N	Oggetto		
bytes_in	bi	network_stats	N	Numero	Parametro delta, >= 0	
bytes_out	bo	network_stats	N	Numero	Parametro delta, >= 0	
packets_in	pi	network_stats	N	Numero	Parametro delta, >= 0	
packets_out	po	network_stats	N	Numero	Parametro delta, >= 0	

Example

La seguente struttura JSON utilizza nomi lunghi.

```
{
  "header": {
    "report_id": 1530304554,
    "version": "1.0"
  },
  "metrics": {
```

```
    "listening_tcp_ports": {
      "ports": [
        {
          "interface": "eth0",
          "port": 24800
        },
        {
          "interface": "eth0",
          "port": 22
        },
        {
          "interface": "eth0",
          "port": 53
        }
      ],
      "total": 3
    },
    "listening_udp_ports": {
      "ports": [
        {
          "interface": "eth0",
          "port": 5353
        },
        {
          "interface": "eth0",
          "port": 67
        }
      ],
      "total": 2
    },
    "network_stats": {
      "bytes_in": 29358693495,
      "bytes_out": 26485035,
      "packets_in": 10013573555,
      "packets_out": 11382615
    },
    "tcp_connections": {
      "established_connections": {
        "connections": [
          {
            "local_interface": "eth0",
            "local_port": 80,
            "remote_addr": "192.168.0.1:8000"
          },
```

```
          {
            "local_interface": "eth0",
            "local_port": 80,
            "remote_addr": "192.168.0.1:8000"
          }
        ],
        "total": 2
      }
    }
  },
  "custom_metrics": {
    "MyMetricOfType_Number": [
      {
        "number": 1
      }
    ],
    "MyMetricOfType_NumberList": [
      {
        "number_list": [
          1,
          2,
          3
        ]
      }
    ],
    "MyMetricOfType_StringList": [
      {
        "string_list": [
          "value_1",
          "value_2"
        ]
      }
    ],
    "MyMetricOfType_IpList": [
      {
        "ip_list": [
          "172.0.0.0",
          "172.0.0.10"
        ]
      }
    ]
  }
}
```

Example Esempio di struttura JSON con nomi brevi

```
{
  "hed": {
    "rid": 1530305228,
    "v": "1.0"
  },
  "met": {
    "tp": {
      "pts": [
        {
          "if": "eth0",
          "pt": 24800
        },
        {
          "if": "eth0",
          "pt": 22
        },
        {
          "if": "eth0",
          "pt": 53
        }
      ],
      "t": 3
    },
    "up": {
      "pts": [
        {
          "if": "eth0",
          "pt": 5353
        },
        {
          "if": "eth0",
          "pt": 67
        }
      ],
      "t": 2
    },
    "ns": {
      "bi": 29359307173,
      "bo": 26490711,
      "pi": 10014614051,
      "po": 11387620
    },
```

```
    "tc": {
      "ec": {
        "cs": [
          {
            "li": "eth0",
            "lp": 80,
            "rad": "192.168.0.1:8000"
          },
          {
            "li": "eth0",
            "lp": 80,
            "rad": "192.168.0.1:8000"
          }
        ],
        "t": 2
      }
    }
  },
  "cmet": {
    "MyMetricOfType_Number": [
      {
        "number": 1
      }
    ],
    "MyMetricOfType_NumberList": [
      {
        "number_list": [
          1,
          2,
          3
        ]
      }
    ],
    "MyMetricOfType_StringList": [
      {
        "string_list": [
          "value_1",
          "value_2"
        ]
      }
    ],
    "MyMetricOfType_IpList": [
      {
        "ip_list": [
```

```
          "172.0.0.0",
          "172.0.0.10"
        ]
      }
    ]
  }
}
```

Invio di parametri dai dispositivi

AWS IoT Device Defender Detect permette di raccogliere, aggregare e monitorare i dati dei parametri generati dai dispositivi AWS IoT per identificare i dispositivi che presentano un comportamento anomalo. In questa sezione viene illustrato come inviare parametri da un dispositivo a AWS IoT Device Defender.

È necessario distribuire in modo sicuro AWS IoT SDK versione due sui dispositivi AWS IoT connessi o nei gateway dei dispositivi per raccogliere i parametri lato dispositivo. Vedi l'elenco completo degli SDK qui.

Puoi utilizzare AWS IoT Device Client per pubblicare parametri perché fornisce un singolo agente che copre le funzionalità presenti in AWS IoT Device Defender e in AWS IoT Device Management. Queste caratteristiche includono processi, tunneling sicuro, pubblicazione di parametri AWS IoT Device Defender e altro ancora.

Pubblichi i parametri lato dispositivo sull'argomento riservato in AWS IoT per la raccolta e la valutazione di AWS IoT Device Defender.

Utilizzo di AWS IoT Device Client per la pubblicazione di parametri

Per installare AWS IoT Device Client, puoi scaricarlo da Github. Dopo aver installato il AWS IoT Device Client sul dispositivo per il quale si desidera raccogliere dati sul lato dispositivo, è necessario configurarlo per inviare parametri sul lato dispositivo a AWS IoT Device Defender. Verificare che l'AWS IoT Device Client File di configurazione abbia i seguenti parametri impostati nella sezione `device-defender`:

```
"device-defender":    {
      "enabled":    true,
      "interval-in-seconds": 300
  }
```

> **Warning**
>
> È necessario impostare l'intervallo di tempo su un minimo di 300 secondi. Se si imposta l'intervallo di tempo su un valore inferiore a 300 secondi, i dati dei parametri potrebbero essere limitati.

Dopo aver aggiornato la configurazione, è possibile creare profili e comportamenti di sicurezza nell'AWS IoT Device Defender console per monitorare i parametri che i dispositivi pubblicano sul cloud. Puoi trovare i parametri pubblicati nell'AWS IoT Core console scegliendo Defend (Protezione), Detect (Rileva) e quindi Metrics (Parametri).

Parametri sul lato cloud

Quando si crea un profilo di sicurezza, è possibile specificare il comportamento previsto del dispositivo IoT configurando comportamenti e soglie per i parametri generati dai dispositivi IoT. Di seguito sono riportati i parametri sul lato cloud, che sono parametri provenienti da AWS IoT.

Dimensioni del messaggio (aws:message-byte-size)

Numero di byte in un messaggio. Usa questo parametro per specificare la dimensione massima o minima (in byte) di ogni messaggio trasmesso da un dispositivo a AWS IoT.

Compatibile con: Rule Detect | ML Detect

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: byte

Example

```
{
  "name": "Max Message Size",
  "metric": "aws:message-byte-size",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 1024
    },
```

```
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio utilizzando un **`statisticalThreshold`**

```
{

  "name": "Large Message Size",
  "metric": "aws:message-byte-size",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
      "statistic": "p90"
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio con ML Detect

```
{
  "name": "Message size ML behavior",
  "metric": "aws:message-byte-size",
  "criteria": {
  "consecutiveDatapointsToAlarm": 1,
  "consecutiveDatapointsToClear": 1,
  "mlDetectionConfig": {
    "confidenceLevel": "HIGH"
   }
 },
  "suppressAlerts": true
}
```

Si verifica un allarme per un dispositivo se, durante tre intervalli di tempo consecutivi di cinque minuti ciascuno, vengono trasmessi messaggi la cui dimensione cumulativa è superiore a quella misurata per il 90% di tutti gli altri dispositivi che segnalano questo comportamento del profilo di sicurezza.

Messaggi inviati (aws:num-messages-sent)

Numero di messaggi inviati da un dispositivo durante un determinato periodo di tempo.

Usa questo parametro per specificare il numero massimo o minimo di messaggi che possono essere inviati tra AWS IoT e ogni dispositivo in un determinato periodo di tempo.

Compatibile con: Rule Detect | ML Detect

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: messaggi

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Example

```
{

  "name": "Out bound message count",
  "metric": "aws:num-messages-sent",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 50
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
    },
  "suppressAlerts": true
}
```

Example Esempio utilizzando un **`statisticalThreshold`**

```
{

  "name": "Out bound message rate",
  "metric": "aws:num-messages-sent",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
```

```
      "statistic": "p99"
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio con ML Detect

```
{
  "name": "Messages sent ML behavior",
  "metric": "aws:num-messages-sent",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Messaggi ricevuti (aws:num-messages-received)

Numero di messaggi ricevuti da un dispositivo durante un determinato periodo di tempo.

Usa questo parametro per specificare il numero massimo o minimo di messaggi che possono essere ricevuti tra AWS IoT e ogni dispositivo in un determinato periodo di tempo.

Compatibile con: Rule Detect | ML Detect

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: messaggi

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Example

```
{
```

```
  "name": "In bound message count",
  "metric": "aws:num-messages-received",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 50
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
    },
  "suppressAlerts": true
}
```

Example Esempio utilizzando un **`statisticalThreshold`**

```
{
  "name": "In bound message rate",
  "metric": "aws:num-messages-received",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
      "statistic": "p99"
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio con ML Detect

```
{
  "name": "Messages received ML behavior",
  "metric": "aws:num-messages-received",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
```

```
  "suppressAlerts": true
}
```

Errori di autorizzazione (aws:num-authorization-failures)

Usa questo parametro per specificare il numero massimo di errori di autorizzazione permessi per ogni dispositivo in un determinato periodo di tempo. Un errore di autorizzazione si verifica quando una richiesta da un dispositivo a AWS IoT viene negata, ad esempio se un dispositivo tenta di eseguire la pubblicazione in un argomento per cui non dispone di autorizzazioni sufficienti.

Compatibile con: Rule Detect | ML Detect

Unità: errori

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Example

```
{
  "name": "Authorization Failures",
  "metric": "aws:num-authorization-failures",
  "criteria": {
    "comparisonOperator": "less-than",
    "value": {
      "count": 5
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio utilizzando un **`statisticalThreshold`**

```
{
  "name": "Authorization Failures",
  "metric": "aws:num-authorization-failures",
```

```
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
      "statistic": "p50"
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio con ML Detect

```
{
  "name": "Authorization failures ML behavior",
  "metric": "aws:num-authorization-failures",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

IP di origine (aws:source-ip-address)

Indirizzo IP da cui un dispositivo si è connesso a AWS IoT.

Usa questo parametro per specificare un set di CIDR consentiti (precedentemente chiamati whitelist) o non consentiti (precedentemente chiamati blacklist) da cui ciascun dispositivo deve o non deve connettersi a AWS IoT.

Compatibile con: Rules Detect

Operatori: in-cidr-set | not-in-cidr-set

Valori: elenco di CIDR

Unità: n/d

Example

```
{
  "name": "Denied source IPs",
  "metric": "aws:source-ip-address",
  "criteria": {
    "comparisonOperator": "not-in-cidr-set",
    "value": {
      "cidrs": [ "12.8.0.0/16", "15.102.16.0/24" ]
    }
  },
  "suppressAlerts": true
}
```

Tentativi di connessione (aws:num-connection-attempts)

il numero di tentativi di connessione di un dispositivo in un determinato periodo di tempo.

Usa questo parametro per specificare il numero massimo o minimo di tentativi di connessione per ciascun dispositivo. Vengono conteggiati sia i tentativi riusciti che quelli non riusciti.

Compatibile con: Rule Detect | ML Detect

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: tentativi di connessione

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Example

```
{
  "name": "Connection Attempts",
  "metric": "aws:num-connection-attempts",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 5
    },
    "durationSeconds": 600,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
```

```
  },
  "suppressAlerts": true
}
```

Example Esempio utilizzando un **`statisticalThreshold`**

```
{
  "name": "Connection Attempts",
  "metric": "aws:num-connection-attempts",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
      "statistic": "p10"
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio con ML Detect

```
{
  "name": "Connection attempts ML behavior",
  "metric": "aws:num-connection-attempts",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": false
}
```

Disconnessioni (aws:num-disconnects)

Il numero di disconnessioni da AWS IoT di un dispositivo durante un determinato periodo di tempo.

Utilizza questo parametro per specificare il numero massimo o minimo di disconnessioni di un dispositivo da AWS IoT durante un determinato periodo di tempo.

Compatibile con: Rule Detect | ML Detect

Operatori: less-than | less-than-equals | greater-than | greater-than-equals

Valore: intero non negativo

Unità: disconnessioni

Durata: un numero intero non negativo. I valori validi sono 300, 600, 900, 1800 o 3.600 secondi.

Example

```
{
  "name": "Disconnections",
  "metric": "aws:num-disconnects",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 5
    },
    "durationSeconds": 600,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio utilizzando un **`statisticalThreshold`**

```
{
  "name": "Disconnections",
  "metric": "aws:num-disconnects",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
      "statistic": "p10"
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Esempio con ML Detect

```
{
  "name": "Disconnects ML behavior",
  "metric": "aws:num-disconnects",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Durata della disconnessione (aws:disconnect-duration)

La durata della disconnessione di un dispositivo da AWS IoT.

Usa questa metrica per specificare la durata massima per la quale un dispositivo rimane disconnesso da AWS IoT.

Compatibile con: Rules Detect

Operatori: less-than | less-than-equals

Valore: intero non negativo (in minuti)

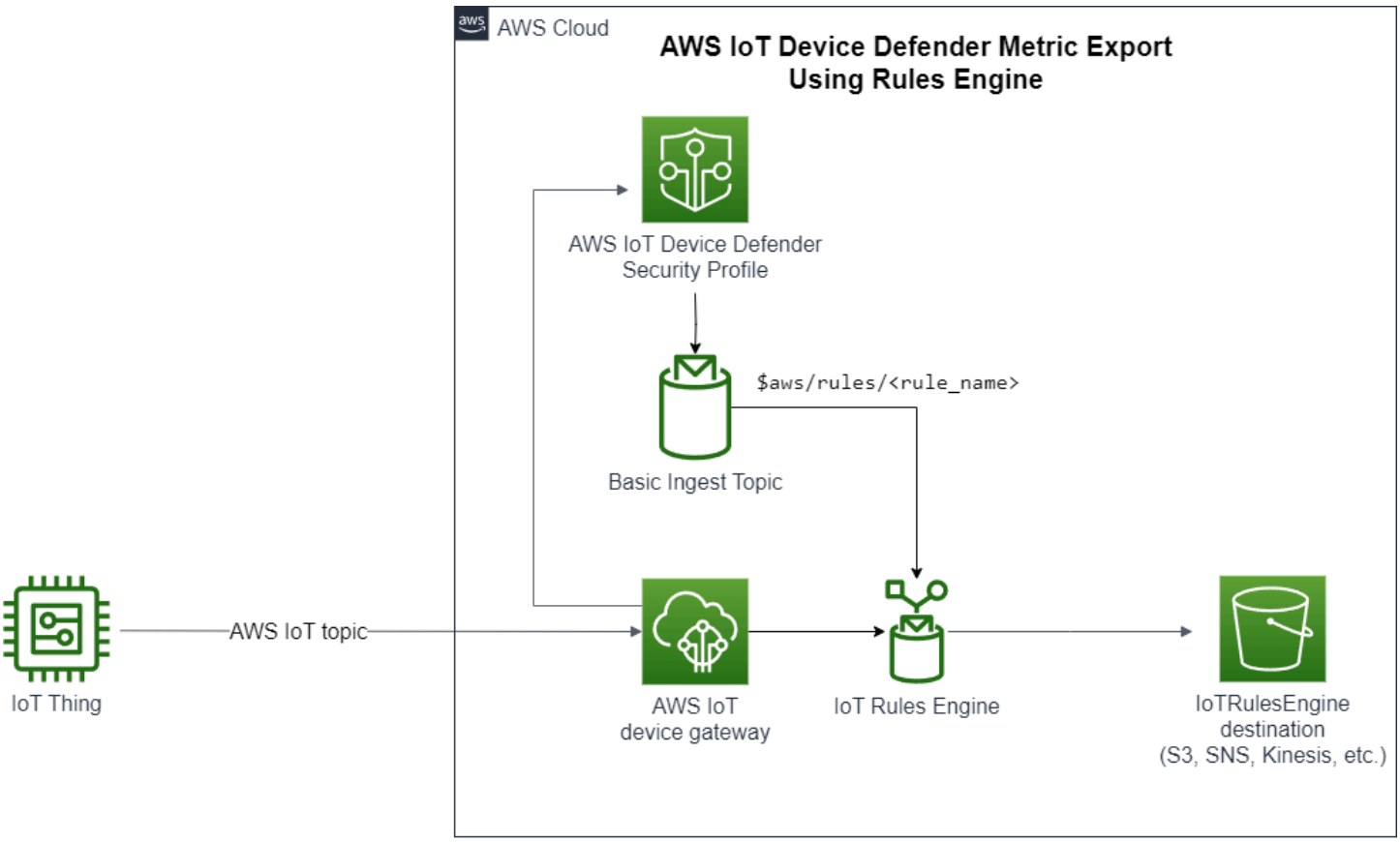
Example

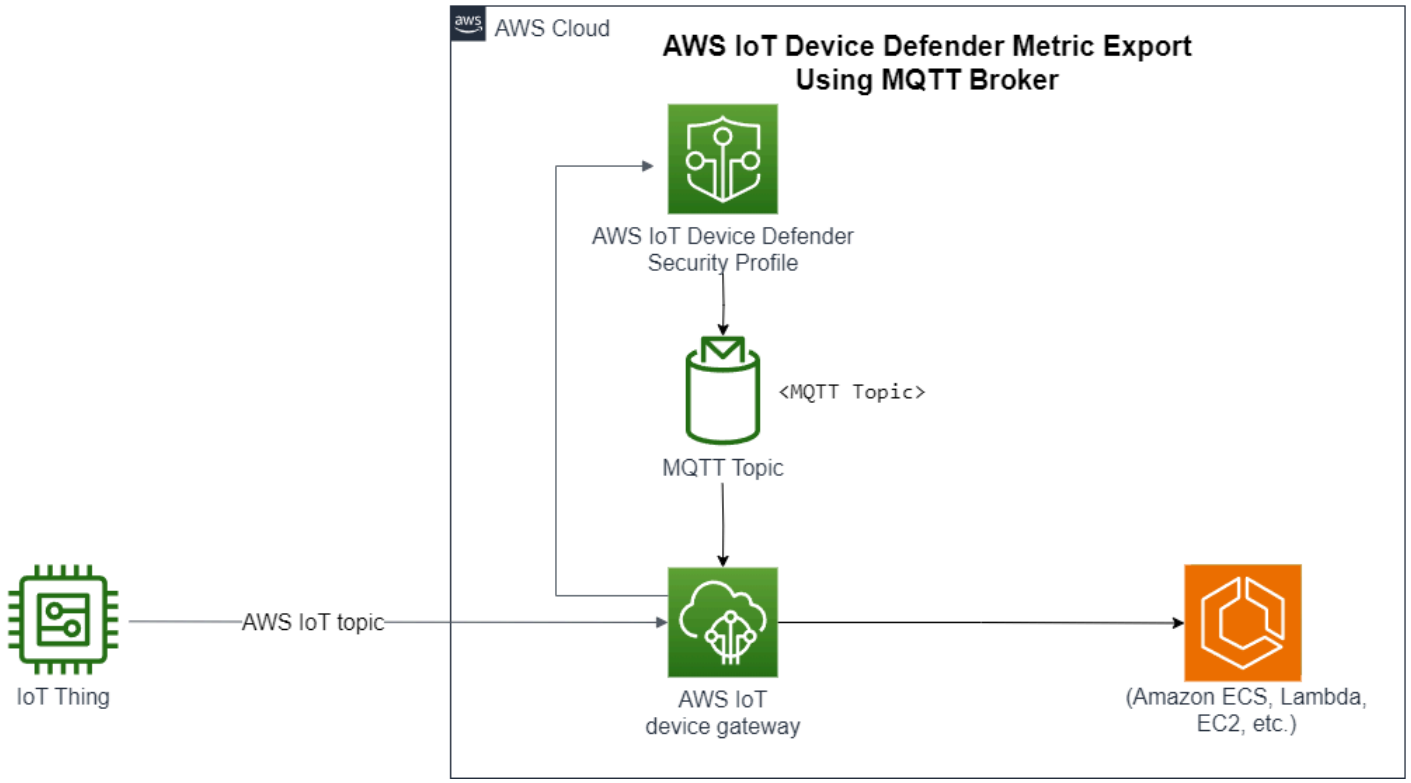
```
{
"name": "DisconnectDuration",
  "metric": "aws:disconnect-duration",
  "criteria": {
"comparisonOperator": "less-than-equals",
    "value": {
"count": 5
    }
  },
  "suppressAlerts": true
}
```

Esportazione delle metriche di rilevamento

Con l'esportazione delle metriche, puoi esportare le metriche lato cloud, lato dispositivo o personalizzate da AWS IoT Device Defender e pubblicarle in un argomento MQTT che hai configurato. Questa funzionalità supporta l'esportazione in blocco delle metriche di Detect, che non solo consente una creazione di report e un'analisi dei dati più efficienti, ma aiuta anche a controllare i costi. È possibile scegliere un argomento MQTT come argomento di inserimento di base delle regole AWS IoT oppure creare un argomento MQTT personalizzato e sottoscriverlo. Configura l'esportazione delle metriche utilizzando la console, l'API o la CLI di AWS IoT Device Defender. Questa funzionalità è supportata in tutte le regioni AWS in cui è disponibile AWS IoT Device Defender.

L'illustrazione seguente mostra come configurare AWS IoT Device Defender per l'esportazione delle metriche. Il primo diagramma mostra come configurare l'esportazione delle metriche per un argomento di inserimento di base. È quindi possibile indirizzare le metriche esportate verso varie destinazioni supportate dalle regole AWS IoT. Il secondo diagramma mostra come configurare AWS IoT Device Defender per la pubblicazione dei dati in un argomento MQTT. Il client MQTT sottoscrive l'argomento. Puoi eseguire un client MQTT in un container su Amazon Elastic Container Service, Lambda o un'istanza Amazon EC2 che sottoscrive lo stesso argomento MQTT. Ogni volta che AWS IoT Device Defender pubblica i dati, il client MQTT li riceve e li elabora. Per ulteriori informazioni, consultare Argomenti MQTT.


AWS Cloud
AWS IoT Device Defender Metric Export
Using Rules Engine
AWS IoT Device Defender
Security Profile
$aws/rules/<rule_name>
Basic Ingest Topic
IoT Thing
AWS IoT topic
AWS IoT
device gateway
IoT Rules Engine
IoTRulesEngine
destination
(S3, SNS, Kinesis, etc.)


AWS Cloud
AWS IoT Device Defender Metric Export
Using MQTT Broker
AWS IoT Device Defender
Security Profile
<MQTT Topic>
MQTT Topic
IoT Thing
AWS IoT topic
AWS IoT
device gateway
(Amazon ECS, Lambda,
EC2, etc.)

Come funziona l'esportazione delle metriche di rilevamento

Quando configuri un profilo di sicurezza, scegli le metriche da esportare e specifichi l'argomento MQTT. Inoltre puoi configurare un ruolo IAM che concede ad AWS IoT Device Defender Detect le autorizzazioni necessarie per pubblicare messaggi nell'argomento MQTT configurato. È possibile configurare un argomento MQTT di inserimento di base delle regole AWS IoT e inviare le metriche esportate alle destinazioni supportate dalle regole AWS IoT. Per istruzioni sull'impostazione e la configurazione delle regole AWS IoT, consulta Regole per AWS IoT nella Guida per gli sviluppatori di AWS IoT.

AWS IoT Device Defender Detect suddivide in batch i valori di ogni metrica configurata e li pubblica a intervalli regolari in un argomento MQTT configurato. A eccezione della dimensione in byte dei messaggi e della dimensione in byte totale, le metriche lato cloud vengono aggregate sommando i valori delle metriche per la durata del batch. Le metriche personalizzate e lato dispositivo non vengono aggregate. Per quanto riguarda la dimensione in byte dei messaggi, i valori di esportazione sono la dimensione minima, massima e totale in byte per la durata del batch. Per la durata della disconnessione, il valore di esportazione è la durata della disconnessione, in secondi, per tutti i dispositivi monitorati. Il valore viene calcolato a ogni intervallo di un'ora e anche per gli eventi di connessione o disconnessione. Per i dispositivi connessi o gli eventi di connessione, il valore è zero. Per ulteriori informazioni sulle metriche lato cloud, lato dispositivo e personalizzate, consulta i seguenti argomenti nella Guida per gli sviluppatori di AWS IoT Device Defender:

- Parametri personalizzati
- Parametri sul lato cloud
- Device-side metrics

Puoi esportare metriche in batch in diverse destinazioni con le regole AWS IoT. Per l'elenco delle destinazioni supportate, consulta Azioni delle regoleAWS IoT. Per inviare singole metriche all'interno di un messaggio di esportazione del batch a una destinazione supportata, utilizza l'opzione batchMode per le azioni delle regole AWS IoT. Se la destinazione delle regole AWS IoT preferita non è supportata da `batchMode`, puoi comunque inviare singole metriche all'interno di un messaggio del batch utilizzando azioni intermedie come Lambda o flusso di dati Kinesis.

Schema di esportazione delle metriche

Consulta lo schema seguente per i dati di esportazione delle metriche in batch.

```
{
 "version": "1.0",
 "metrics": [
 {
 "name": "{metricName}",
 "thing": "{thingName}",
 "value": {
 # a list of Classless Inter-Domain Routings (CIDR) specifying metric
# source-ip-address and destination-ip-address
 "cidrs": ["string"],
 # a single metric value for cloud/device metrics
 "count": number,
 # a single metric value for custom metric
 "number": number,
 # a list of numbers for custom metrics
 "numbers": [number],
 # a list of ports for cloud/device metrics
 "ports": [number],
 # a list of strings for custom metrics
 "strings": ["string"]
 },
 # In some rare cases we may send multiple values for the same thing, metric and
 timestamp.
 # When there are multiple values, please use the value with highest version number
 # and discard other values.
 "version": number,
 # For cloud-side metrics, this is the time when AWS IoT Device Defender Detect
 aggregates the
 # metrics data received from AWS IoT.
 # For device-side and custom metrics, this is the time at which the metrics data
 # is reported by the devices.
 "timestamp": number,
 # The dimension parameters are optional. It's set only if
 # the metrics are configured with a dimension in the security profile.
 "dimension": {
 "name": "{dimensionName}",
 "operator": "{dimensionOperator}"
 }
 }
 ]
}
```

Prezzi dell'esportazione delle metriche di Detect

Quando pubblichi metriche lato cloud, lato dispositivo o personalizzate in un argomento MQTT configurato, non dovrai sostenere i costi per questa fase del processo di esportazione. Tuttavia, nei passaggi successivi, quando trasferisci le metriche pubblicate in una destinazione di tua scelta, utilizzando il motore delle regole o il sistema di messaggistica, dovrai sostenere dei costi in base al metodo di trasferimento scelto. AWS IoT Device Defender pubblica le metriche in batch negli argomenti MQTT come un unico messaggio contenente i dati delle metriche per più dispositivi, consentendo così di controllare i costi. Per ulteriori informazioni sui prezzi, consulta il Calcolatore dei prezzi AWS.

Autorizzazioni

Questa sezione contiene informazioni su come configurare le policy e i ruoli IAM necessari per gestire l'esportazione delle metriche di AWS IoT Device Defender Detect. Per ulteriori informazioni, consultare la Guida per l'utente IAM.

Assegnazione ad AWS IoT Device Defender Detect dell'autorizzazione per pubblicare i messaggi in un argomento MQTT

Se abiliti l'esportazione delle metriche in CreateSecurityProfile, devi specificare un ruolo IAM con due policy: una policy di autorizzazione e una policy di attendibilità. La policy di autorizzazione assegna ad AWS IoT Device Defender l'autorizzazione a pubblicare i messaggi che includono le metriche in un argomento MQTT. La policy di attendibilità concede a AWS IoT Device Defender l'autorizzazione per assumere il ruolo richiesto.

Policy di autorizzazione

```
{
  "Version":"2012-10-17",
  "Statement":[
      {
        "Effect":"Allow",
        "Action":[
          "iot:Publish"
        ],
        "Resource":[
          "arn:aws:iot:region:account-id:topic/your-topic-name"
        ]
```

```
    }
  ]
}
```

Policy di attendibilità

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "iot.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

policy per il passaggio di ruoli

È necessaria anche una policy di autorizzazioni IAM collegata all'utente IAM che consenta all'utente di passare i ruoli. Vedere Concessione di autorizzazioni utente per il passaggio di un ruolo a un servizio AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": [
          "iam:GetRole",
          "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::account-id:role/Role_To_Pass"
    }
  ]
}
```

Configurazione dell'esportazione delle metriche di Detect nella console AWS IoT

Crea, visualizza e modifica un nuovo profilo di sicurezza che include l'esportazione delle metriche nella console.

Prerequisiti

Prima di configurare l'esportazione delle metriche di Detect, assicurati di aver soddisfatto i seguenti prerequisiti:

- Un ruolo IAM. Per ulteriori informazioni sulla creazione di un ruolo IAM, consulta Creating IAM role nella Guida per l'utente di IAM.
- Un account AWS al quale è possibile effettuare l'accesso come un utente AWS Identity and Access Management (IAM) con le autorizzazioni corrette. Per ulteriori informazioni sulle autorizzazioni di AWS IoT Device Defender Detect, consulta Autorizzazioni nella Guida per gli sviluppatori di AWS IoT Core.

Creazione di un nuovo profilo di sicurezza con esportazione delle metriche (console)

Per esportare i dati sul comportamento delle metriche, configura innanzitutto un profilo di sicurezza che includa l'esportazione delle metriche. La procedura seguente descrive in dettaglio come impostare un profilo di sicurezza basato sulle regole che includa l'esportazione delle metriche di Detect.

Per creare un nuovo profilo di sicurezza con esportazione delle metriche

1. Apri la AWS IoT console. Nella barra di navigazione, espandi Sicurezza, Rileva, Profili di sicurezza.
2. Per Crea profilo di sicurezza, scegli Crea profilo di rilevamento anomalie basato su regole.
3. Per specificare le proprietà del profilo di sicurezza, inserisci il Nome del profilo di sicurezza e in Destinazione scegli un gruppo di dispositivi di cui monitorare le anomalie. (Facoltativo) Includi una descrizione e applica i tag per etichettare le risorseAWS. Seleziona Successivo.
4. Per Parametro scegli le metriche per definire il comportamento del dispositivo. Puoi definire la soglia di comportamento per ricevere un avviso quando il dispositivo non soddisfa le aspettative di comportamento.

5. Per ricevere gli avvisi per le anomalie di comportamento scegli Invia un avviso (definisci il comportamento della metrica), quindi specifica il nome del comportamento e le condizioni. Per mantenere le metriche senza avvisi, scegli Non inviare un avviso (mantieni la metrica). Seleziona Next (Successivo).
6. Per configurare l'esportazione delle metriche scegli Attiva l'esportazione delle metriche.
7. Inserisci il nome di un argomento MQTT per pubblicare i dati delle metriche in AWS IoT Core. Scegli un ruolo IAM per assegnare ad AWS IoT l'autorizzazione "AWS IoT:Publish" per pubblicare messaggi nell'argomento configurato. Scegli le metriche che desideri esportare, quindi seleziona Successivo.

   > **Note**
   >
   > Utilizza la barra per rappresentare le informazioni gerarchiche quando inserisci il nome dell'argomento MQTT. Ad esempio `$AWS/rules/rule-name/`.

8. Per inviare gli avvisi alla console AWS quando un dispositivo viola un comportamento impostato, scegli o crea un argomento Amazon SNS e un ruolo IAM. Seleziona Successivo.
9. Rivedi le configurazioni, quindi scegli Successivo.

Visualizzazione e modifica dei dettagli del profilo di sicurezza (console)

Per visualizzare e modificare i dettagli del profilo di sicurezza

1. Apri la AWS IoT console. Nella barra di navigazione, espandi Sicurezza, Rileva, Profili di sicurezza.
2. Scegli il profilo di sicurezza che hai creato per includere l'esportazione delle metriche, quindi in Operazioni seleziona Modifica.
3. In Destinazione seleziona i gruppi di dispositivi di destinazione che desideri modificare, quindi scegli Successivo.
4. Per modificare le configurazioni del comportamento delle metriche, scegli Avvisami (definisci il comportamento del parametro), quindi stabilisci le condizioni per la soddisfazione dei comportamenti delle metriche. Seleziona Successivo.
5. Per disattivare le configurazioni di esportazione delle metriche scegli Disattiva l'esportazione delle metriche. Seleziona Successivo.

6. Per configurare Amazon SNS per inviare gli avvisi alla console AWS IoT quando un dispositivo viola un comportamento impostato, scegli o crea un argomento Amazon SNS e un ruolo IAM. Seleziona Successivo.
7. Rivedi le configurazioni e scegli Successivo.

Creazione di un profilo di sicurezza per abilitare l'esportazione delle metriche

Utilizza il comando `create-security-profile` per creare il profilo di sicurezza e abilitare l'esportazione delle metriche.

Per creare un profilo di sicurezza con esportazione delle metriche

1. Per abilitare l'esportazione delle metriche e indicare se Detect deve esportare le metriche corrispondenti, imposta il valore `exportMetric` su true in `Behavior` e `AdditionalMetricsToRetainV2`.
2. Includi il valore per `MetricsExportConfig`. Specifica il nome della risorsa Amazon (ARN) del ruolo e dell'argomento MQTT richiesto per l'esportazione delle metriche.

> **Note**
>
> Includi `mqttTopic` in modo che AWS IoT Device Defender Detect possa pubblicare i messaggi. L'ARN del ruolo è autorizzato a pubblicare messaggi MQTT, quindi AWS IoT Device Defender Detect può assumere il ruolo e pubblicare messaggi per tuo conto.

```
aws iot create-security-profile \
    --security-profile-name CreateSecurityProfileWithMetricsExport \
    --security-profile-description "create security profile with metrics export
 enabled"  \
    --behaviors "[{\"name\":\"BehaviorNumAuthz\",\"metric\":\"aws:num-authorization-
failures\",\"criteria\":{\"comparisonOperator\":\"less-than\",\"value\":{\"count
\":5}, \"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1,
\"durationSeconds\":300},\"exportMetric\":true}]" \
    --metrics-export-config "{\"mqttTopic\":\"\$aws/rules/metricsExportRule\",\"roleArn
\":\"arn:aws:iam::123456789012:role/iot-test-role\"}" \
    --region us-east-1
```

Output:

```
{
    "securityProfileName": "CreateSecurityProfileWithMetricsExport",
    "securityProfileArn": "arn:aws:iot:us-east-1:123456789012:securityprofile/
CreateSecurityProfileWithMetricsExport"
}
```

Aggiornamento di un profilo di sicurezza per abilitare l'esportazione delle metriche (CLI)

Utilizza il comando `update-security-profile` per aggiornare un profilo di sicurezza esistente e abilitare l'esportazione delle metriche.

Per aggiornare un profilo di sicurezza per abilitare l'esportazione delle metriche

1. Per abilitare l'esportazione delle metriche e indicare se Detect deve esportare le metriche corrispondenti, imposta il valore `exportMetric` su true in `Behavior` e `AdditionalMetricsToRetainV2`.
2. Includi il valore per `MetricsExportConfig`. Specifica il nome della risorsa Amazon (ARN) del ruolo e dell'argomento MQTT richiesto per l'esportazione delle metriche.

> **Note**
>
> Includi `mqttTopic` in modo che AWS IoT Device Defender Detect possa pubblicare i messaggi. L'ARN del ruolo è autorizzato a pubblicare messaggi MQTT, quindi AWS IoT Device Defender Detect può assumere il ruolo e pubblicare messaggi per tuo conto.

```
aws iot update-security-profile \
    --security-profile-name UpdateSecurityProfileWithMetricsExport \
    --security-profile-description "update an existing security profile to enable
 metrics export"  \
    --behaviors "[{\"name\":\"BehaviorNumAuthz\",\"metric\":\"aws:num-authorization-
failures\",\"criteria\":{\"comparisonOperator\":\"less-than\",\"value\":{\"count
\":5}, \"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1,
\"durationSeconds\":300},\"exportMetric\":true}]" \
    --metrics-export-config "{\"mqttTopic\":\"\$aws/rules/metricsExportRule\",\"roleArn
\":\"arn:aws:iam::123456789012:role/iot-test-role\"}" \
```

```
    --region us-east-1
```

Output:

```
{
    "securityProfileName": "UpdateSecurityProfileWithMetricsExport",
    "securityProfileArn": "arn:aws:iot:us-east-1:123456789012:securityprofile/
UpdateSecurityProfileWithMetricsExport",
    "securityProfileDescription": "update an existing security profile to enable
 metrics export",
    "behaviors": [
        {
            "name": "BehaviorNumAuthz",
            "metric": "aws:num-authorization-failures",
            "criteria": {
                "comparisonOperator": "less-than",
                "value": {
                    "count": 5
                },
                "durationSeconds": 300,
                "consecutiveDatapointsToAlarm": 1,
                "consecutiveDatapointsToClear": 1
            },
            "exportMetric": true
        }
    ],
    "version": 2,
    "creationDate": "2023-11-09T16:18:37.183000-08:00",
    "lastModifiedDate": "2023-11-09T16:20:15.486000-08:00",
    "metricsExportConfig": {
        "mqttTopic": "$aws/rules/metricsExportRule",
        "roleArn": "arn:aws:iam::123456789012:role/iot-test-role"
    }
}
```

Aggiornamento di un profilo di sicurezza per disattivare l'esportazione delle metriche (CLI)

Utilizza il comando `update-security-profile` per aggiornare un profilo di sicurezza esistente e disattivare l'esportazione delle metriche.

Per aggiornare un profilo di sicurezza e disattivare l'esportazione delle metriche

- Per aggiornare il profilo di sicurezza e rimuovere la configurazione dell'esportazione delle metriche si usa il comando `--delete-metrics-export-config`.

```
aws iot update-security-profile \
    --security-profile-name UpdateSecurityProfileToDisableMetricsExport \
    --security-profile-description "update an existing security profile to disable
 metrics export"  \
    --behaviors "[{\"name\":\"BehaviorNumAuthz\",\"metric\":\"aws:num-authorization-
failures\",\"criteria\":{\"comparisonOperator\":\"less-than\",\"value\":{\"count
\":5}, \"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1,
\"durationSeconds\":300}}]" \
    --delete-metrics-export-config \
    --region us-east-1
```

Output:

```
{
    "securityProfileName": "UpdateSecurityProfileToDisableMetricsExport",
    "securityProfileArn": "arn:aws:iot:us-east-1:123456789012:securityprofile/
UpdateSecurityProfileWithMetricsExport",
    "securityProfileDescription": "update an existing security profile to disable
 metrics export",
    "behaviors": [
        {
            "name": "BehaviorNumAuthz",
            "metric": "aws:num-authorization-failures",
            "criteria": {
                "comparisonOperator": "less-than",
                "value": {
                    "count": 5
                },
                "durationSeconds": 300,
                "consecutiveDatapointsToAlarm": 1,
                "consecutiveDatapointsToClear": 1
            }
        }
    ],
    "version": 2,
    "creationDate": "2023-11-09T16:18:37.183000-08:00",
    "lastModifiedDate": "2023-11-09T16:31:16.265000-08:00"
```

```
}
```

Per ulteriori informazioni, consulta Comandi di rilevamento nella Guida per gli sviluppatori di AWS IoT.

Comandi CLI per l'esportazione delle metriche

Puoi utilizzare i comandi CLI seguenti per creare e gestire l'esportazione delle metriche di Detect.

- CreateSecurityProfile
- UpdateSecurityProfile
- DescribeSecurityProfile

Operazioni API per l'esportazione delle metriche

Puoi utilizzare le operazioni API seguenti per creare e gestire l'esportazione delle metriche di Detect.

- CreateSecurityProfile
- UpdateSecurityProfile
- DescribeSecurityProfile

Parametri di ambito nei profili di sicurezza utilizzando le dimensioni

Le dimensioni sono attributi che è possibile definire per ottenere dati più precisi sui parametri e sui comportamenti nel profilo di sicurezza. È possibile definire l'ambito fornendo un valore o un modello utilizzato come filtro. Ad esempio, è possibile definire una dimensione del filtro argomento che applica un parametro solo agli argomenti MQTT corrispondenti a un valore particolare, ad esempio "data/bulb/+/activity". Per informazioni sulla definizione di una dimensione che è possibile utilizzare nel profilo di sicurezza, vedere CreateDimension.

I valori di dimensione supportano i caratteri jolly MQTT. I caratteri jolly MQTT consentono di sottoscrivere più argomenti contemporaneamente. Esistono due diversi tipi di caratteri jolly: single-level (+) e multi-level (#). Ad esempio, il valore di dimensione `Data/bulb/+/activity` crea una sottoscrizione che corrisponde a tutti gli argomenti esistenti allo stesso livello di +. I valori di dimensione supportano anche la variabile di sostituzione dell'ID client MQTT ${iot:ClientId}.

Le dimensioni di tipo TOPIC_FILTER sono compatibili con il seguente set di parametri lato cloud:

- Numero di errori di autorizzazione
- Dimensione del byte del messaggio
- Numero di messaggi ricevuti
- Numero di messaggi inviati
- Indirizzo IP di origine (disponibile solo per Rules Detect)

Come utilizzare le dimensioni nella console

Per creare e applicare una dimensione a un comportamento del profilo di sicurezza

1. Apri la AWS IoT console. Nel riquadro di navigazione, espandi Sicurezza, Rileva e scegli Profili di sicurezza.
2. Nella pagina Profili di sicurezza, scegli Crea profilo di sicurezza, quindi scegli Crea profilo di rilevamento anomalie basato su regole. Oppure, per applicare una dimensione a un profilo di sicurezza basato su regole esistente, seleziona il profilo di sicurezza e scegli Modifica.
3. Nella pagina Specifica le proprietà del profilo di sicurezza, immetti un nome per il profilo di sicurezza.
4. Scegli il gruppo di dispositivi di cui desideri individuare eventuali anomalie.
5. Seleziona Avanti.
6. Nella pagina Configura i comportamenti della metrica, scegli una delle dimensioni delle metriche sul lato cloud in Tipo di metrica.
7. Per Comportamento del parametro, scegli Invia un avviso (definisci il comportamento della metrica) per definire il comportamento previsto delle metriche.
8. Scegli quando vuoi ricevere avvisi relativi a comportamenti insoliti del dispositivo.
9. Seleziona Avanti.
10. Esamina la configurazione del profilo di sicurezza e scegli Crea.

Visualizzazione degli allarmi

1. Apri la AWS IoT console. Nel riquadro di navigazione, espandi Sicurezza, Rileva e quindi scegli Allarmi.
2. Nella colonna Nome oggetto, scegli l'oggetto per visualizzare le informazioni sulla causa dell'allarme.

Per visualizzare e aggiornare le dimensioni

1. Apri la AWS IoT console. Nel riquadro di navigazione, espandi Sicurezza, Rileva e quindi scegli Dimensioni.
2. Seleziona la dimensione e scegli Modifica.
3. Modifica la dimensione e scegli Aggiorna.

Per eliminare una dimensione

1. Apri la AWS IoT console. Nel riquadro di navigazione, espandi Sicurezza, Rileva e quindi scegli Dimensioni.
2. Prima di eliminare una dimensione, devi eliminare il comportamento della metrica che fa riferimento alla dimensione. Verifica che la dimensione non sia collegata a un profilo di sicurezza selezionando la colonna Profili di sicurezza. Se la dimensione è collegata a un profilo di sicurezza, apri la pagina Profili di sicurezza a sinistra e modifica il profilo di sicurezza a cui è collegata la dimensione. Quindi procedere con l'eliminazione del comportamento. Se si desidera eliminare un'altra dimensione, attenersi alla procedura descritta in questa sezione.
3. Seleziona la dimensione e scegli Elimina.
4. Digita il nome della dimensione nel campo per confermare e quindi scegli Elimina.

Come utilizzare le dimensioni in AWS CLI

Per creare e applicare una dimensione a un comportamento del profilo di sicurezza

1. Creare innanzitutto la dimensione prima di collegarla a un profilo di sicurezza. Utilizza il comando CreateDimension per creare una dimensione:

```
aws iot create-dimension \
  --name TopicFilterForAuthMessages \
  --type TOPIC_FILTER \
  --string-values device/+/auth
```

   L'output di questo comando è simile al seguente:

```
{
    "arn": "arn:aws:iot:us-west-2:123456789012:dimension/
TopicFilterForAuthMessages",
```

```
    "name": "TopicFilterForAuthMessages"
}
```

2. Aggiungi la dimensione a un profilo di sicurezza esistente utilizzando UpdateSecurityProfile o aggiungila a un nuovo profilo di sicurezza utilizzando CreateSecurityProfile. Nell'esempio seguente viene creato un nuovo profilo di sicurezza che controlla se i messaggi per `TopicFilterForAuthMessages` sono inferiori a 128 byte e mantiene il numero di messaggi inviati ad argomenti non di autenticazione.

```
aws iot create-security-profile \
  --security-profile-name ProfileForConnectedDevice \
  --security-profile-description "Check to see if messages to
 TopicFilterForAuthMessages are under 128 bytes and retains the number of messages
 sent to non-auth topics." \
  --behaviors "[{\"name\":\"CellularBandwidth\",\"metric\":\"aws:message-byte-size
\",\"criteria\":{\"comparisonOperator\":\"less-than\",\"value\":{\"count\":128},
\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}},{\"name
\":\"Authorization\",\"metric\":\"aws:num-authorization-failures\",\"criteria\":
{\"comparisonOperator\":\"less-than\",\"value\":{\"count\":10},\"durationSeconds
\":300,\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}}]" \
  --additional-metrics-to-retain-v2 "[{\"metric\": \"aws:num-authorization-failures
\",\"metricDimension\": {\"dimensionName\": \"TopicFilterForAuthMessages\",
\"operator\": \"NOT_IN\"}}]"
```

L'output di questo comando è simile al seguente:

```
{
    "securityProfileArn": "arn:aws:iot:us-west-2:1234564789012:securityprofile/
ProfileForConnectedDevice",
    "securityProfileName": "ProfileForConnectedDevice"
}
```

È inoltre possibile caricare un parametro da un file invece di digitarlo per intero come valore di parametro della riga di comando. Per ulteriori informazioni, consulta Caricamento dei parametri AWS CLI da un file. Di seguito è riportato il parametro `behavior` in formato JSON espanso:

```
[
  {
    "criteria": {
      "comparisonOperator": "less-than",
      "consecutiveDatapointsToAlarm": 1,
```

```
      "consecutiveDatapointsToClear": 1,
      "value": {
        "count": 128
      }
    },
    "metric": "aws:message-byte-size",
    "metricDimension": {
      "dimensionName:": "TopicFilterForAuthMessages"
    },
    "name": "CellularBandwidth"
  }
]
```

Oppure utilizzare CreateSecurityProfile utilizzando una dimensione con ML come riportato nell'esempio seguente:

```
aws iot create-security-profile --security-profile-name ProfileForConnectedDeviceML
 \
   --security-profile-description “Check to see if messages to
 TopicFilterForAuthMessages are abnormal”  \
   --behaviors “[{\“name\“:\“test1\“,\“metric\“:\“aws:message-byte-size\“,
\“metricDimension\“:{\“dimensionName\“: \“TopicFilterForAuthMessages\“,\“operator
\“: \“IN\“},\“criteria\“:{\“mlDetectionConfig\“:{\“confidenceLevel\“:\“HIGH\“},
\“consecutiveDatapointsToAlarm\“:1,\“consecutiveDatapointsToClear\“:1}}]” \
   --region us-west-2
```

Per visualizzare i profili di sicurezza con una dimensione

- Utilizza il comando ListSecurityProfiles per visualizzare i profili di sicurezza con una determinata dimensione:

```
aws iot list-security-profiles \
  --dimension-name TopicFilterForAuthMessages
```

L'output di questo comando è simile al seguente:

```
{
    "securityProfileIdentifiers": [
        {
            "name": "ProfileForConnectedDevice",
```

```
            "arn": "arn:aws:iot:us-west-2:1234564789012:securityprofile/
ProfileForConnectedDevice"
        }
    ]
}
```

Per aggiornare la dimensione

- Utilizza il comando UpdateDimension per aggiornare una dimensione:

```
aws iot update-dimension \
  --name TopicFilterForAuthMessages \
  --string-values device/${iot:ClientId}/auth
```

L'output di questo comando è simile al seguente:

```
{
    "name": "TopicFilterForAuthMessages",
    "lastModifiedDate": 1585866222.317,
    "stringValues": [
        "device/${iot:ClientId}/auth"
    ],
    "creationDate": 1585854500.474,
    "type": "TOPIC_FILTER",
    "arn": "arn:aws:iot:us-west-2:1234564789012:dimension/
TopicFilterForAuthMessages"
}
```

Per eliminare una dimensione

1. Per eliminare una dimensione, scollegarla prima da tutti i profili di sicurezza a cui è collegata. Utilizza il comando ListSecurityProfiles per visualizzare i profili di sicurezza con una determinata dimensione.
2. Per rimuovere una dimensione da un profilo di sicurezza, utilizza il comando UpdateSecurityProfile. Immettere tutte le informazioni che si desidera conservare, ma escludere la dimensione:

```
aws iot update-security-profile \
  --security-profile-name ProfileForConnectedDevice \
```

```
  --security-profile-description "Check to see if authorization fails 10 times in 5
 minutes or if cellular bandwidth exceeds 128" \
  --behaviors "[{\"name\":\"metric\":\"aws:message-byte-size\",\"criteria
\":{\"comparisonOperator\":\"less-than\",\"value\":{\"count\":128},
\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}},{\"name
\":\"Authorization\",\"metric\":\"aws:num-authorization-failures\",\"criteria\":
{\comparisonOperator\":\"less-than\",\"value\"{\"count\":10},\"durationSeconds
\":300,\"consecutiveDatapointsToAlarm\":1,\"consecutiveDatapointsToClear\":1}}]"
```

L'output di questo comando è simile al seguente:

```
{
  "behaviors": [
    {
      "metric": "aws:message-byte-size",
      "name": "CellularBandwidth",
      "criteria": {
        "consecutiveDatapointsToClear": 1,
        "comparisonOperator": "less-than",
        "consecutiveDatapointsToAlarm": 1,
        "value": {
          "count": 128
        }
      }
    },
    {
      "metric": "aws:num-authorization-failures",
      "name": "Authorization",
      "criteria": {
        "durationSeconds": 300,
        "comparisonOperator": "less-than",
        "consecutiveDatapointsToClear": 1,
        "consecutiveDatapointsToAlarm": 1,
        "value": {
          "count": 10
        }
      }
    }
  ],
  "securityProfileName": "ProfileForConnectedDevice",
  "lastModifiedDate": 1585936349.12,
  "securityProfileDescription": "Check to see if authorization fails 10 times in 5
 minutes or if cellular bandwidth exceeds 128",
```

```
  "version": 2,
  "securityProfileArn": "arn:aws:iot:us-west-2:123456789012:securityprofile/Preo/
ProfileForConnectedDevice",
  "creationDate": 1585846909.127
}
```

3. Dopo che la dimensione è stata scollegata, utilizza il comando DeleteDimension per eliminarla:

```
aws iot delete-dimension \
  --name TopicFilterForAuthMessages
```

Autorizzazioni

Questa sezione contiene informazioni su come configurare le policy e i ruoli IAM necessari per gestire AWS IoT Device Defender Detect. Per ulteriori informazioni, consulta Guida per l'utente di IAM.

Concedi ad AWS IoT Device Defender Detect l'autorizzazione per pubblicare gli avvisi in un argomento SNS

Se usi il parametro `alertTargets` in CreateSecurityProfile, devi specificare un ruolo IAM con due policy, una policy di autorizzazioni e una policy di trust. La policy di autorizzazioni concede a AWS IoT Device Defender l'autorizzazione per pubblicare le notifiche nell'argomento SNS. La policy di attendibilità concede a AWS IoT Device Defender l'autorizzazione per assumere il ruolo richiesto.

Policy di autorizzazione

```
{
  "Version":"2012-10-17",
  "Statement":[
      {
        "Effect":"Allow",
        "Action":[
          "sns:Publish"
        ],
        "Resource":[
          "arn:aws:sns:region:account-id:your-topic-name"
        ]
    }
  ]
}
```

Policy di attendibilità

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "iot.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

policy per il passaggio di ruoli

È necessaria anche una policy di autorizzazioni IAM collegata all'utente IAM che consenta all'utente di passare i ruoli. Vedere Concessione di autorizzazioni utente per il passaggio di un ruolo a un servizio AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": [
          "iam:GetRole",
          "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::account-id:role/Role_To_Pass"
    }
  ]
}
```

Comandi di rilevamento

È possibile utilizzare i comandi Detect in questa sezione per configurare i profili di ML Detect o di Rules Detect, per identificare e monitorare i comportamenti insoliti che potrebbero indicare un dispositivo compromesso.

Comandi delle operazioni DetectMitigation

Avviare e gestire l'esecuzione di Detect
CancelDetectMitigationActionsTask
DescribeDetectMitigationActionsTask
ListDetectMitigationActionsTasks
StartDetectMitigationActionsTask
ListDetectMitigationActionsExecutions

Comandi delle operazioni di dimensioni

Avviare e gestire l'esecuzione della funzione Dimensioni
CreateDimension
DescribeDimension
ListDimensions
DeleteDimension
UpdateDimension

Comandi dell'operazione CustomMetric

Avviare e gestire l'esecuzione di CustomMetric
CreateCustomMetric

Avviare e gestire l'esecuzione di CustomMetric
UpdateCustomMetric
DescribeCustomMetric
ListCustomMetrics
DeleteCustomMetric

Comandi di operazioni del profilo di sicurezza

Avviare e gestire l'esecuzione del profilo di sicurezza
CreateSecurityProfile
AttachSecurityProfile
DetachSecurityProfile
DeleteSecurityProfile
DescribeSecurityProfile
ListTargetsForSecurityProfile
UpdateSecurityProfile
ValidateSecurityProfileBehaviors
ListSecurityProfilesForTarget

Comandi per l'operazione degli allarmi

Gestione degli allarmi e delle destinazioni
ListActiveViolations
ListViolationEvents

Gestione degli allarmi e delle destinazioni
PutVerificationStateOnViolation

Comandi di operazione di ML Detect

Elenca i dati di formazione del modello ML
GetBehaviorModelTrainingSummaries

Come utilizzare AWS IoT Device Defender Detect

1. Puoi usare AWS IoT Device Defender Detect con solo i parametri lato cloud, ma se prevedi di usare parametri segnalati dai dispositivi, dovrai innanzitutto distribuire un SDK AWS IoT nei gateway dei dispositivi o nei dispositivi connessi a AWS IoT. Per ulteriori informazioni, consultare Invio di parametri dai dispositivi.
2. Considerare di visualizzare le metriche generate dai dispositivi prima di definire i comportamenti e creare gli allarmi. AWS IoT è in grado di raccogliere i parametri dai tuoi dispositivi in modo da identificare innanzitutto un comportamento consueto o insolito per un gruppo di dispositivi o per tutti i dispositivi nel tuo account. Utilizza CreateSecurityProfile, ma specifica solo i parametri `additionalMetricsToRetain` di interesse. Non specificare `behaviors` a questo punto.

   Utilizza la console AWS IoT per vedere i parametri del tuo dispositivo e definire in cosa consiste il comportamento tipico dei tuoi dispositivi.
3. Crea un set di comportamenti per il profilo di sicurezza. I comportamenti contengono parametri che specificano il comportamento normale per un gruppo di dispositivi o per tutti i dispositivi nell'account. Per ulteriori informazioni ed esempi, consulta Parametri sul lato cloud e Device-side metrics. Dopo aver creato un set di comportamenti, puoi convalidarli con ValidateSecurityProfileBehaviors.
4. Usa l'operazione CreateSecurityProfile per creare un profilo di sicurezza che includa i comportamenti. Puoi fare in modo che vengano inviati allarmi a un target (un argomento SNS) quando un dispositivo viola un comportamento utilizzando il parametro `alertTargets`. Se invii allarmi tramite SNS, tieni presente che verranno conteggiati per il raggiungimento della quota SNS per l'account Account AWS. È possibile che una grande quantità di violazioni possa determinare il superamento della quota di argomenti SNS. È inoltre possibile utilizzare i

parametri CloudWatch per verificare la presenza di violazioni. Per ulteriori informazioni, consulta Monitorare allarmi e metriche di AWS IoT utilizzando Amazon CloudWatch nella Guida per gli sviluppatori di AWS IoT Core.

5. Utilizza l'operazione AttachSecurityProfile per collegare il profilo di sicurezza a un gruppo di dispositivi (un gruppo di oggetti), tutti gli oggetti registrati nel tuo account, tutti gli oggetti non registrati o tutti i dispositivi. AWS IoT Device Defender Detect inizia a verificare la presenza di comportamenti anomali e, se viene rilevato il comportamento di eventuali violazioni, invia allarmi. È possibile allegare un profilo di sicurezza a tutti gli oggetti non registrati se, ad esempio, si prevede di interagire con dispositivi mobili che non sono nel registro degli oggetti del tuo account. È possibile definire comportamenti diversi per i diversi gruppi di dispositivi per soddisfare le tue esigenze.

   Per collegare un profilo di sicurezza a un gruppo di dispositivi, è necessario specificare l'ARN del gruppo di oggetti che li contiene. L'ARN di un gruppo di oggetti ha il formato seguente.

   ```
   arn:aws:iot:region:account-id:thinggroup/thing-group-name
   ```

   Per collegare un profilo di sicurezza a tutti gli oggetti registrati in un account Account AWS (ignorando gli oggetti non registrati), è necessario specificare un ARN con il seguente formato.

   ```
   arn:aws:iot:region:account-id:all/registered-things
   ```

   Per allegare un profilo di sicurezza a tutti gli oggetti non registrati, è necessario specificare un ARN con il seguente formato.

   ```
   arn:aws:iot:region:account-id:all/unregistered-things
   ```

   Per allegare un profilo di sicurezza a tutti i dispositivi, è necessario specificare un ARN con il seguente formato.

   ```
   arn:aws:iot:region:account-id:all/things
   ```

6. È anche possibile tenere traccia delle violazioni con l'operazione ListActiveViolations, che consente di visualizzare le violazioni rilevate per un determinato profilo di sicurezza o dispositivo target.

Utilizzare l'operazione ListViolationEvents per vedere quali violazioni sono state rilevate durante un periodo di tempo specificato. È possibile filtrare i risultati in base a un determinato profilo, dispositivo o stato di verifica dall'allarme.

7. È possibile verificare, organizzare e gestire gli allarmi, contrassegnandone lo stato di verifica e fornendo una descrizione dello stato di verifica, utilizzando l'operazione PutVerificationStateOnViolation.
8. Se i tuoi dispositivi violano i comportamenti definiti troppo spesso o non abbastanza spesso, è consigliabile affinare le definizioni del comportamento.
9. Per esaminare i profili di sicurezza configurati e i dispositivi monitorati, utilizza le operazioni ListSecurityProfiles, ListSecurityProfilesForTarget, e ListTargetsForSecurityProfile.

   Utilizza l'operazione DescribeSecurityProfile per ottenere ulteriori dettagli su un profilo di sicurezza.
10. Per aggiornare un profilo di sicurezza, utilizza l'operazione UpdateSecurityProfile. Utilizza l'operazione DetachSecurityProfile per distaccare un profilo di sicurezza da parte di un account o di un gruppo di oggetti target. Utilizza l'operazione DeleteSecurityProfile per eliminare completamente un profilo di sicurezza.

Operazioni di mitigazione

Puoi utilizzare AWS IoT Device Defender per eseguire operazioni per mitigare i problemi rilevati in un avviso di audit o un Detect allarmi.

> **Note**
>
> Le operazioni di mitigazione non verranno eseguite sui risultati di audit soppressi. Per ulteriori informazioni sulle soppressioni dei risultati di audit, consulta Soppressioni della ricerca di audit.

Operazioni di mitigazione di verifica

AWS IoT Device Defender fornisce operazioni predefinite per i diversi controlli di audit. Puoi configurare queste operazioni nel tuo Account AWS, e quindi applicarle a un set di risultati. Questi risultati possono essere:

- Tutti i risultati di un audit. Questa opzione è disponibile sia nella console AWS IoT, sia utilizzando AWS CLI.
- Un elenco dei singoli risultati. Questa opzione è disponibile solo utilizzando AWS CLI.
- Un set filtrato di risultati di un audit.

La tabella seguente elenca i tipi di controlli di auditing e le operazione di mitigazione supportate per ognuno:

Mapping dai controlli di auditing alle operazioni di mitigazione

Controllo di auditing	Operazioni di mitigazione supportate
REVOKED_CA_CERT_CHECK	PUBLISH_FINDING_TO_SNS, UPDATE_CA_CERTIFICATE
INTERMEDIATE_CA_REVOKED_FOR_ACTIVE_DEVICE_CERTIFICATES_CHECK	PUBLISH_FINDING_TO_SNS, UPDATE_DEVICE_CERTIFICATE, ADD_THINGS_TO_THING_GROUP

Controllo di auditing	Operazioni di mitigazione supportate
DEVICE_CERTIFICATE_SHARED_CHECK	PUBLISH_FINDING_TO_SNS, UPDATE_DEVICE_CERTIFICATE, ADD_THINGS_TO_THING_GROUP
UNAUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK	PUBLISH_FINDING_TO_SNS
AUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK	PUBLISH_FINDING_TO_SNS
IOT_POLICY_OVERLY_PERMISSIVE_CHECK	PUBLISH_FINDING_TO_SNS, REPLACE_DEFAULT_POLICY_VERSION
IOT_POLICY_POTENTIAL_MISCONFIGURATION_CHECK	PUBLISH_FINDING_TO_SNS, REPLACE_DEFAULT_POLICY_VERSION
CA_CERTIFICATE_EXPIRING_CHECK	PUBLISH_FINDING_TO_SNS, UPDATE_CA_CERTIFICATE
CONFLICTING_CLIENT_IDS_CHECK	PUBLISH_FINDING_TO_SNS
DEVICE_CERTIFICATE_EXPIRING_CHECK	PUBLISH_FINDING_TO_SNS, UPDATE_DEVICE_CERTIFICATE, ADD_THINGS_TO_THING_GROUP
REVOKED_DEVICE_CERTIFICATE_STILL_ACTIVE_CHECK	PUBLISH_FINDING_TO_SNS, UPDATE_DEVICE_CERTIFICATE, ADD_THINGS_TO_THING_GROUP
LOGGING_DISABLED_CHECK	PUBLISH_FINDING_TO_SNS, ENABLE_IOT_LOGGING
DEVICE_CERTIFICATE_KEY_QUALITY_CHECK	PUBLISH_FINDING_TO_SNS, UPDATE_DEVICE_CERTIFICATE, ADD_THINGS_TO_THING_GROUP

Controllo di auditing	Operazioni di mitigazione supportate
CA_CERTIFICATE_KEY_QUALITY_CHECK	PUBLISH_FINDING_TO_SNS, UPDATE_CA_CERTIFICATE
IOT_ROLE_ALIAS_OVERLY_PERMISSIVE_CHECK	PUBLISH_FINDING_TO_SNS
IOT_ROLE_ALIAS_ALLOWS_ACCESS_TO_UNUSED_SERVICES_CHECK	PUBLISH_FINDING_TO_SNS

Tutti i controlli di audit supportano la pubblicazione dei risultati di audit in Amazon SNS per consentirti di effettuare operazioni personalizzate in risposta alla notifica. Ogni tipo di controllo di auditing può supportare altre operazioni di mitigazione:

REVOKED_CA_CERT_CHECK

- Cambiare lo stato del certificato per contrassegnarlo come inattivo in AWS IoT.

DEVICE_CERTIFICATE_SHARED_CHECK

- Cambiare lo stato del certificato del dispositivo per contrassegnarlo come inattivo in AWS IoT.
- Aggiungere i dispositivi che utilizzano il certificato a un gruppo di oggetti.

UNAUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK

- Nessun'altra operazione supportata.

AUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK

- Nessun'altra operazione supportata.

IOT_POLICY_OVERLY_PERMISSIVE_CHECK

- Aggiungere una versione della policy AWS IoT vuota per limitare le autorizzazioni.

IOT_POLICY_POTENTIAL_MISCONFIGURATION_CHECK

- Identificare potenziali errori di configurazione nelle policy AWS IoT.

CA_CERT_APPROACHING_EXPIRATION_CHECK

- Cambiare lo stato del certificato per contrassegnarlo come inattivo in AWS IoT.

CONFLICTING_CLIENT_IDS_CHECK

- Nessun'altra operazione supportata.

DEVICE_CERT_APPROACHING_EXPIRATION_CHECK

- Cambiare lo stato del certificato del dispositivo per contrassegnarlo come inattivo in AWS IoT.
- Aggiungere i dispositivi che utilizzano il certificato a un gruppo di oggetti.

DEVICE_CERTIFICATE_KEY_QUALITY_CHECK

- Cambiare lo stato del certificato del dispositivo per contrassegnarlo come inattivo in AWS IoT.
- Aggiungere i dispositivi che utilizzano il certificato a un gruppo di oggetti.

CA_CERTIFICATE_KEY_QUALITY_CHECK

- Cambiare lo stato del certificato per contrassegnarlo come inattivo in AWS IoT.

REVOKED_DEVICE_CERT_CHECK

- Cambiare lo stato del certificato del dispositivo per contrassegnarlo come inattivo in AWS IoT.
- Aggiungere i dispositivi che utilizzano il certificato a un gruppo di oggetti.

LOGGING_DISABLED_CHECK

- Attivare la registrazione nel log.

AWS IoT Device Defender supporta i seguenti tipi di operazioni di mitigazione sui risultati di controllo audit:

Tipo di operazione	Note
ADD_THINGS_TO_THING_GROUP	Specifica il gruppo a cui aggiungere i dispositi vi. Specifica anche se l'appartenenza a uno o più gruppi dinamici deve essere ignorata se supererebbe il numero massimo di gruppi a cui l'oggetto può appartenere.
ENABLE_IOT_LOGGING	Specifica il livello di logging e il ruolo con le autorizzazioni per il logging. Non è possibile specificare un livello di logging `DISABLED`.
PUBLISH_FINDING_TO_SNS	Specifica l'argomento in cui deve essere pubblicato il risultato.
REPLACE_DEFAULT_POLICY_VERSION	Specifica il nome del modello. Sostituisce la versione della policy con una policy predefini

Tipo di operazione	Note
	ta o vuota. Al momento è supportato solo un valore `BLANK_POLICY` .
UPDATE_CA_CERTIFICATE	Specifica il nuovo stato per il certificato CA. Al momento è supportato solo un valore `DEACTIVATE` .
UPDATE_DEVICE_CERTIFICATE	Specifica il nuovo stato per il certificato del dispositivo. Al momento è supportato solo un valore `DEACTIVATE` .

Configurando operazioni standard quando vengono rilevati problemi durante un audit, puoi rispondere a quei problemi in maniera coerente. Con queste operazioni di mitigazione definite, inoltre, puoi risolvere i problemi più rapidamente e con meno probabilità di errore umano.

> **Important**
>
> L'applicazione di operazioni di mitigazione che modificano i certificati, aggiungono oggetti a un nuovo gruppo di oggetti o sostituiscono la policy possono avere un impatto sui tuoi dispositivi e sulle tue applicazioni. Ad esempio, i dispositivi potrebbero non riuscire a connettersi. Valuta le implicazioni delle operazioni di mitigazione prima di applicarle. Potrebbe essere necessario eseguire altre operazioni per correggere i problemi prima che i tuoi dispositivi e le tue applicazioni possano funzionare normalmente. Ad esempio, potrebbe essere necessario fornire certificati dei dispositivi aggiornati. Le operazioni di mitigazione possono essere utili per limitare rapidamente il rischio, ma devi comunque attuare misure correttive per risolvere i problemi sottostanti.

Alcune operazioni, ad esempio la riattivazione di un certificato di dispositivo, possono essere eseguite solo manualmente. AWS IoT Device Defender non fornisce un meccanismo per eseguire automaticamente il rollback delle operazioni di mitigazione applicate.

Rilevare operazioni di mitigazione

AWS IoT Device Defender supporta i seguenti tipi di operazioni di mitigazione sul Detect allarmi:

Tipo di operazione	Note
ADD_THINGS_TO_THING_GROUP	Specifica il gruppo a cui aggiungere i dispositivi. Specifica anche se l'appartenenza a uno o più gruppi dinamici deve essere ignorata se supererebbe il numero massimo di gruppi a cui l'oggetto può appartenere.

Come definire e gestire le operazioni di mitigazione

Puoi utilizzare la console AWS IoT o la AWS CLI per definire e gestire le operazioni di mitigazione per il tuo Account AWS.

Creare operazioni di mitigazione

Ogni operazione di mitigazione personalizzata è una combinazione di un tipo di operazione predefinito e di parametri specifici del tuo account.

Per utilizzare la console AWS IoT per creare operazioni di mitigazione

1. Apri la pagina Mitigation actions (Operazioni di mitigazione) nella console AWS IoT.
2. Nella pagina Mitigation actions (Operazioni di mitigazione) scegli Create (Crea).
3. Nella pagina Create a new mitigation action (Crea una nuova operazione di mitigazione), in Action name (Nome operazione), immetti un nome univoco per l'operazione di mitigazione.
4. In Action type (Tipo di operazione) specificare il tipo di operazione da definire.
5. In Permissions (Autorizzazioni), scegli il ruolo IAM con le cui autorizzazioni viene applicata l'operazione.
6. Ogni tipo di operazione richiede un diverso set di parametri. Inserire i parametri per l'operazione. Ad esempio, se si sceglie il tipo di operazione Add things to thing group (Aggiungi oggetti a un gruppo di oggetti), scegliere il gruppo di destinazione e selezionare o deselezionare Override dynamic groups (Ignora gruppi dinamici).
7. Scegli Save (Salva) per salvare l'operazione di mitigazione per l'account AWS.

Per utilizzare AWS CLI per creare operazioni di mitigazione

- Utilizza il comando CreateMitigationAction per creare un'operazione di mitigazione. Il nome univoco assegnato all'operazione viene utilizzato quando si applica quell'operazione ai risultati di audit. Scegliere un nome significativo.

Per utilizzare la console AWS IoT per visualizzare e modificare le operazioni di mitigazione

1. Apri la pagina Mitigation actions (Operazioni di mitigazione) nella console AWS IoT.

   Nella pagina Mitigation Actions (Operazioni di mitigazione) viene riportato un elenco di tutte le operazioni di mitigazione definite per il tuo Account AWS.
2. Scegliere il link con il nome dell'operazione per l'operazione di mitigazione da modificare.
3. Scegli Edit (Modifica) per apportare modifiche all'operazione di mitigazione. Non è possibile modificare il nome perché il nome dell'operazione di mitigazione viene utilizzato per identificarla.
4. Scegli Update (Aggiorna) per salvare le modifiche apportate all'operazione di mitigazione nel tuo Account AWS.

Per utilizzare AWS CLI per elencare un'operazione di mitigazione

- Utilizza il comando ListMitigationAction per elencare le operazioni di mitigazione. Se si intende modificare o eliminare un'operazione di mitigazione, prendere nota del nome.

Per utilizzare AWS CLI per aggiornare un'operazione di mitigazione

- Utilizza il comando UpdateMitigationAction per modificare un'operazione di mitigazione.

Per utilizzare la console AWS IoT per eliminare un'operazione di mitigazione

1. Apri la pagina Mitigation actions (Operazioni di mitigazione) nella console AWS IoT.

   Nella pagina Mitigation Actions (Operazioni di mitigazione) sono riportate tutte le operazioni di mitigazione definite per il tuo Account AWS.
2. Scegli l'operazione di mitigazione che desideri eliminare e quindi seleziona Delete (Elimina).
3. Nella finestra Are you sure you want to delete (Eliminare), scegli Delete (Elimina).

Per utilizzare AWS CLI per eliminare operazioni di mitigazione

- Utilizza il comando UpdateMitigationAction per modificare un'operazione di mitigazione.

Per utilizzare la console AWS IoT per visualizzare i dettagli delle operazioni di mitigazione

1. Apri la pagina Mitigation actions (Operazioni di mitigazione) nella console AWS IoT.

   Nella pagina Mitigation Actions (Operazioni di mitigazione) sono riportate tutte le operazioni di mitigazione definite per il tuo Account AWS.
2. Scegli il link con il nome dell'operazione per l'operazione di mitigazione da visualizzare.

Per utilizzare AWS CLI per visualizzare i dettagli delle operazioni di mitigazione

- Utilizza il comando DescribeMitigationAction per visualizzare i dettagli dell'operazione di mitigazione.

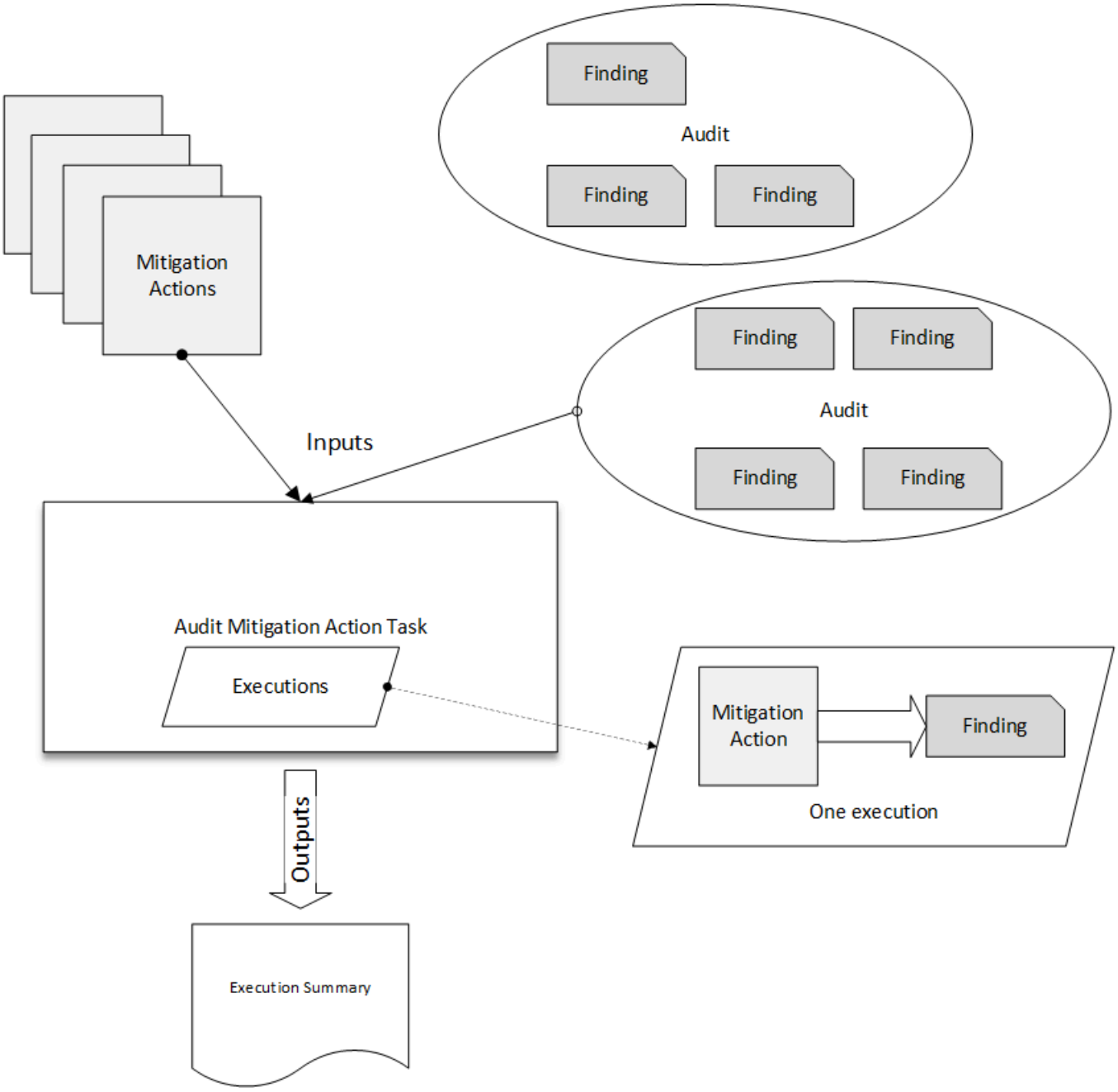
Applicare le operazioni di mitigazione

Dopo aver definito un set di operazioni di mitigazione, è possibile applicarle ai risultati di un audit. Quando si applicano le operazioni, si avvia un'attività di operazioni di mitigazione di audit. Questa operazione potrebbe richiedere alcuni minuti, a seconda del set di risultati e delle operazioni applicate. Ad esempio, in presenza di un ampio pool di dispositivi con certificati scaduti, potrebbero essere necessari alcuni minuti per disattivare tutti i certificati o spostare i dispositivi in un gruppo di quarantena. Altre operazioni, come l'abilitazione del logging, possono essere completate rapidamente.

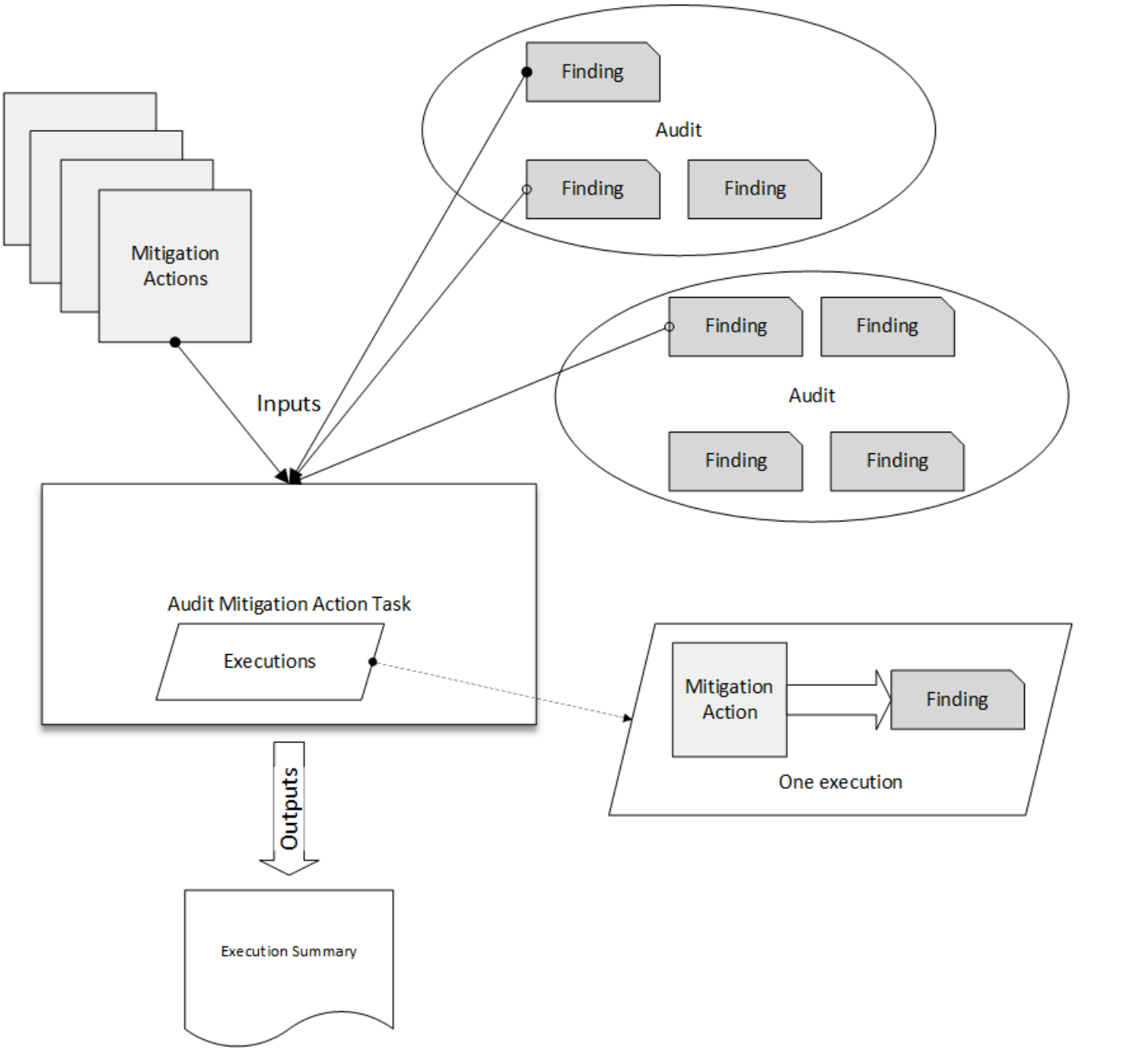
Puoi visualizzare l'elenco delle esecuzioni di operazioni e annullare un'esecuzione non ancora completata. Non viene effettuato il rollback delle operazioni già eseguite nell'ambito dell'esecuzione di operazioni annullata. Se stai applicando più operazioni a un set di risultati e una di tali operazioni non è riuscita, le operazioni successive vengono ignorate per quel risultato (ma vengono comunque applicate agli altri risultati). Lo stato attività per il risultato è FAILED. `taskStatus` è impostato su non riuscito se una o più operazioni hanno avuto esito negativo durante l'applicazione ai risultati. Le operazioni vengono applicate in base all'ordine in cui vengono definite.

Ogni esecuzione di operazioni applica un set di operazioni a un target. Questo target può essere un elenco di risultati oppure tutti i risultati di un audit.

Il seguente diagramma mostra come definire un'attività di mitigazione di audit che acquisisce tutti i risultati di un audit e applica un set di operazioni a tali risultati. Una singola esecuzione applica un'operazione a un risultato. L'output dell'attività di operazioni di mitigazione di audit è un riepilogo di esecuzione.



Il seguente diagramma mostra come definire un'attività di mitigazione di audit che acquisisce un elenco di singoli risultati da uno o più audit e applica un set di operazioni a tali risultati. Una singola esecuzione applica un'operazione a un risultato. L'output dell'attività di operazioni di mitigazione di audit è un riepilogo di esecuzione.



Puoi utilizzare la console AWS IoT o AWS CLI per applicare le operazioni di mitigazione.

Per utilizzare la console AWS IoT per applicare le operazioni di mitigazione avviando l'esecuzione di un'operazione

1. Apri la pagina Audit results (Risultati della revisione) nella console AWS IoT.
2. Scegliere il nome per l'audit a cui applicare le operazioni.

3. Scegli Start mitigation actions (Avvia operazioni di mitigazione). Questo pulsante non è disponibile se tutti i tuoi controlli sono conformi.
4. In Start a new mitigation action (Avvia una nuova operazione di mitigazione), il nome predefinito dell'attività è l'ID audit, ma è possibile modificarlo per usarne uno più significativo.
5. Per ogni tipo di controllo con uno o più risultati non conformi nell'audit, è possibile scegliere una o più operazioni da applicare. Vengono visualizzate solo le operazioni valide per il tipo di controllo.

   > **Note**
   >
   > Se non sono state configurate operazioni per il tuo Account AWS, l'elenco di operazioni sarà vuoto. Puoi scegliere il link Create mitigation action (Crea operazione di mitigazione) per creare una o più operazioni di mitigazione.

6. Una volta specificate tutte le operazioni da applicare, scegli Start task (Avvia attività).

Per utilizzare AWS CLI per applicare le operazioni di mitigazione avviando l'esecuzione di operazioni di mitigazione di audit

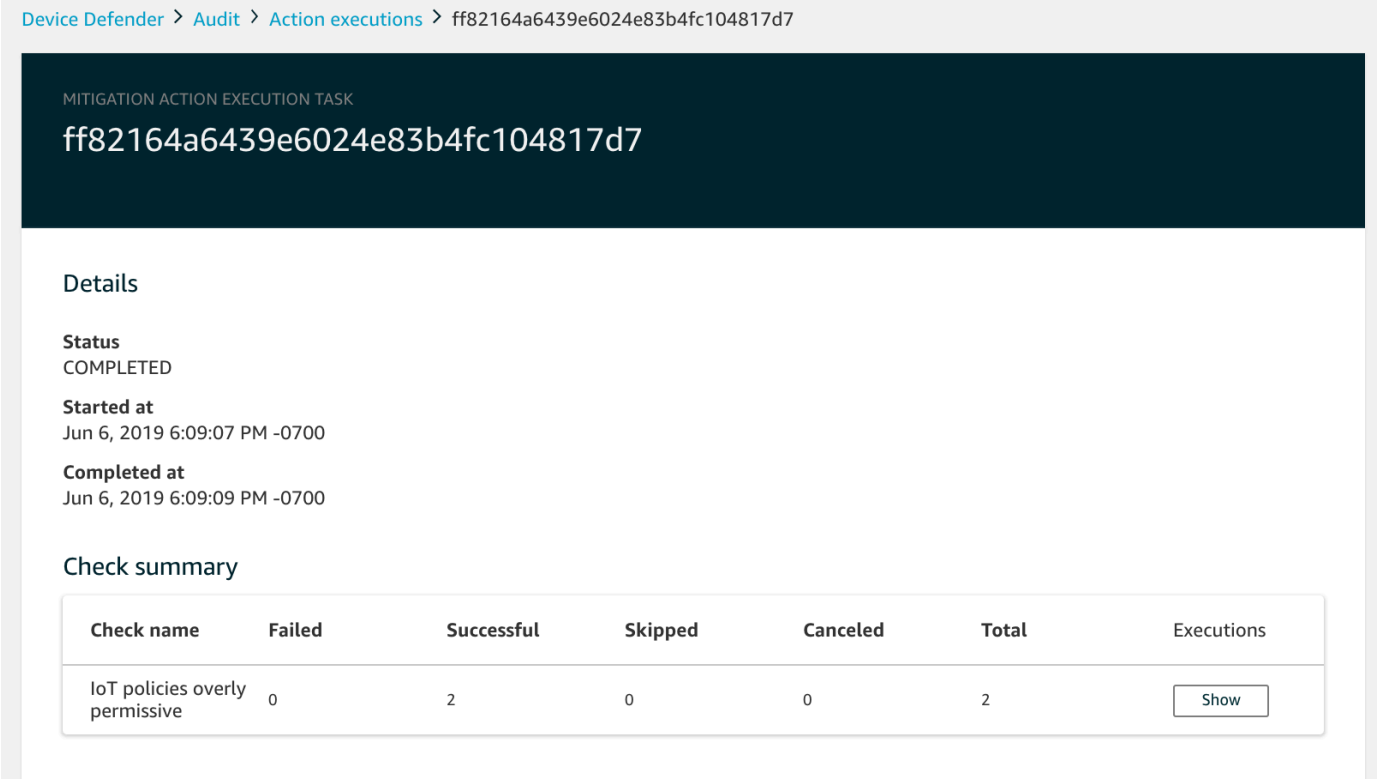
1. Per applicare le operazioni a tutti i risultati per l'audit, utilizza il comando ListAuditTasks per trovare l'ID attività.
2. Per applicare le operazioni solo a determinati risultati, utilizza il comando ListAuditFindings per ottenere gli ID risultato.
3. Utilizza il comando ListMitigationActions e annota i nomi delle operazioni di mitigazione da applicare.
4. Utilizza il comando StartAuditMitigationActionsTask per applicare le operazioni alla destinazione. Annotare l'ID attività. Questo ID consente di controllare lo stato dell'esecuzione dell'operazione, rivedere i dettagli o annullarla.

Per utilizzare la console AWS IoT per visualizzare le esecuzioni di operazioni

1. Apri la pagina Action tasks (Attività di operazione) nella console AWS IoT.

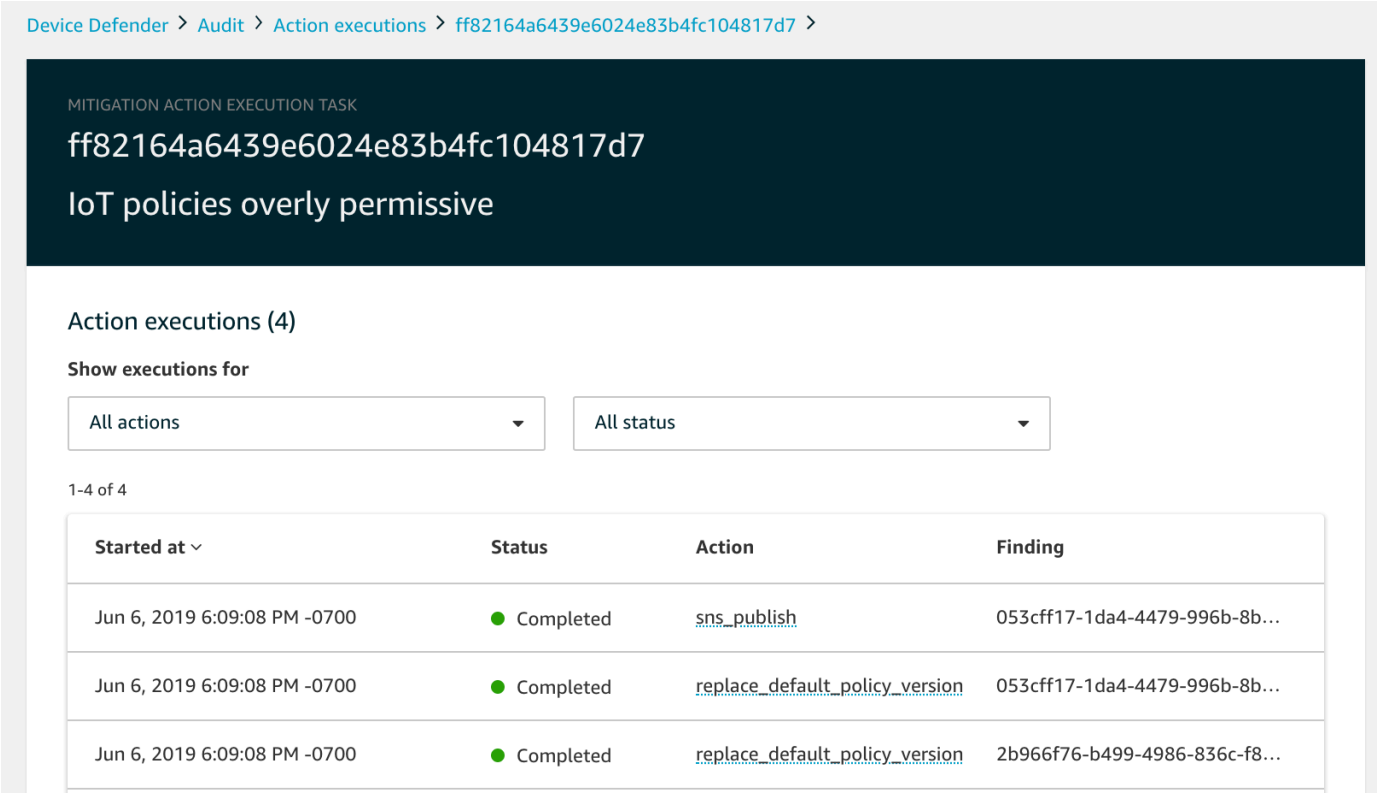
   Un elenco di attività delle operazioni mostra quando ognuna di esse è stata inviata e lo stato corrente.

2. Scegliere il link Name (Nome) per visualizzare i dettagli dell'attività. I dettagli includono tutte le operazioni applicate dall'attività, il relativo target e il relativo stato.



È possibile utilizzare i filtri Show executions for (Mostra esecuzioni per) per concentrarsi sui tipi di azioni o stati di azione.

3. Per visualizzare i dettagli dell'attività, in Executions (Esecuzioni), scegliere Show (Mostra).



Per utilizzare AWS CLI per elencare le attività avviate

1. Utilizza ListAuditMitigationActionsTasks per visualizzare le attività delle operazioni di mitigazione di audit. È possibile specificare filtri per restringere i risultati. Se si desidera visualizzare i dettagli dell'attività, prendere nota dell'ID attività.
2. Utilizza ListAuditMitigationActionsExecutions per visualizzare i dettagli di esecuzione per una determinata attività delle operazioni di mitigazione di audit.
3. Utilizza DescribeAuditMitigationActionsTask per visualizzare i dettagli dell'attività, ad esempio i parametri specificati quando è stata avviata.

Per utilizzare AWS CLI per annullare un'attività di operazioni di mitigazione di audit

1. Utilizza il comando ListAuditMitigationActionsTasks per trovare l'ID attività per l'attività di cui si vuole annullare l'esecuzione. È possibile specificare filtri per restringere i risultati.
2. Utilizza il comando ListDetectMitigationActionsExecutions, con l'ID attività, per annullare le attività delle operazioni di mitigazione di audit. Non è possibile annullare le attività già completate. Quando si annulla un'attività, le operazioni rimanenti non vengono applicate, ma non viene eseguito il rollback delle operazioni di mitigazione già applicate.

Autorizzazioni

Per ogni operazione di mitigazione definita dall'utente, è necessario specificare il ruolo utilizzato per applicare l'operazione.

Autorizzazioni per le operazioni di mitigazione

Tipo di operazione	Modello della policy di autorizzazione	

UPDATE_DEVICE_CERTIFICATE	{
	"Version":"2012-10-17",
	"Statement":[
	{
	"Effect":"Allow",
	"Action":[
	"iot:UpdateCertificate"
	],
	"Resource":[
	"*"
	]
	}
	]
	}	

UPDATE_CA_CERTIFICATE	{ "Version":"2012-10-17", "Statement":[{ "Effect":"Allow", "Action":[	

Tipo di operazione	Modello della policy di autorizzazione
	"iot:UpdateCACertificate"], "Resource": ["*"] }] }

ADD_THINGS_TO_THING_GROUP	{
	"Version":"2012-10-17",
	"Statement":[
	{
	"Effect":
	"Allow",
	"Action":[
	"iot:ListPrincipalThings",
	"iot:AddThingToThingGroup"
	],
	"Resource":
	[
	"*"
	]
	}
	]
	}

Tipo di operazione	Modello della policy di autorizzazione	

REPLACE_DEFAULT_POLICY_VERSION	{
	"Version":"2012-10-17",
	"Statement":[
	{
	"Effect":"Allow",
	"Action":[
	"iot:CreatePolicyVersion"
	],
	"Resource":[
	"*"
	]
	}
	]
	}	

Tipo di operazione	Modello della policy di autorizzazione	

ENABLE_IOT_LOGGING	{
	"Version":"2012-10-17",
	"Statement":[
	{
	"Effect": "Allow",
	"Action":[
	"iot:SetV2LoggingOptions"
	],
	"Resource": [
	"*"
	]
	},
	{
	"Effect": "Allow",
	"Action":[
	"iam:PassRole"
	],
	"Resource": [
	"*<IAM role ARN used for setting up logging>*"
	]
	}
	]
	}	

Tipo di operazione	Modello della policy di autorizzazione	

PUBLISH_FINDING_TO_SNS	{
	"Version":"2012-10-17",
	"Statement":[
	{
	"Effect": "Allow",
	"Action":[
	"sns:Publish"
	],
	"Resource": [
	"<The SNS topic to which the finding is published> "
	]
	}
	]
	}	

Per tutti i tipi di operazioni di mitigazione, utilizzare il seguente modello di policy di trust:


```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "iot.amazonaws.com"
      },
      "Action": "sts:AssumeRole",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:iot:*:111122223333::*"
        },
```

```
        "StringEquals": {
          "aws:SourceAccount": "111122223333:"
        }
      }
    }
  ]
}
```

Comandi delle operazioni di mitigazione

È possibile utilizzare questi comandi delle operazioni di mitigazione per definire un set di operazioni per il tuo Account AWS, da applicare in seguito a uno o più set di risultati di audit. Sono disponibili tre categorie di comandi:

- Comandi utilizzati per definire e gestire le operazioni.
- Comandi utilizzati per avviare e gestire l'applicazione di tali operazioni ai risultati di audit.
- Comandi utilizzati per avviare e gestire l'applicazione di tali operazioni a Detect allarmi.

Comandi delle operazioni di mitigazione

Definire e gestire le operazioni	Avviare e gestire l'esecuzione dell'audit	Avviare e gestire l'esecuzione di Detect
CreateMitigationAction	CancelAuditMitigationActionsTask	CancelDetectMitigationActionsTask
DeleteMitigationAction	DescribeAuditMitigationActionsTask	DescribeDetectMitigationActionsTask
DescribeMitigationAction	ListAuditMitigationActionsTasks	ListDetectMitigationActionsTasks
ListMitigationActions	StartAuditMitigationActionsTask	StartDetectMitigationActionsTask
UpdateMitigationAction	ListAuditMitigationActionsExecutions	ListDetectMitigationActionsExecutions

Uso di AWS IoT Device Defender con altri servizi AWS

Utilizzo di AWS IoT Device Defender con dispositivi in esecuzione AWS IoT Greengrass

AWS IoT Greengrass fornisce l'integrazione predefinita con AWS IoT Device Defender per monitorare i comportamenti dei dispositivi su base continuativa.

- Integrazione di Device Defender con AWS IoT Greengrass V1
- Integrazione di Device Defender con AWS IoT Greengrass V2

Utilizzo di AWS IoT Device Defender con FreeRTOS e dispositivi incorporati

Per utilizzare AWS IoT Device Defender su un dispositivo FreeRTOS, il dispositivo deve avere installati l'SDK for Embedded C per FreeRTOS o la libreria di AWS IoT Device Defender. Il FreeRTOS Embedded C SDK include la libreria AWS IoT Device Defender. Per informazioni su come integrare AWS IoT Device Defender con i tuoi dispositivi FreeRTOS, vedi le seguenti demo:

- AWS IoT Device Defender per le demo dei parametri standard e dei parametri personalizzati di FreeRTOS
- Utilizzo dell'agente MQTT per inviare i parametri a AWS IoT Device Defender
- Utilizzo della libreria principale MQTT per inviare i parametri a AWS IoT Device Defender

Per utilizzare AWS IoT Device Defender su un dispositivo incorporato senza FreeRTOS, il dispositivo deve avere l'SDK AWS IoT Embedded C o la libreria AWS IoT Device Defender. L'AWS IoT Embedded C SDK include la libreria AWS IoT Device Defender. Per informazioni su come integrare AWS IoT Device Defender con i tuoi dispositivi incorporati, consulta le seguenti demo, AWS IoT Device Defender per demo dei parametri standard e personalizzati di AWS IoT Embedded SDK).

Uso di AWS IoT Device Defender con AWS IoT Device Management

È possibile utilizzare l'indicizzazione del parco istanze di AWS IoT Device Management per indicizzare, ricercare e aggregare le violazioni identificate da AWS IoT Device Defender. Dopo che i dati delle violazioni di Device Defender sono stati indicizzati in nell'indicizzazione del parco istanze, puoi accedere ed effettuare query sui dati delle violazioni di Device Defender dalle applicazioni Fleet Hub, creare allarmi del parco istanze basati sui dati delle violazioni per monitorare le anomalie nella tua flotta di dispositivi, e visualizzare gli allarmi de lparco istanze nelle dashboard di Fleet Hub.

> **Note**
>
> La funzione di indicizzazione del parco istanze per supportare l'indicizzazione di dati delle violazioni AWS IoT Device Defender è in versione di anteprima per AWS IoT Device Management ed è soggetta a modifiche.

- Gestione dell'indicizzazione del parco istanze
- Sintassi delle query
- Gestione dell'indicizzazione del parco istanze per le applicazioni Fleet Hub
- Nozioni di base

Integrazione con AWS Security Hub

AWS Security Hub fornisce una visione completa dello stato di sicurezza in AWS e ti aiuta a controllare l'ambiente rispetto agli standard di sicurezza del settore e alle best practice. Security Hub raccoglie i dati di sicurezza da Account AWS, servizi e prodotti di terze parti supportati. È possibile utilizzare Security Hub per analizzare le tendenze di sicurezza e identificare i problemi di sicurezza più urgenti.

Grazie all'integrazione AWS IoT Device Defender con Security Hub, è possibile inviare i risultati da AWS IoT Device Defender a Security Hub. Security Hub include tali risultati nella sua analisi della posizione di sicurezza.

Indice

- Abilitazione e configurazione dell'integrazione

Abilitazione e configurazione dell'integrazione

Prima di integrare AWS IoT Device Defender con Security Hub, è necessario abilitare Security Hub. Per informazioni su come abilitare Security Hub, consulta la sezione relativa alla configurazione di Security Hub nella Guida per l'utente di AWS Security Hub.

Dopo aver abilitato AWS IoT Device Defender e Security Hub, aprire la pagina relativa alla integrazioni nella console di Security Hub, quindi scegliere Accept findings (Accetta i risultati) per Audit, Detect o entrambi. AWS IoT Device Defender inizia a inviare i risultati a Security Hub.

In che modo AWS IoT Device Defender invia gli esiti alla Centrale di sicurezza

In Security Hub, i problemi di sicurezza vengono monitorati come risultati. Alcuni risultati provengono da problemi rilevati da altri servizi AWS o da prodotti di terze parti.

Security Hub fornisce strumenti per gestire i risultati da tutte queste fonti. È possibile visualizzare e filtrare gli elenchi di risultati e visualizzare i dettagli per un riscontro. Per ulteriori informazioni, consulta Visualizzazione dei riscontri nella Guida per l'utenteAWS Security Hub. È inoltre possibile monitorare lo stato di un'indagine in un esito. Per ulteriori informazioni, consulta Azioni sugli esiti nella Guida per l'utente di AWS Security Hub.

Tutti i risultati in Security Hub utilizzano un formato JSON standard denominato AWS Security Finding Format (ASFF). L'ASFF include dettagli sull'origine del problema, sulle risorse interessate e sullo stato corrente del risultato. Per ulteriori informazioni su ASFF, consulta AWS Security Finding Format (ASFF) in Guida per l'utente di AWS Security Hub.

AWS IoT Device Defender è uno dei servizi AWS che invia i risultati a Security Hub.

Tipi di risultati che AWS IoT Device Defender invia

Dopo aver abilitato l'integrazione di Security Hub, AWS IoT Device Defender Audit invia i risultati generati (chiamati riepiloghi del controllo) a Security Hub. I riepiloghi del controllo sono informazioni generali per un tipo di controllo di auditing specifico e un'attività di auditing specifica. Per ulteriori informazioni, consulta Controlli di auditing.

AWS IoT Device Defender Audit invia gli aggiornamenti dei risultati a Security Hub per i riepiloghi del controllo di auditing e per i risultati di audit in ogni attività di auditing. Se tutte le risorse trovate nei controlli di auditing sono conformi o un'attività di auditing viene annullata, Audit aggiorna i riepiloghi del controllo in Security Hub in uno stato del record ARCHIVIATO. Se una risorsa è stata segnalata come non conforme per un controllo di audit, ma è stata segnalata come conforme nell'ultima attività di audit, viene modificata da Audit per renderla conforme e anche il risultato in Security Hub viene aggiornato in uno stato del record ARCHIVIATO.

AWS IoT Device Defender Detect invia i risultati di violazione a Security Hub. Questi risultati di violazione includono comportamenti machine learning (ML), statistico e statico.

Per inviare i risultati a Securiy Hub, AWS IoT Device Defender utilizza AWS Security Finding Format (ASFF). In ASFF, il `Types` campo fornisce il tipo di esito. I risultati ottenuti da AWS IoT Device Defender possono avere i seguenti valori per `Types`.

Comportamenti insoliti

Il tipo di risultato per ID client MQTT in conflitto e controlli condivisi dei certificati dei dispositivi e il tipo di risultato per Detect.

Controllo del software e della configurazione/vulnerabilità

Il tipo di risultato per tutti gli altri controlli di audit.

Latenza per l'invio degli esiti

Quando AWS IoT Device Defender Audit crea un nuovo risultato, viene inviato immediatamente a Security Hub al termine dell'attività di audit. La latenza dipende dal volume dei risultati generati nell'attività di audit. Security Hub riceve in genere i risultati entro un'ora.

AWS IoT Device Defender Detect invia i risultati delle violazioni quasi in tempo reale. Dopo che una violazione attiva o disattiva l'allarme (ovvero l'allarme viene creato o eliminato), il risultato Security Hub corrispondente viene immediatamente creato o archiviato.

Riprova quando Security Hub non è disponibile

Se Security Hub non è disponibile, AWS IoT Device Defender Audit e AWS IoT Device Defender Detect tentano di inviare i risultati finché non vengono ricevuti.

Aggiornamento degli esiti esistenti nella Centrale di sicurezza

Dopo che un risultato AWS IoT Device Defender Audit viene inviato a Security Hub, può essere identificato tramite l'identificatore della risorsa controllata e il tipo di controllo di audit. Se un nuovo risultato di audit viene generato con una successiva attività di audit per la stessa risorsa e controllo di audit, AWS IoT Device Defender Audit invia a Security Hub aggiornamenti per riportare osservazioni aggiuntive dell'attività del risultato in Security Hub. Se non viene generato alcun risultato di audit aggiuntivo con un'attività di audit successiva per la stessa risorsa e controllo di audit, la risorsa cambia per la conformità con il controllo di audit. AWS IoT Device Defender Audit archivia quindi i risultati in Security Hub.

AWS IoT Device Defender Audit aggiorna anche i riepiloghi del controllo in Security Hub. Se vengono rilevate risorse non conformi in un controllo di audit o il controllo non va a buon fine, lo stato del risultato di Security Hub diventa attivo. In caso contrario, AWS IoT Device Defender Audit archivia il risultato in Security Hub.

AWS IoT Device Defender Detect crea un risultato Security Hub che rileva quando c'è una violazione (ad esempio, in-alarm). Tale risultato viene aggiornato solo se viene soddisfatto uno dei criteri seguenti:

- Il risultato scadrà a breve in Security Hub, quindi AWS IoT Device Defender invia un aggiornamento per mantenere il risultato aggiornato. I risultati vengono eliminati 90 giorni dopo l'aggiornamento più recente o 90 giorni dopo la data di creazione se non viene eseguito un aggiornamento. Per ulteriori informazioni, consulta Quote di Security Hub nella Guida per l'utente di AWS Security Hub.
- La violazione corrispondente esce dall'allarme, pertanto AWS IoT Device Defender aggiorna il suo stato risultato su ARCHIVED.

Risultato tipico da AWS IoT Device Defender

AWS IoT Device Defender utilizza AWS Security Finding Format (ASFF) per inviare i risultati a Security Hub.

L'esempio seguente mostra un risultato tipico di Security Hub per un risultato di audit. `ReportType` in `ProductFields` è `AuditFinding`.


```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "336757784525/IOT_POLICY/policyexample/1/IOT_POLICY_OVERLY_PERMISSIVE_CHECK/
ALLOWS_BROAD_ACCESS_TO_IOT_DATA_PLANE_ACTIONS",
  "ProductArn": "arn:aws:securityhub:us-west-2::product/aws/iot-device-defender-audit",
  "ProductName": "IoT Device Defender - Audit",
  "CompanyName": "AWS",
  "Region": "us-west-2",
  "GeneratorId": "1928b87ab338ee2f541f6fab8c41c4f5",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Check/Vulnerabilities"
  ],
  "CreatedAt": "2022-11-06T22:11:40.941Z",
  "UpdatedAt": "2022-11-06T22:11:40.941Z",
  "Severity": {
    "Label": "CRITICAL",
    "Normalized": 90
  },
  "Title": "IOT_POLICY_OVERLY_PERMISSIVE_CHECK:
 ALLOWS_BROAD_ACCESS_TO_IOT_DATA_PLANE_ACTIONS",
  "Description": "IOT_POLICY policyexample:1 is reported as non-compliant for
 IOT_POLICY_OVERLY_PERMISSIVE_CHECK by Audit task 9f71b6e90cfb57d4ac671be3a4898e6a.
 The non-compliant reason is Policy allows broad access to IoT data plane actions:
 [iot:Connect].",
  "SourceUrl": "https://us-west-2.console.aws.amazon.com/iot/home?region=us-west-2#/
policy/policyexample",
  "ProductFields": {
    "CheckName": "IOT_POLICY_OVERLY_PERMISSIVE_CHECK",
    "TaskId": "9f71b6e90cfb57d4ac671be3a4898e6a",
    "TaskType": "ON_DEMAND_AUDIT_TASK",
    "PolicyName": "policyexample",
    "IsSuppressed": "false",
    "ReasonForNonComplianceCode": "ALLOWS_BROAD_ACCESS_TO_IOT_DATA_PLANE_ACTIONS",
    "ResourceType": "IOT_POLICY",
    "FindingId": "1928b87ab338ee2f541f6fab8c41c4f5",
    "PolicyVersionId": "1",
    "ReportType": "AuditFinding",
    "TaskStartTime": "1667772700554",
```

```
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-west-2::product/
aws/iot-device-defender-audit/336757784525/IOT_POLICY/policyexample/1/
IOT_POLICY_OVERLY_PERMISSIVE_CHECK/ALLOWS_BROAD_ACCESS_TO_IOT_DATA_PLANE_ACTIONS",
    "aws/securityhub/ProductName": "IoT Device Defender - Audit",
    "aws/securityhub/CompanyName": "AWS"
  },
  "Resources": [
    {
      "Type": "AwsIotPolicy",
      "Id": "policyexample",
      "Partition": "aws",
      "Region": "us-west-2",
      "Details": {
        "Other": {
          "PolicyVersionId": "1"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "CRITICAL"
    },
    "Types": [
      "Software and Configuration Check/Vulnerabilities"
    ]
  }
}
```

L'esempio seguente mostra un risultato di Security Hub per un riepilogo del controllo di audit. `ReportType` in `ProductFields` è `CheckSummary`.

```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "615243839755/SCHEDULED_AUDIT_TASK/daily_audit_schedule_checks/
DEVICE_CERTIFICATE_KEY_QUALITY_CHECK",
```

```
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/iot-device-defender-audit",
  "ProductName": "IoT Device Defender - Audit",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "f3021945485adf92487c273558fcaa51",
  "AwsAccountId": "123456789012",
  "Types": [
    "Software and Configuration Check/Vulnerabilities/CVE"
  ],
  "CreatedAt": "2022-10-18T14:20:13.933Z",
  "UpdatedAt": "2022-10-18T14:20:13.933Z",
  "Severity": {
    "Label": "CRITICAL",
    "Normalized": 90
  },
  "Title": "DEVICE_CERTIFICATE_KEY_QUALITY_CHECK Summary: Completed with 2 non-
compliant resources",
  "Description": "Task f3021945485adf92487c273558fcaa51 of weekly scheduled Audit
 daily_audit_schedule_checks completes. 2 non-cimpliant resources are found for
 DEVICE_CERTIFICATE_KEY_QUALITY_CHECK out of 1000 resources in the account. The
 percentage of non-compliant resources is 0.2%.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/iot/home?region=us-east-1#/dd/
audit/results/f3021945485adf92487c273558fcaa51/DEVICE_CERTIFICATE_KEY_QUALITY_CHECK",
  "ProductFields": {
    "TaskId": "f3021945485adf92487c273558fcaa51",
    "TaskType": "SCHEDULED_AUDIT_TASK",
    "ScheduledAuditName": "daily_audit_schedule_checks",
    "CheckName": "DEVICE_CERTIFICATE_KEY_QUALITY_CHECK",
    "ReportType": "CheckSummary",
    "CheckRunStatus": "COMPLETED_NON_COMPLIANT",
    "NonComopliantResourcesCount": "2",
    "SuppressedNonCompliantResourcesCount": "1",
    "TotalResourcesCount": "1000",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/
iot-device-defender-audit/615243839755/SCHEDULED/daily_audit_schedule_checks/
DEVICE_CERTIFICATE_KEY_QUALITY_CHECK",
    "aws/securityhub/ProductName": "IoT Device Defender - Audit",
    "aws/securityhub/CompanyName": "AWS"
  },
  "Resources": [
    {
      "Type": "AwsIotAuditTask",
      "Id": "f3021945485adf92487c273558fcaa51",
      "Region": "us-east-1"
```

```
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
  "FindingProviderFields": {
    "Severity": {
      "Label": "CRITICAL"
    },
    "Types": [
      "Software and Configuration Check/Vulnerabilities/CVE"
    ]
  }
}
```

L'esempio seguente mostra un risultato tipico di Security Hub per una violazione AWS IoT Device Defender Detect.

```
  {
  "SchemaVersion": "2018-10-08",
  "Id": "e92a782593c6f5b1fc7cb6a443dc1a12",
  "ProductArn": "arn:aws:securityhub:us-east-1::product/aws/iot-device-defender-
detect",
  "ProductName": "IoT Device Defender - Detect",
  "CompanyName": "AWS",
  "Region": "us-east-1",
  "GeneratorId": "arn:aws:iot:us-east-1:123456789012:securityprofile/
MySecurityProfile",
  "AwsAccountId": "123456789012",
  "Types": [
    "Unusual Behaviors"
  ],
  "CreatedAt": "2022-11-09T22:45:00Z",
  "UpdatedAt": "2022-11-09T22:45:00Z",
  "Severity": {
    "Label": "MEDIUM",
    "Normalized": 40
  },
  "Title": "Registered thing MyThing is in alarm for STATIC behavior MyBehavior.",
```

```
  "Description": "Registered thing MyThing violates STATIC behavior MyBehavior of
 security profile MySecurityProfile. Violation was triggered because the device did not
 conform to aws:num-disconnects less-than 1.",
  "SourceUrl": "https://us-east-1.console.aws.amazon.com/iot/home?region=us-east-1#/dd/
securityProfile/MySecurityProfile?tab=violations",
  "ProductFields": {
    "ComparisonOperator": "less-than",
    "BehaviorName": "MyBehavior",
    "ViolationId": "e92a782593c6f5b1fc7cb6a443dc1a12",
    "ViolationStartTime": "1668033900000",
    "SuppressAlerts": "false",
    "ConsecutiveDatapointsToAlarm": "1",
    "ConsecutiveDatapointsToClear": "1",
    "DurationSeconds": "300",
    "Count": "1",
    "MetricName": "aws:num-disconnects",
    "BehaviorCriteriaType": "STATIC",
    "ThingName": "MyThing",
    "SecurityProfileName": "MySecurityProfile",
    "aws/securityhub/FindingId": "arn:aws:securityhub:us-east-1::product/aws/iot-
device-defender-detect/e92a782593c6f5b1fc7cb6a443dc1a12",
    "aws/securityhub/ProductName": "IoT Device Defender - Detect",
    "aws/securityhub/CompanyName": "AWS"
  },
  "Resources": [
    {
      "Type": "AwsIotRegisteredThing",
      "Id": "MyThing",
      "Region": "us-east-1",
      "Details": {
        "Other": {
          "SourceUrl": "https://us-east-1.console.aws.amazon.com/iot/home?region=us-
east-1#/thing/MyThing?tab=violations",
          "IsRegisteredThing": "true",
          "ThingArn": "arn:aws:iot:us-east-1:123456789012:thing/MyThing"
        }
      }
    }
  ],
  "WorkflowState": "NEW",
  "Workflow": {
    "Status": "NEW"
  },
  "RecordState": "ACTIVE",
```

```
  "FindingProviderFields": {
    "Severity": {
      "Label": "MEDIUM"
    },
    "Types": [
      "Unusual Behaviors"
    ]
  }
}
```

Impedire a AWS IoT Device Defender di inviare i risultati a Security Hub

Per interrompere l'invio dei risultati a Security Hub, puoi utilizzare la console o l'API di Security Hub.

Per ulteriori informazioni, consulta Disabilitazione e abilitazione del flusso di risultati di un'integrazione (Console) o Disabilitazione del flusso di risultati di un'integrazione (API Security Hub, AWS CLI) nella Guida per l'utente di AWS Security Hub.

Prevenzione del confused deputy tra servizi

Con "confused deputy" si intende un problema di sicurezza in cui un'entità che non dispone dell'autorizzazione per eseguire una certa operazione può costringere un'entità con più privilegi a eseguire tale operazione. In AWS, la rappresentazione cross-service può comportare il problema confused deputy. La rappresentazione tra servizi può verificarsi quando un servizio (il servizio chiamante) effettua una chiamata a un altro servizio (il servizio chiamato). Il servizio chiamante può essere manipolato in modo da utilizzarne le autorizzazioni per agire sulle risorse di un altro cliente, a cui normalmente non avrebbe accesso, tramite il servizio stesso. Per evitare ciò, AWS fornisce strumenti per poterti a proteggere i tuoi dati per tutti i servizi con entità di servizio a cui è stato concesso l'accesso alle risorse del tuo account.

Sono tre le risorse cui AWS IoT Device Defender accede da parte tua che possono essere interessate dal problema di sicurezza "deputy confused": esecuzione di verifiche, invio di notifiche SNS per violazioni del profilo di sicurezza ed esecuzione di operazioni di mitigazione. Per ciascuna di queste operazioni, i valori per `aws:SourceArn` devono essere i seguenti:

- Per le risorse trasmesse all'API UpdateAccountAuditConfiguration (attributi RoleArn e notificationTarget RoleArn), è necessario esaminare la policy della risorsa utilizzando `aws:SourceArn` come `arn:`*`arnPartition`*`:iot:`*`region`*`:`*`accountId`*`:.`

- Per le risorse trasmesse all'API CreateMitigationAction (l'attributo RoleArn), è necessario esaminare la policy della risorsa utilizzando `aws:SourceArn` come `arn:arnPartition:iot:region:accountId:mitigationaction/mitigationActionName`.
- Per le risorse trasmesse all'API CreateSecurityProfile (l'attributo alertTargets), è necessario esaminare la policy della risorsa utilizzando `aws:SourceArn` come `arn:arnPartition:iot:region:accountId:securityprofile/securityprofileName`.

Il modo più efficace per proteggersi dal problema "confused deputy" è quello di usare la chiave di contesto della condizione globale `aws:SourceArn` con l'ARN completo della risorsa. Se non si conosce l'ARN completo della risorsa o si scelgono più risorse, è necessario utilizzare la chiave di contesto della condizione globale `aws:SourceArn` con caratteri jolly (*) per le parti sconosciute dell'ARN. Ad esempio, `arn:aws:servicename:*:123456789012:*`.

L'esempio seguente mostra il modo in cui puoi utilizzare le chiavi di contesto delle condizioni globali `aws:SourceArn` e `aws:SourceAccount` in AWS IoT Device Defender per prevenire il problema "confused deputy".

```
 {
"Version": "2012-10-17",
"Statement": {
  "Sid": "ConfusedDeputyPreventionExamplePolicy",
  "Effect": "Allow",
  "Principal": {
    "Service": "iot.amazonaws.com"
  },
  "Action": "sts:AssumeRole",
  "Condition": {
    "ArnLike": {
      "aws:SourceArn": "arn:aws:iot:*:123456789012::*"
    },
    "StringEquals": {
      "aws:SourceAccount": "123456789012:"
    }
  }
}
}
```

Best practice per la sicurezza degli agenti dei dispositivi

Privilegio minimo

Al processo dell'agente devono venire concesse solo le autorizzazioni minime necessarie.

Meccanismi di base

- L'agente deve essere eseguito come utente non root.
- L'agente deve essere eseguito come utente dedicato, nel proprio gruppo.
- A utenti e gruppi devono essere concesse le autorizzazioni di sola lettura sulle risorse necessarie per raccogliere e trasmettere i parametri.
- Esempio: autorizzazione di sola lettura in /proc /sys per l'agente di esempio.
- Per un esempio di configurazione di un processo per l'esecuzione con autorizzazioni ridotte, consulta le istruzioni di configurazione incluse con l'agente di esempio Python.

Sono disponibili diversi meccanismi Linux noti che possono aiutare a limitare/isolare ulteriormente il processo dell'agente:

Meccanismi avanzati

- CGroups
- SELinux
- Chroot
- Spazi dei nomi Linux

Resilienza operativa

Il processo di un agente deve essere resiliente alle eccezioni e agli errori operativi imprevisti e non deve arrestarsi in modo anomalo o chiudersi definitivamente. Il codice deve gestire nel modo appropriato le eccezioni e, come precauzione, deve essere configurato per il riavvio automatico in caso di interruzione imprevista (ad esempio, a causa del riavvio del sistema o di eccezioni non intercettate).

Dipendenze minime

Un agente deve usare il minor numero possibile di dipendenze (ad esempio librerie di terze parti) nella sua implementazione. Se l'uso di una libreria è giustificato dalla complessità di un'attività (ad esempio, Transport Layer Security), usa solo dipendenze ben gestite e stabilisci un meccanismo per mantenerle aggiornate. Se le dipendenze aggiunte contengono funzionalità non usate

dall'agente e attive per impostazione predefinita (ad esempio l'apertura di porte o i socket di dominio), disabilitale nel codice o attraverso i file di configurazione della libreria.

Isolamento dei processi

Il processo di un agente deve contenere solo le funzionalità necessarie per raccogliere e trasmettere i parametri dei dispositivi. Non deve usare altri processi di sistema come container o implementare funzionalità per altri casi d'uso non previsti. Il processo dell'agente non deve inoltre creare canali di comunicazione in entrata, ad esempio socket di dominio e porte di servizio di rete, che potrebbero permettere a processi locali o remoti di interferire con il funzionamento e influire sull'integrità e sull'isolamento.

Segretezza

Il nome del processo di un agente non deve contenere parole chiave come sicurezza, monitoraggio o audit che ne indicano lo scopo e l'importanza per la sicurezza. È preferibile usare nomi in codice generici o nomi di processi casuali univoci per ogni dispositivo. Lo stesso principio deve essere seguito nell'assegnazione del nome della directory in cui si trovano i file binari dell'agente e di eventuali nomi e valori degli argomenti del processo.

Condivisione di informazioni minime

Qualsiasi elemento di un agente distribuito nei dispositivi non deve contenere informazioni sensibili, ad esempio credenziali con privilegi, codice di debug o codice non utilizzato oppure commenti in linea o file di documentazione che rivelino dettagli sull'elaborazione lato server dei parametri raccolti dall'agente o altri dettagli sui sistemi back-end.

Transport Layer Security

Per stabilire canali TLS sicuri per la trasmissione dei dati, un processo dell'agente deve applicare tutte le convalide lato client, ad esempio la convalida della catena di certificati e del nome di dominio, a livello di applicazione, se questa opzione non è abilitata per impostazione predefinita. Un agente deve inoltre usare un archivio di certificati root contenente autorità attendibili e che non contiene certificati appartenenti a emittenti di certificati compromessi.

Distribuzione sicura

Tutti i meccanismi di distribuzione dell'agente, ad esempio la sincronizzazione o il push di codice e i repository contenenti i dati binari, il codice sorgente e i file di configurazione (inclusi i certificati root attendibili), devono essere controllati per impedire l'inserimento di codice non autorizzato o la manomissione. Se il meccanismo di distribuzione si basa sulla comunicazione di rete, è necessario usare metodi di crittografia per proteggere l'integrità degli elementi di distribuzione in transito.

Approfondimenti

- Sicurezza in AWS IoT Device Defender
- Informazioni sul Modello di sicurezza AWS IoT
- Redhat: presentazione di Python
- 10 problemi di sicurezza comuni in Python e come evitarli
- Informazioni sui privilegi minimi e sulla loro utilità
- 10 indicazioni sulla sicurezza integrata di OWASP
- Progetto IoT OWASP

Risoluzione dei problemi di AWS IoT Device Defender

Aiutaci a migliorare questo argomento

Facci sapere che cosa contribuirebbe a migliorarlo

Generali

D: Sono previsti prerequisiti per l'uso di AWS IoT Device Defender?

R: se si desidera utilizzare parametri riportati sul dispositivo, è necessario distribuire un agente sul dispositivo o il gateway di dispositivi AWS IoT connessi. I dispositivi devono fornire un identificatore client coerente o un nome dell'oggetto.

Audit

D: Ho abilitato un controllo e lo stato dell'audit è rimasto "In corso" per molto tempo. C'è qualcosa che non funziona? Quando posso aspettarmi i risultati?

R: Quando un controllo viene abilitato, la raccolta dei dati inizia immediatamente. Tuttavia, se il tuo account ha una grande quantità di dati da raccogliere (certificati, oggetti o policy), i risultati del controllo potrebbero non essere disponibili per qualche tempo dopo l'abilitazione.

Rilevamento

D: Come faccio a sapere le soglie da impostare in un comportamento del profilo di sicurezza AWS IoT Device Defender?

R: Inizia creando un comportamento del profilo di sicurezza con soglie basse e collegalo a un gruppo di oggetti che contiene un set di dispositivi rappresentativo. È possibile utilizzare AWS IoT Device Defender per visualizzare i parametri correnti e quindi modificare le soglie del comportamento del dispositivo per ottenere la corrispondenza al tuo caso d'uso.

D: Ho creato un comportamento, ma non attiva una violazione quando previsto. Come posso risolvere il problema?

R: Quando si definisce un comportamento, si specifica in cosa consista un comportamento normale da parte del dispositivo. Se, ad esempio, hai una telecamera di sicurezza che si connette

solo a un server centrale sulla porta TCP 8888, non è previsto che vengano stabilite altre connessioni. Per ricevere un avviso se la telecamera stabilisce una connessione su un'altra porta, puoi definire un comportamento, ad esempio:

```
{
  "name": "Listening TCP Ports",
  "metric": "aws:listening-tcp-ports",
  "criteria": {
    "comparisonOperator": "in-port-set",
    "value": {
      "ports": [ 8888 ]
    }
  }
}
```

Se la fotocamera invia una connessione TCP sulla porta TCP 443, il comportamento del dispositivo viene violato e viene attivato un avviso.

D: Uno o più dei comportamenti hanno provocato una violazione. Come posso cancellare la violazione?

R: Gli allarmi si disattivano quando il dispositivo torna al comportamento previsto, secondo quanto definito nei profili di comportamento. I profili di comportamento vengono valutati al momento della ricezione dei dati dei parametri per il dispositivo. Se il dispositivo non pubblica alcun parametro per più di due giorni, l'evento di violazione è impostato automaticamente su `alarm-invalidated`.

D: Ho eliminato un comportamento che provocava una violazione, come posso interrompere gli avvisi?

R: L'eliminazione di un comportamento interrompe tutte le violazioni future e gli avvisi relativi a tale comportamento. Gli avvisi precedenti devono essere eliminati dal tuo meccanismo di notifica. Quando, tuttavia, un comportamento viene eliminato, la registrazione delle violazioni per tale comportamento viene conservata per lo stesso periodo di tempo applicato ad altre violazioni nell'account.

Parametri dei dispositivi

D: Sto inviando segnalazioni di parametri che so che violano i miei comportamenti, ma non vengono attivate violazioni. Qual è il problema?

R: Controlla le segnalazioni di parametri vengano accettate sottoscrivendo gli argomenti MQTT seguenti:

```
$aws/things/THING_NAME/defender/metrics/FORMAT/rejected
$aws/things/THING_NAME/defender/metrics/FORMAT/accepted
```

`THING_NAME` è il nome dell'oggetto che segnala il parametro e `FORMAT` è "JSON" o "CBOR", a seconda del formato della segnalazione di parametri inviata dall'oggetto.

Dopo aver eseguito la sottoscrizione, dovresti ricevere messaggi su questi argomenti per ogni segnalazione di parametri inviata. Un messaggio `rejected` indica che si è verificato un problema durante l'analisi della segnalazione di parametri. Nel payload del messaggio è incluso un messaggio di errore utile per correggere eventuali errori nella segnalazione di parametri. Un messaggio `accepted` indica che la segnalazione di parametri è stata analizzata correttamente.

D: Cosa succede se invio un parametro vuoto nella segnalazione?

R: Un elenco vuoto di porte o indirizzi IP è sempre considerato conforme al comportamento corrispondente. Se il comportamento corrispondente risultava violato, la violazione verrà cancellata.

D: Perché i miei report sui parametri del dispositivo contengono messaggi per i dispositivi che non sono nel registro AWS IoT?

Se disponi di uno o più profili di sicurezza associati a tutti gli oggetti o a tutti gli oggetti non registrati, AWS IoT Device Defender include i parametri degli oggetti non registrati. Se si desidera escludere i parametri dagli oggetti non registrati, è possibile allegare i profili a tutti i dispositivi registrati invece che a tutti i dispositivi.

D: Non riesco a visualizzare i messaggi provenienti da uno o più dispositivi non registrati anche se viene applicato un profilo di sicurezza a tutti i dispositivi non registrati o a tutti i dispositivi. Come posso risolvere il problema?

Verifica che la segnalazione dei parametri che stai inviando sia formalmente corretta e si avvalga di uno dei formati supportati. Per informazioni, consulta Specifica del documento di parametri dei dispositivi. Verificare che i dispositivi non registrati utilizzino un identificatore client coerente o un

nome oggetto. I messaggi riferiti dai dispositivi vengono rifiutati se il nome dell'oggetto contiene caratteri di controllo oppure è più lungo di 128 byte di caratteri di codifica UTF-8.

D: Cosa succede se un dispositivo non registrato viene aggiunto al registro o un dispositivo registrato diventa non registrato?

R: Se un dispositivo viene aggiunto o rimosso dal registro:

- Puoi vedere due diverse violazioni per il dispositivo (una sotto il suo nome oggetto registrato, una sotto la propria identità non registrata), se continuerà a pubblicare i parametri per violazioni. Le violazioni attive per la vecchia identità non vengono più visualizzate dopo due giorni, ma sono disponibili nello storico delle violazioni per un massimo di 14 giorni.

D: Quale valore devo fornire nel campo ID della segnalazione dei parametri di un dispositivo?

R: Devi usare un valore univoco per ogni segnalazione di parametri, espresso come valore intero positivo. In genere è consigliabile usare un timestamp di epoca (Unix epoch).

D: È consigliabile creare una connessione MQTT dedicata per i parametri di AWS IoT Device Defender?

R: Non è necessaria una connessione MQTT separata.

D: Quale ID client devo usare per la connessione per la pubblicazione di parametri del dispositivo?

Per i dispositivi (oggetti) che si trovano nel registro AWS IoT, utilizzare il nome dell'oggetto registrato. Per i dispositivi che non sono presenti nel registro AWS IoT, utilizzare un identificatore coerente durante la connessione a AWS IoT. Questa pratica consente di abbinare le violazioni al nome dell'oggetto.

D: È possibile pubblicare parametri per un dispositivo con un ID client diverso?

È possibile pubblicare i parametri per conto di un altro oggetto. A tale scopo, è possibile pubblicare i parametri per l'argomento AWS IoT Device Defender riservato per quel dispositivo. Ad esempio, `Thing-1` vorrebbe pubblicare i parametri per sé e anche per conto di `Thing-2`. `Thing-1` raccoglie i propri parametri e li pubblica sull'argomento MQTT:

```
$aws/things/Thing-1/defender/metrics/json
```

`Thing-1` quindi ottiene i parametri da `Thing-2` e pubblica tali parametri nell'argomento MQTT:

```
$aws/things/Thing-2/defender/metrics/json
```

D: Quanti profili di sicurezza e comportamenti possono essere presenti nell'account?

R: Consulta Endpoint e quote AWS IoT Device Defender.

D: Cos'è un ruolo target prototipo per un target di avvisi?

R: Un ruolo che permette a AWS IoT Device Defender di pubblicare avvisi nel target (argomento SNS) richiede 2 elementi:

- Una relazione di trust che specifica iot.amazonaws.com come entità attendibile e
- Una policy collegata per la concessione dell'autorizzazione AWS IoT per pubblicare su un argomento SNS specifico. Ad esempio:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sns:Publish",
            "Resource": "<sns-topic-arn>"
        }
    ]
}
```

- Se l'argomento SNS utilizzato per la pubblicazione degli avvisi è un argomento crittografato, si devono concedere a AWS IoT l'autorizzazione per la pubblicazione sull'argomento SNS e altre due autorizzazioni. Ad esempio:

```
{
    "Version": "2012-10-17",
    "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "sns:Publish",
               "kms:Decrypt",
               "kms:GenerateDataKey"
           ],
           "Resource": "<sns-topic-arn>"
       }
    ]
}
```

D: L'invio della segnalazione dei parametri con un tipo di parametro personalizzato `number` fallisce con il messaggio di errore `Malformed metrics report`. Qual è il problema?

R: Il tipo `number` assume solo un singolo valore di parametro come input, ma durante l'invio del valore del parametro nel report DeviceMetrics deve essere trasmesso come array con un singolo valore. Assicurati di inviare il valore del parametro come array.

Errore di payload:

```
{"header":{"report_id":12334567,"version":"1.0"},"metrics":{"network_stats":
{"bytes_in":30680,"bytes_out":10652,"packets_in":113,"packets_out":118}},"custom_metrics":
{"my_custom_metric":{"number":0}}}
```

Messaggio di errore:

```
{"thingName":"myThing","status":"REJECTED","statusDetails":
{"ErrorCode":"InvalidPayload","ErrorMessage":"Malformed metrics
 report"},"timestamp":1635802047699}
```

Payload senza errori:

```
{"header":{"report_id":12334567,"version":"1.0"},"metrics":{"network_stats":
{"bytes_in":30680,"bytes_out":10652,"packets_in":113,"packets_out":118}},"custom_metrics":
{"my_custom_metric":[{"number":0}]}}
```

Risposta:

```
{"thingName":"myThing","12334567":1635800375,"status":"ACCEPTED","timestamp":1635801636023}
```

Sicurezza in AWS IoT Device Defender

Per AWS, la sicurezza del cloud ha la massima priorità. In quanto cliente AWS, puoi trarre vantaggio da un'architettura di data center e di rete progettata per soddisfare i requisiti delle aziende più esigenti a livello di sicurezza.

La sicurezza è una responsabilità condivisa tra AWSe l'utente. Il modello di responsabilità condivisa fa riferimento ad una sicurezza del cloud e nel cloud:

- Sicurezza del cloud: AWS è responsabile della protezione dell'infrastruttura che esegue i servizi AWS in Cloud AWS. AWS fornisce inoltre i servizi che è possibile utilizzare in modo sicuro. Revisori di terze parti testano regolarmente e verificano l'efficacia della nostra sicurezza nell'ambito dei Programmi di conformità AWS. Per informazioni sui programmi di conformità applicabili a AWS IoT Device Defender, consulta Servizi AWScoperti dal programma di conformità.
- Sicurezza nel cloud: la tua responsabilità è determinata dal servizio AWS 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 serve a facilitare la comprensione dell'applicazione del modello di responsabilità condivisa quando si utilizza l'AWS IoT Device Defender. I seguenti argomenti illustrano come configurare l'AWS IoT Device Defender per soddisfare gli obiettivi di sicurezza e conformità. Scoprirai anche come utilizzare altri servizi di AWS per monitorare e proteggere le risorse AWS IoT Device Defender. Per ulteriori informazioni sulla sicurezza in AWS IoT Core, consulta il capitolo sulla sicurezza nella Guida per gli sviluppatori di AWS IoT Core

Argomenti

- Protezione dei dati in AWS IoT Device Defender
- Gestione delle identità e degli accessi per l'AWS IoT Device Defender
- Convalida della conformità per AWS IoT Device Defender
- Resilienza in AWS IoT Device Defender

Protezione dei dati in AWS IoT Device Defender

Il modello di responsabilità condivisa di AWS si applica alla protezione dei dati in AWS IoT Device Defender. Come descritto in questo modello, AWS è responsabile della protezione dell'infrastruttura

globale che esegue tutto l'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 AWSe GDPR nel Blog sulla sicurezza AWS.

Per garantire la protezione dei dati, ti suggeriamo di proteggere le credenziali Account AWSe di configurare i singoli utenti con AWS IAM Identity Centero 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.
- Utilizza SSL/TLS per comunicare con le risorse AWS. È richiesto TLS 1.2 ed è consigliato TLS 1.3.
- Configura l'API e la registrazione delle attività degli utenti con AWS CloudTrail.
- Utilizza le soluzioni di crittografia AWS, insieme a tutti i controlli di sicurezza di default all'interno dei 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 necessiti di moduli crittografici convalidati FIPS 140-3 quando accedi ad AWS attraverso un'interfaccia a riga di comando o un'API, utilizza un endpoint FIPS. Per ulteriori informazioni sugli endpoint FIPS disponibili, consulta il Federal Information Processing Standard (FIPS) 140-3.

Ti consigliamo vivamente di non inserire mai informazioni riservate o sensibili, ad esempio gli indirizzi e-mail dei clienti, nei tag o nei campi di testo in formato libero, ad esempio nel campo Nome. Questo vale quanto utilizzi AWS IoT Device Defender o altri Servizi AWS con la console, l'API, la AWS CLI o gli SDK AWS. 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.

Gestione delle identità e degli accessi per l'AWS IoT Device Defender

AWS Identity and Access Management (IAM) è un Servizio AWSche consente agli amministratori di controllare in modo sicuro l'accesso alle risorse AWS. Gli amministratori IAM controllano chi può essere autenticato (ha effettuato l'accesso) e autorizzato (dispone di autorizzazioni) a utilizzare le risorse AWS IoT Device Defender. IAM è un Servizio AWS il cui uso non comporta costi aggiuntivi.

Argomenti

Destinatari

Le modalità di utilizzo di AWS Identity and Access Management (IAM) cambiano in base alle operazioni eseguite in AWS IoT Device Defender.

Utente del servizio: se utilizzi il servizio AWS IoT Device Defender per svolgere il tuo lavoro, l'amministratore ti fornisce le credenziali e le autorizzazioni necessarie. All'aumentare del numero di funzionalità AWS IoT Device Defender utilizzate per il lavoro, potrebbero essere necessarie ulteriori autorizzazioni. La comprensione della gestione dell'accesso ti consente di richiedere le autorizzazioni corrette all'amministratore. Se non riesci ad accedere a una funzionalità di AWS IoT Device Defender, consulta Risoluzione dei problemi di identità e accesso in AWS IoT Device Defender.

Amministratore del servizio: se sei il responsabile delle risorse di AWS IoT Device Defender della tua azienda, probabilmente disponi dell'accesso completo ad AWS IoT Device Defender. Il tuo compito è determinare le funzionalità e le risorse AWS IoT Device Defender a cui gli utenti del servizio devono accedere. 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 AWS IoT Device Defender, consulta Funzionamento di AWS IoT Device Defendercon IAM.

Amministratore IAM: un amministratore IAM potrebbe essere interessato a ottenere dei dettagli su come scrivere le policy per gestire l'accesso ad AWS IoT Device Defender. Per vedere le policy basate su identità di AWS IoT Device Defender di esempio che puoi utilizzare in IAM, consulta Esempi di policy basate su identità per AWS IoT Device Defender.

Autenticazione con identità

L'autenticazione è la procedura di accesso ad AWScon le credenziali di identità. Devi essere autenticato (connesso a AWS) come utente root Utente root dell'account AWS, come utente IAM o assumere un ruolo IAM.

Puoi accedere ad AWScome identità federata utilizzando le credenziali fornite attraverso un'origine di identità. AWS IAM Identity Center Gli esempi di identità federate comprendono gli utenti del centro identità IAM, l'autenticazione Single Sign-On (SSO) dell'azienda e le credenziali di Google o Facebook. Se accedi come identità federata, l'amministratore ha configurato in precedenza la federazione delle identità utilizzando i ruoli IAM. Se accedi ad AWStramite la federazione, assumi indirettamente un ruolo.

A seconda del tipo di utente, puoi accedere alla AWS Management Consoleo al portale di accesso AWS. Per ulteriori informazioni sull'accesso ad AWS, consulta la sezione Come accedere al tuo Account AWSnella Guida per l'utente di Accedi ad AWS.

Se accedi ad AWSin modo programmatico, AWSfornisce un Software Development Kit (SDK) e un'interfaccia della linea di comando (CLI) per firmare crittograficamente le richieste utilizzando le tue credenziali. Se non utilizzi gli strumenti AWS, devi firmare le richieste personalmente. Per ulteriori informazioni sulla firma delle richieste, consultare Firma delle richieste AWS nella Guida per l'utente IAM.

A prescindere dal metodo di autenticazione utilizzato, potrebbe essere necessario specificare ulteriori informazioni sulla sicurezza. AWS consiglia ad esempio di utilizzare l'autenticazione a più fattori (MFA) per aumentare la sicurezza dell'account. Per ulteriori informazioni, consulta Autenticazione a più fattori nella Guida per l'utente di AWS IAM Identity Centere Utilizzo dell'autenticazione a più fattori (MFA) in AWSnella Guida per l'utente IAM.

Utente root di un Account AWS

Quando crei un Account AWS, inizi con una singola identità di accesso che ha accesso completo a tutti i Servizi AWSe le risorse nell'account. Tale identità è detta utente root Account AWSed è possibile accedervi 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 best practice, richiedere agli utenti umani, compresi quelli che richiedono l'accesso di amministratore, di utilizzare la federazione con un provider di identità per accedere a Servizi AWSutilizzando credenziali temporanee.

Un'identità federata è un utente della directory degli utenti aziendali, un provider di identità Web, AWS Directory Service, la directory Identity Center o qualsiasi utente che accede ad Servizi AWSutilizzando le credenziali fornite tramite un'origine di identità. Quando le identità federate accedono a Account AWS, assumono ruoli e i ruoli forniscono credenziali temporanee.

Per la gestione centralizzata degli accessi, consigliamo di utilizzare AWS IAM Identity Center. È possibile creare utenti e gruppi in IAM Identity Center oppure connettersi e sincronizzarsi con un gruppo di utenti e gruppi nell'origine di identità per utilizzarli in tutte le applicazioni e gli 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 una identità all'interno del tuo Account AWSche 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, è possibile avere un gruppo denominato IAMAdmins e concedere a tale gruppo le autorizzazioni per amministrare le risorse IAM.

Gli utenti sono diversi dai ruoli. Un utente è associato in modo univoco a una persona o un'applicazione, mentre un ruolo è destinato a essere assunto da chiunque ne abbia bisogno. Gli

utenti dispongono di credenziali a lungo termine permanenti, mentre i ruoli forniscono credenziali temporanee. Per ulteriori informazioni, consulta Quando creare un utente IAM (invece di un ruolo) nella Guida per l'utente IAM.

Ruoli IAM

Un ruolo IAM è un'identità all'interno di Account AWSche dispone di autorizzazioni specifiche. È simile a un utente IAM, ma non è associato a una persona specifica. È possibile assumere temporaneamente un ruolo IAM nella AWS Management Consolemediante lo scambio di ruoli. È possibile assumere un ruolo chiamando un'operazione AWS CLIo API AWSoppure 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 Creazione di un ruolo per un provider di identità di terza parte 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, per alcuni dei Servizi AWS, è possibile collegare 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 multi-servizio: alcuni Servizi AWSutilizzano funzionalità che in altri Servizi AWS. Ad esempio, quando effettui una chiamata in un servizio, è comune che tale servizio esegua applicazioni in Amazon EC2 o archivi oggetti in Amazon S3. Un servizio può eseguire questa operazione utilizzando le autorizzazioni dell'entità chiamante, utilizzando un ruolo di servizio o utilizzando un ruolo collegato al servizio.

- Forward access sessions (FAS): quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'azione che attiva un'altra azione in un servizio diverso. La tecnologia FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con la richiesta di un Servizio AWS per effettuare richieste a servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che comporta interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Forward access sessions.
- Ruolo di servizio: un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire azioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella 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 ai servizi sono visualizzati nell'account Account AWSe 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: è possibile utilizzare un ruolo IAM per gestire credenziali temporanee per le applicazioni in esecuzione su un'istanza EC2 che eseguono richieste di AWS CLIo dell'API AWS. Ciò è preferibile all'archiviazione delle chiavi di accesso nell'istanza EC2. Per assegnare un ruolo AWSa un'istanza EC2, affinché sia disponibile per tutte le relative applicazioni, puoi creare un profilo dell'istanza collegato all'istanza. Un profilo dell'istanza contiene il ruolo e consente ai programmi in esecuzione sull'istanza EC2 di ottenere le credenziali temporanee. Per ulteriori informazioni, consulta Utilizzo di un ruolo IAM per concedere autorizzazioni ad applicazioni in esecuzione su istanze di Amazon EC2 nella Guida per l'utente IAM.

Per informazioni sull'utilizzo dei ruoli IAM, consulta Quando creare un ruolo IAM (invece di un utente) nella Guida per l'utente IAM.

Gestione dell'accesso con policy

Per controllare l'accesso a AWSè possibile creare policy e collegarle a identità o risorse AWS. Una policy è un oggetto in AWSche, quando associato a un'identità o a una risorsa, ne definisce le autorizzazioni. AWSvaluta queste policy quando un principale IAM (utente, utente root o sessione

ruolo) effettua una richiesta. Le autorizzazioni nelle policy determinano l'approvazione o il rifiuto della richiesta. La maggior parte delle policy viene archiviata in AWSsotto forma di 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 JSON AWS per specificare gli accessi ai diversi elementi. In altre parole, quale principale può eseguire azioni su quali risorse e in quali condizioni.

Per impostazione predefinita, utenti e ruoli non dispongono di autorizzazioni. Per concedere agli utenti l'autorizzazione a eseguire 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 dalla AWS Management Console, la AWS CLIo l'API AWS.

Policy basate su identità

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente 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 policy gestite sono policy autonome che possono essere collegate a più utenti, gruppi e ruoli in Account AWS. Le policy gestite includono le policy gestite da AWSe le policy gestite dal cliente. 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 su risorse

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali

condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Le policy basate sulle risorse sono policy inline che si trovano in tale servizio. Non è possibile utilizzare le policy gestite da AWSda IAM in una policy basata su risorse.

Liste di controllo degli accessi (ACL)

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate sulle risorse, sebbene non utilizzino il formato del documento di policy JSON.

Amazon S3, AWS WAFe Amazon VPC sono esempi di servizi che supportano le ACL. Per maggiori informazioni sulle ACL, consulta Panoramica delle liste di controllo degli accessi (ACL) nella Guida per gli sviluppatori di Amazon Simple Storage Service.

Altri tipi di policy

AWS supporta altri tipi di policy 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.
- Policy di controllo dei servizi (SCP): le SCP sono policy JSON che specificano il numero massimo di autorizzazioni per un'organizzazione o unità organizzativa (OU) in AWS Organizations. AWS Organizationsè un servizio per il raggruppamento e la gestione centralizzata degli Account AWSmultipli di proprietà dell'azienda. Se abiliti tutte le funzionalità in un'organizzazione, puoi applicare le policy di controllo dei servizi (SCP) a uno o tutti i tuoi account. La SCP limita le autorizzazioni per le entità negli account membri, compreso ogni Utente root dell'account AWS. Per ulteriori informazioni sulle SCP, consulta Policy di controllo dei servizi nella AWS OrganizationsGuida per l'utente di AWS Organizations.
- Policy di sessione: le policy di sessione sono policy avanzate che vengono trasmesse come parametro quando si crea in modo programmatico una sessione temporanea per un ruolo o un

utente federato. Le autorizzazioni della sessione risultante sono l'intersezione delle policy basate su identità del ruolo o dell'utente e le policy di sessione. Le autorizzazioni possono anche provenire da una policy basata su risorse. Un rifiuto esplicito in una qualsiasi di queste policy sostituisce l'autorizzazione. Per ulteriori informazioni, consulta Policy di sessione nella Guida per l'utente IAM.

Più tipi di policy

Quando più tipi di policy si applicano a una richiesta, le autorizzazioni risultanti sono più complicate da comprendere. Per informazioni su come AWSdetermina se consentire una richiesta quando sono coinvolti più tipi di policy, consultare Logica di valutazione delle policy nella Guida per l'utente di IAM.

Funzionamento di AWS IoT Device Defendercon IAM

Prima di utilizzare IAM per gestire l'accesso ad AWS IoT Device Defender, scopri quali funzionalità di IAM sono disponibili per l'uso con AWS IoT Device Defender.

Funzionalità IAM che è possibile utilizzare con AWS IoT Device Defender

Funzionalità IAM	Supporto di AWS IoT Device Defender
Policy basate su identità	Sì
Policy basate su risorse	No
Azioni di policy	Sì
Risorse relative alle policy	Sì
Chiavi di condizione delle policy	Sì
Liste di controllo degli accessi (ACL)	No
ABAC (tag nelle policy)	Parziale
Credenziali temporanee	Sì
Autorizzazioni del principale	Sì
Ruoli di servizio	Sì

Funzionalità IAM	Supporto di AWS IoT Device Defender
Ruoli collegati al servizio	No

Per ottenere un quadro generale del funzionamento di AWS IoT Device Defender e altri servizi AWS con la maggior parte delle caratteristiche di IAM, consulta Servizi AWS supportati da IAM nella Guida per l'utente IAM.

Policy basate su identità per AWS IoT Device Defender

Supporta le policy basate su identità: sì

Le policy basate su identità sono documenti di policy di autorizzazione JSON che è possibile allegare a un'identità (utente, gruppo di utenti o ruolo IAM). Tali policy definiscono le azioni che utenti e ruoli possono eseguire, su quali risorse e in quali condizioni. Per informazioni su come creare una policy basata su identità, consulta Creazione di policy IAM nella Guida per l'utente 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 su identità per AWS IoT Device Defender

Per vedere esempi di policy basate su identità di AWS IoT Device Defender, consulta Esempi di policy basate su identità per AWS IoT Device Defender.

Policy basate su risorse all'interno di AWS IoT Device Defender

Supporta le policy basate su risorse: no

Le policy basate su risorse sono documenti di policy JSON che è possibile collegare a una risorsa. Gli esempi più comuni di policy basate su risorse sono le policy di attendibilità dei ruoli IAM e le policy dei bucket Amazon S3. Nei servizi che supportano policy basate sulle risorse, gli amministratori dei servizi possono utilizzarli per controllare l'accesso a una risorsa specifica. Quando è collegata a una risorsa, una policy definisce le azioni che un principale può eseguire su tale risorsa e a quali

condizioni. È necessario specificare un principale in una policy basata sulle risorse. I principali possono includere account, utenti, ruoli, utenti federati o Servizi AWS.

Per consentire l'accesso multi-account, puoi specificare un intero account o entità IAM in un altro account come principale in una policy basata sulle risorse. L'aggiunta di un principale multi-account a una policy basata sulle risorse rappresenta solo una parte della relazione di trust. Quando l'entità principale e la risorsa si trovano in diversi Account AWS, un amministratore IAM nell'account attendibile deve concedere all'entità principale (utente o ruolo) anche l'autorizzazione per 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.

Operazioni di policy per AWS IoT Device Defender

Supporta le operazioni di policy: si

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Action`di una policy JSON descrive le azioni che è possibile utilizzare per consentire o negare l'accesso a un criterio. Le azioni di policy hanno spesso lo stesso nome dell'operazione API AWS. Ci sono alcune eccezioni, ad esempio le azioni di sola autorizzazione che non hanno un'operazione API corrispondente. Esistono anche alcune operazioni che richiedono più operazioni in una policy. Queste operazioni aggiuntive sono denominate operazioni dipendenti.

Includi le operazioni in una policy per concedere le autorizzazioni a eseguire l'operazione associata.

Per vedere un elenco di operazioni AWS IoT Device Defender, consulta Service Authorization Reference.

Le operazioni delle policy in AWS IoT Device Defender utilizzano il seguente prefisso prima dell'operazione:

```
```

Per specificare più operazioni in una sola istruzione, occorre separarle con la virgola.

```
"Action": [
      ":action1",
```

```
      ":action2"
         ]
```

Per vedere esempi di policy basate su identità di AWS IoT Device Defender, consulta Esempi di policy basate su identità per AWS IoT Device Defender.

Risorse relative alle policy per AWS IoT Device Defender

Supporta le risorse di policy: sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire operazioni su quali risorse, e in quali condizioni.

L'elemento JSON `Resource`della policy specifica l'oggetto o gli oggetti ai quali si applica l'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). Puoi eseguire questa operazione per azioni che supportano un tipo di risorsa specifico, note come autorizzazioni a livello di risorsa.

Per le azioni che non supportano le autorizzazioni a livello di risorsa, ad esempio le operazioni di elenco, utilizza un carattere jolly (*) per indicare che l'istruzione si applica a tutte le risorse.

```
"Resource": "*"
```

Per vedere un elenco di tipi di risorse AWS IoT Device Defender e i relativi ARN, consulta Service Authorization Reference. Per informazioni sulle operazioni con cui è possibile specificare l'ARN di ogni risorsa, consulta .

Per vedere esempi di policy basate su identità di AWS IoT Device Defender, consulta Esempi di policy basate su identità per AWS IoT Device Defender.

Chiavi di condizione delle policy per AWS IoT Device Defender

Supporta le chiavi di condizione delle policy specifiche del servizio: sì

Gli amministratori possono utilizzare le policy JSON AWS per specificare gli accessi ai diversi elementi. Cioè, quale principale può eseguire azioni su quali risorse, e in quali condizioni.

L'elemento `Condition`(o blocco `Condition`) consente di specificare le condizioni in cui un'istruzione è in vigore. L'elemento `Condition`è facoltativo. Puoi compilare espressioni condizionali che utilizzano operatori di condizione, ad esempio uguale a o minore di, per soddisfare la condizione nella policy con i valori nella richiesta.

Se specifichi più elementi `Condition`in un'istruzione o più chiavi in un singolo elemento `Condition`, questi vengono valutati da AWSutilizzando un'operazione `AND`logica. Se specifichi più valori per una singola chiave di condizione, AWSvaluta la condizione utilizzando un'operazione `OR`logica. Tutte le condizioni devono essere soddisfatte prima che le autorizzazioni dell'istruzione vengano concesse.

Puoi anche utilizzare variabili segnaposto quando specifichi le condizioni. Ad esempio, puoi autorizzare un utente IAM ad accedere a una risorsa solo se è stata taggata con il relativo nome utente IAM. Per ulteriori informazioni, consulta Elementi delle policy IAM: variabili e tag nella Guida per l'utente di IAM.

AWS supporta chiavi di condizione globali e chiavi di condizione specifiche per il servizio. Per visualizzare tutte le chiavi di condizione globali di AWS, consulta Chiavi di contesto delle condizioni globali di AWS nella Guida per l'utente di IAM.

Per vedere un elenco di chiavi di condizione AWS IoT Device Defender, consulta Service Authorization Reference. Per informazioni su operazioni e risorse con cui è possibile utilizzare una chiave di condizione, consulta .

Per vedere esempi di policy basate su identità di AWS IoT Device Defender, consulta Esempi di policy basate su identità per AWS IoT Device Defender.

Liste di controllo degli accessi in AWS IoT Device Defender

Supporta le ACL: no

Le liste di controllo degli accessi (ACL) controllano quali principali (membri, utenti o ruoli dell'account) hanno le autorizzazioni per accedere a una risorsa. Le ACL sono simili alle policy basate su risorse, sebbene non utilizzino il formato del documento di policy JSON.

ABAC con AWS IoT Device Defender

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, tali attributi sono denominati tag. È possibile collegare

dei tag alle entità IAM (utenti o ruoli) e a numerose risorse AWS. L'assegnazione di tag alle entità e alle risorse è il primo passaggio di ABAC. In seguito, vengono progettate policy ABAC per consentire operazioni quando il tag dell'entità principale corrisponde al tag sulla risorsa a cui si sta provando ad accedere.

La strategia ABAC è utile in ambienti soggetti a una rapida crescita e aiuta in situazioni in cui la gestione delle policy diventa impegnativa.

Per controllare l'accesso basato su tag, fornisci informazioni sui tag nell'elemento condizione di una policy utilizzando le chiavi di condizione `aws:ResourceTag/key-name`, `aws:RequestTag/key-name`o `aws:TagKeys`.

Se un servizio supporta tutte e tre le chiavi di condizione per ogni tipo di risorsa, il valore per il servizio è Yes (Sì). Se un servizio supporta tutte e tre le chiavi di condizione solo per alcuni tipi di risorsa, allora il valore sarà Parziale.

Per ulteriori informazioni su ABAC, consulta Che cos'è ABAC? nella Guida per l'utente 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 AWS IoT Device Defender

Supporta le credenziali temporanee: sì

Alcuni Servizi AWSnon funzionano quando si accede utilizzando credenziali temporanee. Per ulteriori informazioni, inclusi i Servizi AWSche funzionano con le credenziali temporanee, consulta Servizi AWSsupportati da IAM nella Guida per l'utente IAM.

Le credenziali temporanee sono utilizzate se si accede alla AWS Management Consoleutilizzando qualsiasi metodo che non sia la combinazione di nome utente e password. Ad esempio, quando accedi alla AWSutilizzando il collegamento Single Sign-On (SSO) della tua azienda, tale processo crea in automatico credenziali temporanee. Le credenziali temporanee vengono create in automatico anche quando accedi alla console come utente e poi cambi ruolo. Per ulteriori informazioni sullo scambio dei ruoli, consulta Cambio di un ruolo (console) nella Guida per l'utente IAM.

È possibile creare manualmente credenziali temporanee utilizzando la AWS CLIo l'API AWS. È quindi possibile utilizzare tali credenziali temporanee per accedere ad AWS. AWSconsiglia di generare le credenziali temporanee dinamicamente anziché utilizzare chiavi di accesso a lungo termine. Per ulteriori informazioni, consulta Credenziali di sicurezza provvisorie in IAM.

Autorizzazioni del principale tra servizi per AWS IoT Device Defender

Supporta l'inoltro delle sessioni di accesso (FAS): sì

Quando si utilizza un utente o un ruolo IAM per eseguire operazioni in AWS, si viene considerati un principale. Quando si utilizzano alcuni servizi, è possibile eseguire un'operazione che attiva un'altra operazione in un servizio diverso. La tecnologia FAS utilizza le autorizzazioni del principale che effettua la chiamata a un Servizio AWS, combinate con la richiesta di un Servizio AWS per effettuare richieste a servizi downstream. Le richieste FAS vengono effettuate solo quando un servizio riceve una richiesta che comporta interazioni con altri Servizi AWS o risorse per essere completata. In questo caso è necessario disporre delle autorizzazioni per eseguire entrambe le azioni. Per i dettagli delle policy relative alle richieste FAS, consulta la pagina Inoltro sessioni di accesso.

Ruoli di servizio per AWS IoT Device Defender

Supporta i ruoli di servizio: sì

Un ruolo di servizio è un ruolo IAM che un servizio assume per eseguire operazioni per tuo conto. Un amministratore IAM può creare, modificare ed eliminare un ruolo di servizio dall'interno di IAM. Per ulteriori informazioni, consulta la sezione Creazione di un ruolo per delegare le autorizzazioni a un Servizio AWSnella Guida per l'utente IAM.

> **Warning**
>
> La modifica delle autorizzazioni per un ruolo di servizio potrebbe compromettere la funzionalità di AWS IoT Device Defender. Modifica i ruoli di servizio solo quando AWS IoT Device Defender fornisce le indicazioni per farlo.

Ruoli collegati ai servizi per l'AWS IoT Device Defender

Supporta i ruoli collegati ai servizi: no

Un ruolo collegato ai servizi è un tipo di ruolo di servizio che è collegato a un Servizio AWS. Il servizio può assumere il ruolo per eseguire un'azione per tuo conto. I ruoli collegati ai servizi sono visualizzati nell'account Account AWSe sono di proprietà del servizio. Un amministratore IAM può visualizzare le autorizzazioni per i ruoli collegati ai servizi, ma non modificarle.

Per ulteriori informazioni su come creare e gestire i ruoli collegati ai servizi, consulta Servizi AWS supportati da 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 su identità per AWS IoT Device Defender

Per impostazione predefinita, gli utenti e i ruoli non dispongono dell'autorizzazione per creare o modificare le risorse AWS IoT Device Defender. Inoltre, non sono in grado di eseguire attività utilizzando la AWS Management Console, l'AWS Command Line Interface (AWS CLI) o l'API AWS. 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 nella Guida per l'utente di IAM.

Per informazioni dettagliate sulle operazioni e sui tipi di risorse definiti da AWS IoT Device Defender, incluso il formato degli ARN per ogni tipo di risorsa, consulta Actions, Resources, and Condition Keys for AWS IoT Device Defender in Service Authorization Reference.

Argomenti

- Best practice per le policy
- Utilizzo della console di AWS IoT Device Defender
- Consentire agli utenti di visualizzare le loro autorizzazioni

Best practice per le policy

Le policy basate su identità determinano se qualcuno può creare, accedere o eliminare risorse AWS IoT Device Defender 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:

- Nozioni di base sulle policy gestite da AWSe passaggio alle autorizzazioni con privilegio minimo: per le informazioni di base su come concedere autorizzazioni a utenti e carichi di lavoro, utilizza le policy gestite da AWSche concedono le autorizzazioni per molti casi d'uso comuni. Sono disponibili nel tuo Account AWS. Ti consigliamo pertanto di ridurre ulteriormente le autorizzazioni definendo policy gestite dal cliente di AWS specifiche per i tuoi casi d'uso. Per ulteriori informazioni, consulta Policy gestite da AWSo Policy gestite da AWSper 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. Puoi farlo definendo le azioni che possono essere intraprese su risorse specifiche in condizioni specifiche, note anche come autorizzazioni con privilegi minimi. Per ulteriori informazioni sull'utilizzo di IAM per applicare le autorizzazioni, consulta Policy e autorizzazioni in IAM nella Guida per l'utente IAM.
- Condizioni d'uso nelle policy IAM per limitare ulteriormente l'accesso: per limitare l'accesso a operazioni e risorse puoi aggiungere una condizione alle tue policy. Ad esempio, è possibile scrivere una condizione di policy per specificare che tutte le richieste devono essere inviate utilizzando SSL. Puoi inoltre utilizzare le condizioni per concedere l'accesso alle operazioni di servizio, ma solo 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 IAM Access Analyzer nella Guida per l'utente IAM.
- Richiesta dell'autenticazione a più fattori (MFA): se hai uno scenario che richiede utenti IAM o utenti root nel tuo Account AWS, attiva MFA per una maggiore sicurezza. Per richiedere la MFA quando vengono chiamate le operazioni API, aggiungi le condizioni MFA alle policy. Per ulteriori informazioni, consulta Configurazione dell'accesso alle API protetto con MFA nella Guida per l'utente 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 di AWS IoT Device Defender

Per accedere alla console AWS IoT Device Defender, è necessario disporre di un set di autorizzazioni minimo. Queste autorizzazioni devono consentirti di elencare e visualizzare i dettagli relativi alle risorse AWS IoT Device Defender nell'account 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 concedere le autorizzazioni minime della console agli utenti che effettuano chiamate solo alla AWS CLI o all'API AWS. Al contrario, concedi l'accesso solo alle operazioni che corrispondono all'operazione API che stanno cercando di eseguire.

Per assicurarti che gli utenti e i ruoli possano continuare a utilizzare la console AWS IoT Device Defender, collega alle entità anche la policy gestita da AWS IoT Device Defender *ConsoleAccess* o *ReadOnly* AWS. 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 operazione sulla console o a livello di codice utilizzando AWS CLI o l'API 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": "*"
        }
```

```
    ]
}
```

Risoluzione dei problemi di identità e accesso in AWS IoT Device Defender

Usa le informazioni seguenti per diagnosticare e risolvere i problemi comuni che possono verificarsi durante l'utilizzo di AWS IoT Device Defender e IAM.

Argomenti

- Non sono autorizzato a eseguire un'operazione in AWS IoT Device Defender
- Non sono autorizzato a eseguire iam:PassRole
- Voglio consentire alle persone esterne al mio account Account AWSdi accedere alle mie risorse AWS IoT Device Defender

Non sono autorizzato a eseguire un'operazione in AWS IoT Device Defender

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 `:`*`GetWidget`* fittizie.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: :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 `:`*`GetWidget`*.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Non sono autorizzato a eseguire iam:PassRole

Se ricevi un errore che indica che non sei autorizzato a eseguire l'operazione `iam:PassRole`, le tue policy devono essere aggiornate per poter passare un ruolo a AWS IoT Device Defender.

Alcuni Servizi AWSconsentono di trasmettere un ruolo esistente a tale servizio, invece di creare un nuovo ruolo di servizio o un ruolo collegato ai servizi. Per eseguire questa operazione, è necessario disporre delle autorizzazioni per trasmettere il ruolo al servizio.

L'errore di esempio seguente si verifica quando un utente IAM denominato `marymajor` cerca di utilizzare la console per eseguire un'operazione in AWS IoT Device Defender. 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`.

Per ulteriore assistenza con l'accesso, contatta l'amministratore AWS. L'amministratore è la persona che ti ha fornito le credenziali di accesso.

Voglio consentire alle persone esterne al mio account Account AWSdi accedere alle mie risorse AWS IoT Device Defender

È possibile creare un ruolo con il quale utenti in altri account o persone esterne all'organizzazione possono accedere alle tue risorse. È possibile specificare chi è attendibile per l'assunzione del ruolo. Per servizi che supportano policy basate su risorse o liste di controllo degli accessi (ACL), utilizza tali policy per concedere alle persone l'accesso alle tue risorse.

Per ulteriori informazioni, consulta gli argomenti seguenti:

- Per capire se AWS IoT Device Defender supporta queste funzionalità, consulta Funzionamento di AWS IoT Device Defendercon IAM.
- Per informazioni su come garantire l'accesso alle risorse negli Account AWSche possiedi, consulta Fornire l'accesso a un utente IAM in un altro Account AWSin tuo possesso nella Guida per l'utente IAM.
- Per informazioni su come fornire l'accesso alle risorse ad Account AWSdi terze parti, consulta Fornire l'accesso agli Account AWSdi 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.

Convalida della conformità per AWS IoT Device Defender

Per sapere se il Servizio AWSè coperto da programmi di conformità specifici, consulta i Servizi AWScoperti dal programma di conformità e scegli il programma di conformità desiderato. Per informazioni generali, consulta Programmi per la conformità di AWS.

È possibile scaricare i report di audit di terze parti utilizzando AWS Artifact. Per ulteriori informazioni, consulta Download di report in AWS Artifact.

La responsabilità di conformità durante l'utilizzo dei Servizi AWSè determinata dalla riservatezza dei dati, dagli obiettivi di conformità dell'azienda e dalle normative vigenti. Per semplificare il rispetto della conformità, AWSmette a disposizione le seguenti risorse:

- Guide Quick Start per la sicurezza e conformità: queste guide all'implementazione illustrano considerazioni relative all'architettura e forniscono la procedura per l'implementazione di ambienti di base su AWSincentrati sulla sicurezza e sulla conformità.
- Architetture per la sicurezza e la conformità HIPAA su Amazon Web Services: questo whitepaper descrive come le aziende possono utilizzare AWSper creare applicazioni conformi alla normativa HIPAA.

  > **Note**
  >
  > Non tutti i Servizi AWSsono conformi ai requisiti HIPAA. Per ulteriori informazioni, consulta la sezione Riferimenti sui servizi conformi ai requisiti HIPAA.

- Risorse per la conformità AWS: una raccolta di cartelle di lavoro e guide suddivise per settore e area geografica.
- AWSGuide alla conformità dei clienti: comprendi il modello di responsabilità condivisa attraverso la lente della conformità. Le guide riassumono le migliori pratiche per la protezione Servizi AWS e mappano le linee guida per i controlli di sicurezza su più framework (tra cui il National Institute of Standards and Technology (NIST), il Payment Card Industry Security Standards Council (PCI) e l'International Organization for Standardization (ISO)).

- Valutazione delle risorse con le regole nella Guida per gli sviluppatori di AWS Config: il servizio AWS Configvaluta il livello di conformità delle configurazioni delle risorse con pratiche interne, linee guida e regolamenti.
- AWS Security Hub: questo Servizio AWSfornisce una visione completa dello stato di sicurezza all'interno di AWS. La Centrale di sicurezza utilizza i controlli di sicurezza per valutare le risorse AWSe 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: questo Servizio AWS rileva potenziali minacce ad Account AWS, carichi di lavoro, container e dati monitorando l'ambiente alla ricerca di attività sospette e dannose. GuardDuty soddisfa i requisiti di rilevamento delle intrusioni imposti da determinati framework di conformità e garantisce il rispetto di vari standard come il PCI DSS.
- AWS Audit Manager: grazie a questo Servizio AWS esegui l'audit continuo dell'utilizzo di AWS, semplificando la gestione dei rischi e della conformità alle normative e agli standard di settore.

Resilienza in AWS IoT Device Defender

L'infrastruttura globale dei servizi AWS è progettata attorno a regioni Regioni AWS e zone di disponibilità. Le regioni di Regioni AWS forniscono più zone di disponibilità fisicamente separate e isolate che sono connesse tramite reti altamente ridondanti, a bassa latenza e a velocità di trasmissione effettiva elevata. Con le zone di disponibilità, puoi progettare e gestire applicazioni e database che eseguono automaticamente il failover tra zone di disponibilità senza interruzioni. Le zone di disponibilità sono più disponibili, tolleranti ai guasti e scalabili rispetto alle infrastrutture a data center singolo o multiplo tradizionali.

Per ulteriori informazioni sulle Regioni AWS e le zone di disponibilità, consulta Infrastruttura globale di AWS.

Oltre all'infrastruttura globale AWS, AWS IoT Device Defender offre numerose funzionalità per supportare la resilienza dei dati e le esigenze di backup.

Cronologia dei documenti per la Guida per l'utente di AWS IoT Device Defender

La tabella seguente descrive i rilasci della documentazione per AWS IoT Device Defender.

Modifica	Descrizione	Data
Disponibilità generale	Questa è la versione pubblica iniziale di AWS IoT Device Defender.	2 agosto 2023
AWS IoT Device Defender ora supporta il monitoraggio della durata della disconnessione dei dispositivi	AWS IoT Device Defender Rules Detect ora supporta la metrica per monitorare la durata della disconnessione di ciascun dispositivo. Con questa metrica aggiuntiv a, puoi tenere traccia del tempo di disconnessione di un dispositivo per verificare se funziona come previsto. Puoi anche configurare allarmi a livelli di soglia predefiniti e ricevere un avviso in caso di problemi persistenti di connettività del dispositivo. Per la documentazione, consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.	20 luglio 2023
La funzionalità di controllo di AWS IoT Device Defender identifica potenziali errori di configurazione nelle policy IoT	Identifica i difetti, risolvi i problemi e intraprendi le azioni correttive necessari e utilizzando la funzional ità Audit. Questa nuova	6 dicembre 2022

funzionalità consente anche di identificare le policy IoT con istruzioni di autorizza zione permissive tramite cui i dispositivi possono accedere a risorse indesiderate. Esamina inoltre l'uso di caratteri jolly MQTT nelle istruzioni di rifiuto che potrebbero essere aggirate dai dispositivi quando sostituiscono i caratteri jolly con stringhe specifiche. Per ulteriori informazioni, consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.

Supporto per metriche e dimensioni personalizzate AWS IoT Device Defender ML Detect	AWS IoT Device Defender ora supporta un nuovo controllo di audit per l'Autorità di certificazione (CA) intermedi a revocata. Se una CA revoca una CA intermedi a perché è potenzialmente compromessa, anche tutti i certificati emessi da tale CA intermedia sono considerati potenzialmente compromes si e non validi. Questo nuovo controllo di audit identifica i certificati di dispositivo attivi emessi da una CA intermedi a revocata e consente ai clienti di esaminare e sostituir e questi certificati di dispositi vo attivi. Per ulteriori informazi oni, consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.	10 novembre 2022

Supporto per metriche e dimensioni personalizzate AWS IoT Device Defender ML Detect	ML Detect ora supporta il monitoraggio delle metriche personalizzate che consentono di valutare i parametri dell'integrità operativa specifici del parco istanze. Oltre a impostare manualmente gli allarmi statici con Rules Detect, ora è possibile utilizzare il machine learning per apprendere automaticamente i comportamenti previsti del parco istanze in base ai parametri personalizzati. Inoltre, con il nuovo supporto del filtro Dimensioni di ML Detect, puoi definire gli attributi per valutare metriche più precise nel profilo di sicurezza di ML. Consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.	14 settembre 2022

Gestione del dispositivo AWS IoT e AWS IoT Device Defender ora supportano il monitoraggio delle metriche dei dispositivi tramite l'API ListMetricValues	Accedi alle metriche storiche lato dispositivo, lato cloud e personalizzate dei dispositivi connessi che appartengono a un profilo di sicurezza utilizzando l'API ListMetricValues. Oltre a visualizzare i dati nella console di gestione AWS IoT, ora hai la flessibilità di monitorare a livello di codice e creare una tua visualizzazione personalizzata. Per la documentazione, consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.	5 aprile 2022
AWS IoT Device Defender ora supporta gli stati di verifica degli allarmi di Detect	Verifica un allarme in base all'indagine sulle anomalie comportamentali rilevate. Un allarme può essere definito come Vero positivo, Benigno positivo, Falso positivo o Sconosciuto e viene fornita una descrizione della verifica. Per la documentazione, consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.	24 settembre 2021

Rilascio di AWS IoT Device Defender Audit One-Click	Audit One-Click consente ai clienti AWS IoT Core di migliorare facilmente la baseline di sicurezza, permettendo loro di eseguire audit sul proprio account e sui dispositivi IoT rispetto alle best practice di sicurezza con un solo clic. Audit One-Click consente ai clienti di attivare un audit AWS IoT Device Defender con configurazioni preimpostate, tra cui l'abilita zione di tutti i controlli di audit disponibili e di un programma di audit giornaliero. Fornisce inoltre spiegazioni contestua li sui vantaggi degli audit di sicurezza regolari. Audit One-Click è disponibile solo dalla console AWS IoT. Per la documentazione, consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.	22 settembre 2021

Supporto di AWS IoT Device Defender CloudFormation	AWS IoT Device Defender Rules Detect ora supporta una nuova metrica per monitorare la durata della disconnessione. AWS IoT Device Defender ora supporta AWS CloudFormation per la creazione e la configurazione di risorse AWS IoT Device Defender come audit pianificati e profili di sicurezza in modo sicuro, efficiente e ripetibile. Per ulteriori informazioni sui tipi di risorse AWS CloudFormation supportati da AWS IoT Device Defender, consulta IoT resource type reference.	5 marzo 2021
AWS IoT Device Defender aggiunge il supporto per le metriche personalizzate	Utilizza AWS IoT Device Defender per il monitoraggio delle metriche dell'integrità operativa specifiche del parco istanze. Gli avvisi possono essere visualizzati nella console di Device Defender o condivisi tramite AWS Simple Notification Service (SNS). Per la documentazione, consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.	15 dicembre 2020

AWS IoT Device Defender lancia l'eliminazione dei risultati di audit	La funzionalità Eliminazione dei risultati di audit consente di scegliere quali risultati di audit visualizzare e di disattiva re i risultati non conformi per risorse specifiche. Inoltre, è possibile configurare l'elimina zione dei risultati degli audit per un periodo di tempo definito o a tempo indetermi nato. Per la documentazione, consulta Audit nella Guida per gli sviluppatori di AWS IoT Device Defender.	12 agosto 2020
AWS IoT Device Defender ora supporta le dimensioni per il monitoraggio delle metriche basato su argomenti	La funzionalità Dimensioni consente ai clienti di filtrare le metriche che Device Defender Detect valuta in base all'argom ento MQTT. Sono supportat e le seguenti metriche lato cloud: numero di messaggi ricevuti, dimensione in byte dei messaggi, numero di messaggi inviati, IP di origine e numero di errori di autorizza zione. Per la documenta zione, consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.	2 aprile 2020

Disponibilità generale di AWS IoT Device Defender ML Detect	La funzionalità ML Detect di AWS IoT Device Defender rileva automaticamente le anomalie operative e di sicurezza a livello di dispositivo nel parco istanze, apprendendo dai dati passati. Per la documentazione, consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.	24 marzo 2020

AWS IoT Device Defender aggiunge quattro nuovi controlli alla capacità di audit	Usa AWS IoT Device Defender Audit per verificare la presenza di dispositivi del parco istanze che dispongono di autorizzazioni eccessivamente permissive, hanno accesso a servizi che non vengono utilizzati da più di 365 giorni, utilizzano versioni OpenSSL su sistemi operativi basati su Debian identificati come dotati di chiavi crittografiche prevedibili che li rendono suscettibili agli attacchi di forza bruta o utilizzano versioni della libreria Infineon RSA che sono state identificate per gestire in modo errato la generazione delle chiavi RSA rendendole suscettibili agli attacchi di hacking. Per la documentazione, consulta Audit nella Guida per gli sviluppatori di AWS IoT Device Defender.	25 novembre 2019
AWS IoT Device Defender supporta le azioni di mitigazione per i risultati di audit	AWS IoT Device Defender supporta la capacità di applicare le azioni di mitigazione ai risultati degli audit da parte dei clienti. Per la documentazione, consulta Audit nella Guida per gli sviluppatori di AWS IoT Device Defender.	6 agosto 2019

AWS IoT Device Defender supporta il monitoraggio del comportamento dei dispositivi non registrati	Identifica i comportamenti insoliti dei dispositivi che non sono registrati nel registro AWS IoT Core. Per la documentazione, consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.	15 maggio 2019
AWS IoT Device Defender ora fornisce il rilevamento statistico delle anomalie e la visualizzazione dei dati	Usa il rilevamento statistico delle anomalie e ricevi gli avvisi quando un dispositivo non rientra nella soglia basata sui percentili. Per la documentazione, consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.	19 febbraio 2019
AWS IoT Device Defender ora supporta il monitoraggio della durata della disconnessione dei dispositivi	AWS IoT Device Defender ora supporta due metriche aggiuntive lato cloud, il numero di tentativi di connessione e il numero di disconnessioni. Per la documentazione, consulta Parametri sul lato cloud nella Guida per gli sviluppatori di AWS IoT Device Defender.	19 dicembre 2018