Guía para desarrolladores de AWS IoT Device Defender

AWS IoT Device Defender

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

AWS IoT Device Defender: Guía para desarrolladores de AWS IoT Device Defender

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

Las marcas registradas y la imagen comercial de Amazon no se pueden utilizar en ningún producto o servicio que no sea de Amazon de ninguna manera que pueda causar confusión entre los clientes y que menosprecie o desacredite a Amazon. Todas las demás marcas registradas que no son propiedad de Amazon, sino que son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es AWS IoT Device Defender? ... 1
¿Es la primera vez que usa AWS IoT Device Defender? ... 2
Cómo funciona AWS IoT Device Defender ... 2
Características de AWS IoT Device Defender ... 3
Cómo comenzar con AWS IoT Device Defender ... 5
Servicios relacionados ... 6
Acceso a AWS IoT Device Defender ... 6
Precios de AWS IoT Device Defender ... 6
Introducción a AWS IoT Device Defender ... 7
Configuración ... 7
Registro en una Cuenta de AWS ... 7
Creación de un usuario con acceso administrativo ... 8
Guía de auditoría ... 9
Requisitos previos ... 10
Habilitación de comprobaciones de auditoría ... 10
Visualización de los resultados de auditoría ... 10
Creación de acciones de mitigación de auditoría ... 11
Aplicación de acciones de mitigación a los resultados de la auditoría ... 11
Creación de un rol de IAM de auditoría de AWS IoT Device Defender (opcional) ... 12
Habilitación de notificaciones de SNS (opcional) ... 13
Habilitación del registro (opcional) ... 14
Guía de ML Detect ... 14
Requisitos previos ... 15
Cómo utilizar ML Detect en la consola ... 15
Cómo usar ML Detect con la CLI ... 32
Personalizar cuándo y cómo ver los resultados de auditoría de AWS IoT Device Defender ... 46
Introducción ... 47
Personalización de los resultados de la auditoría en la consola ... 48
Personalización de los resultados de la auditoría en la CLI ... 51
Auditoría ... 59
Gravedad del problema ... 59
Siguientes pasos ... 60
Comprobaciones de auditoría ... 60

Se ha revocado la entidad de certificación intermedia para comprobar los certificados de los dispositivos activos ... 61
El certificado de entidad de certificación revocado sigue activo ... 63
Certificado de dispositivo compartido ... 64
Calidad de la clave del certificado del dispositivo ... 65
Calidad de la clave del certificado de entidad de certificación ... 67
El rol de Cognito no autenticado es demasiado permisivo ... 69
El rol de Cognito autenticado es demasiado permisivo ... 77
Políticas de AWS IoT demasiado permisivas ... 87
La política de AWS IoT está potencialmente mal configurada ... 93
El alias de rol es demasiado permisivo ... 97
El alias del rol permite el acceso a los servicios no utilizados ... 99
El certificado de entidad de certificación está caducando ... 100
Identificadores de cliente MQTT contradictorios ... 101
El certificado de dispositivo está caducando ... 103
Comprobación de la antigüedad del certificado del dispositivo ... 104
Un certificado del dispositivo revocado sigue activo ... 105
Registro desactivado ... 107
Comandos de auditoría ... 108
Administrar la configuración de auditorías ... 108
Programación de auditorías ... 115
Ejecutar una auditoría bajo demanda ... 128
Administrar instancias de auditoría ... 130
Comprobar resultados de auditoría ... 140
Supresiones de resultados de auditoría ... 150
Cómo funcionan las supresiones de resultados de auditoría ... 150
Cómo utilizar las supresiones de los resultados de auditoría en la consola ... 151
Cómo utilizar las supresiones de resultados de auditoría en la CLI ... 158
API de supresiones de resultados de auditoría ... 160
Detect ... 161
Monitorización del comportamiento de dispositivos no registrados ... 162
Casos de uso de seguridad ... 163
Casos de uso en la nube ... 163
Casos de uso del lado del dispositivo ... 166
Conceptos ... 171
Comportamientos ... 173

ML Detect ... 176
Casos de uso de ML Detect ... 177
Cómo funciona ML Detect ... 177
Requisitos mínimos ... 178
Limitaciones ... 179
Marcar los falsos positivos y otros estados de verificación en las alarmas ... 179
Métricas admitidas ... 180
Service Quotas ... 180
Comandos de la CLI de ML Detect ... 180
API ML Detect API ... 181
Pausar o eliminar un perfil de seguridad de ML Detect ... 181
Métricas personalizadas ... 183
Cómo usar las métricas personalizadas en la consola ... 183
Cómo usar métricas personalizadas desde la CLI ... 186
Comandos de la CLI para métricas personalizadas ... 191
API de métricas personalizadas ... 191
Métricas del lado del dispositivo ... 191
Bytes salientes (`aws:all-bytes-out`) ... 191
Bytes entrantes (`aws:all-bytes-in`) ... 193
Recuento de puertos TCP de escucha (`aws:num-listening-tcp-ports`) ... 194
Recuento de puertos UDP de escucha (`aws:num-listening-udp-ports`) ... 196
Paquetes salientes (`aws:all-packets-out`) ... 198
Paquetes entrantes (`aws:all-packets-in`) ... 199
IP de destino (`aws:destination-ip-addresses`) ... 201
Puertos TCP de escucha (`aws:listening-tcp-ports`) ... 201
Puertos UDP de escucha (`aws:listening-udp-ports`) ... 202
Recuento de conexiones TCP establecidas (`aws:num-established-tcp-connections`) ... 203
Especificación de documentos de métricas de dispositivos ... 204
Envío de métricas desde dispositivos ... 213
Métricas del lado de la nube ... 215
Tamaño del mensaje (aws:message-byte-size) ... 215
Mensajes enviados (aws:num-messages-sent) ... 216
Mensajes recibidos (aws:num-messages-received) ... 218
Fallos de autorización (aws:num-authorization-failures) ... 219
IP de origen (aws:source-ip-address) ... 221

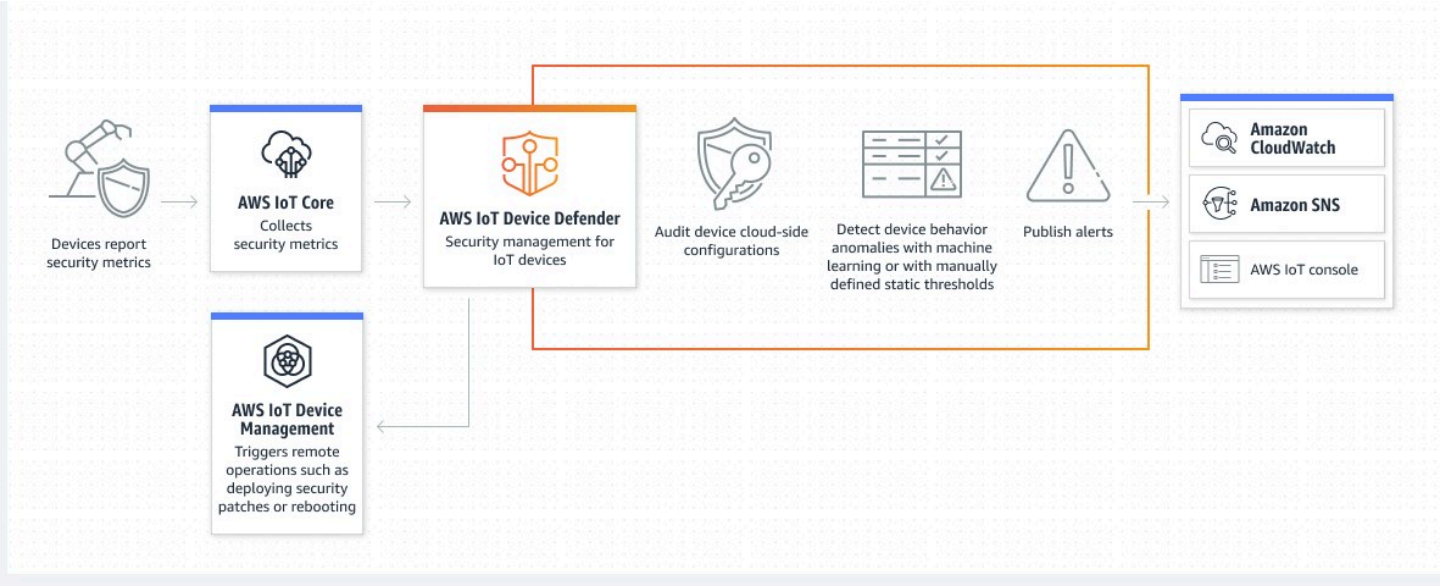
Intentos de conexión (aws:num-connection-attempts) ... 222
Desconexiones (aws:num-disconnects) ... 223
Duración de la desconexión (aws:disconnect-duration) ... 225
Exportación de métricas de Detect ... 225
Cómo funciona la exportación de métricas de Detect ... 228
Esquema de exportación de métricas ... 228
Precios de exportación de métricas de Detect ... 230
Permisos ... 230
Configuración de la exportación de métricas de Detect en la consola de AWS IoT ... 231
Crear un perfil de seguridad y habilitar la exportación de métricas ... 234
Actualización de un perfil de seguridad para habilitar la exportación de métricas (CLI) ... 235
Actualización de un perfil de seguridad para deshabilitar la exportación de métricas (CLI) ... 236
Comandos de la CLI para exportación de métricas ... 238
Operaciones de la API de exportación de métricas ... 238
Establecer el ámbito de las métricas en los perfiles de seguridad utilizando dimensiones ... 238
Cómo utilizar las dimensiones en la consola ... 239
Cómo utilizar las dimensiones en la AWS CLI ... 240
Permisos ... 245
Otorgar permiso a AWS IoT Device Defender Detect para publicar alarmas en un tema de SNS ... 245
Comandos de detección ... 247
Cómo utilizar AWS IoT Device Defender Detect ... 249
Acciones de mitigación ... 252
Acciones de mitigación de auditoría ... 252
Acciones de mitigación de Detect ... 257
Cómo definir y administrar las acciones de mitigación ... 257
Creación de acciones de mitigación ... 257
Aplicación de acciones de mitigación ... 259
Permisos ... 265
Comandos de las acciones de mitigación ... 270
Uso de AWS IoT Device Defender con otros servicios de AWS. ... 271
Uso de AWS IoT Device Defender con dispositivos que ejecutan AWS IoT Greengrass ... 271
Uso de AWS IoT Device Defender con FreeRTOS y dispositivos integrados ... 271
Uso de AWS IoT Device Defender con AWS IoT Device Management ... 272
Integración de Security Hub ... 272
Habilitación y configuración de la integración ... 273

Cómo AWS IoT Device Defender envía los resultados a Security Hub 273
Resultado típico de AWS IoT Device Defender 276
Impedir que AWS IoT Device Defender envíe resultados a Security Hub 281
Prevención de la sustitución confusa entre servicios 281
Prácticas recomendadas de seguridad para agentes de dispositivos 283
Guía para solucionar problemas de AWS IoT Device Defender 286
Seguridad 292
Protección de datos 293
Administración de identidades y accesos 294
Público 294
Autenticación con identidades 295
Administración de acceso mediante políticas 299
Cómo AWS IoT Device Defender funciona con IAM 302
Ejemplos de políticas basadas en identidades 308
Resolución de problemas 312
Validación de conformidad 314
Resiliencia 315
Historial de documentos 316

¿Qué es AWS IoT Device Defender?

Utilice AWS IoT Device Defender, un servicio de seguridad y supervisión que permite auditar la configuración de sus dispositivos, monitorizar los dispositivos conectados y mitigar los riesgos de seguridad. Con AWS IoT Device Defender, puede aplicar políticas de seguridad uniformes en toda la flota de dispositivos de AWS IoT y responder rápidamente cuando los dispositivos sufran ataques. Las flotas de IoT pueden constar de un gran número de dispositivos que tienen diversas funcionalidades, son de larga duración y están distribuidos geográficamente. Estas características hacen que la configuración de la flota sea compleja y propensa a errores. Dado que los dispositivos a menudo tienen limitaciones de potencia informática, memoria y capacidad de almacenamiento, esto acota el uso del cifrado y otras formas de seguridad en los propios dispositivos.

Los dispositivos a menudo usan software con vulnerabilidades conocidas. Por todos estos factores, las flotas de IoT son un objetivo atractivo para los piratas informáticos y la protección continua de estas es un desafío. AWS IoT Device Defender aborda estos obstáculos ofreciendo las herramientas necesarias para identificar los problemas de seguridad y las desviaciones con respecto a los procedimientos recomendados. AWS IoT Device Defender puede auditar las flotas de dispositivos para ver si cumplen con dichos procedimientos y para detectar un comportamiento anómalo en los dispositivos. En el siguiente diagrama, se muestra la arquitectura básica de AWS IoT Device Defender, así como de su relación con servicios como AWS IoT Core, Amazon CloudWatch y Amazon SNS.



Temas

- ¿Es la primera vez que usa AWS IoT Device Defender?

- Cómo funciona AWS IoT Device Defender
- Características de AWS IoT Device Defender
- Cómo comenzar con AWS IoT Device Defender
- Servicios relacionados
- Acceso a AWS IoT Device Defender
- Precios de AWS IoT Device Defender

¿Es la primera vez que usa AWS IoT Device Defender?

Si es la primera vez que usa AWS IoT Device Defender, le recomendamos que empiece leyendo las siguientes secciones:

- Cómo funciona AWS IoT Device Defender
- Características de AWS IoT Device Defender
- Cómo comenzar con AWS IoT Device Defender
- Servicios relacionados
- Acceso a AWS IoT Device Defender
- Precios de AWS IoT Device Defender

Cómo funciona AWS IoT Device Defender

AWS IoT Device Defender es un servicio de seguridad y supervisión totalmente administrado que le ayuda a proteger su flota de dispositivos IoT. AWS IoT Device Defender audita los recursos IoT asociados a sus dispositivos para confirmar que cumplen con los procedimientos recomendados de seguridad. Las comprobaciones de auditoría envían alertas si se detecta algún riesgo de seguridad y proporcionan información relevante para mitigar cualquier problema. AWS IoT Device Defender también supervisa continuamente las métricas de seguridad desde la nube y desde el lado del dispositivo para detectar comportamientos inesperados e identificar cualquier dispositivo que pueda estar comprometido. Puede iniciar comprobaciones de auditoría bajo demanda o de forma programada para evaluar las configuraciones de sus dispositivos de IoT.

AWS IoT Device Defender funciona con AWS IoT Core para incorporar el contexto de las interacciones entre los dispositivos a fin de aumentar la precisión de las comprobaciones de

auditoría. AWS IoT Device Defender recopila y analiza métricas de seguridad de alto valor de los dispositivos conectados para detectar comportamientos anómalos. Al utilizar Rules Detect, los datos de las métricas se evalúan continuamente comparándolos con los comportamientos definidos por el usuario. Cuando se utiliza ML Detect, los datos de las métricas se evalúan de forma continua mediante modelos de machine learning (ML) creados automáticamente para identificar las anomalías.

Los resultados de las tareas de auditoría programadas y cualquier anomalía detectada en la actividad del dispositivo se publican en la consola de AWS IoT y en la API de AWS IoT Device Defender. Se puede acceder a estos desde Amazon CloudWatch Además, puede configurar AWS IoT Device Defender para que los resultados se envíen a los temas de Amazon SNS, a fin de integrarlos con los paneles de seguridad o de iniciar flujos de trabajo de corrección automatizados.

AWS IoT Device Defender se puede emplear en una amplia gama de casos de uso, como los siguientes:

- Protección de dispositivos: puede auditar sus recursos relacionados con los dispositivos comparándolos con los procedimientos recomendados de seguridad de AWS IoT a fin de detectar las vulnerabilidades de los dispositivos. Las auditorías de AWS IoT Device Defender pueden ayudarle a identificar y descubrir los riesgos para sus dispositivos, así como a confirmar si se han implementado medidas de seguridad.
- Detección de comportamiento inusual en dispositivos: puede detectar con precisión los cambios en los patrones de conexión, revelar la comunicación del dispositivo con puntos de conexión no autorizados e identificar los cambios en los patrones de tráfico entrante y saliente de los dispositivos.
- Obtener información para mitigar riesgos: puede tomar medidas para mitigar los problemas descubiertos en un resultado de Audit o en una alarma de Detect.
- Mantener la seguridad de los dispositivos: puede utilizar la información de las comprobaciones de Audit y Detect para diagnosticar y corregir posibles brechas de seguridad.
- Mejorar la seguridad de los dispositivos: puede distinguir un dispositivo configurado incorrectamente, comprobar el estado de sus flotas de dispositivos y localizar métricas de comportamiento inesperado del dispositivo.

Características de AWS IoT Device Defender

Estas son algunas de las características más importantes de AWS IoT Device Defender.

Características principales de

Auditoría	AWS IoT Device Defender audita sus recursos relacionados con los dispositivos comparánd olos con los procedimientos recomendados de seguridad de AWS IoT, en la Guía del usuario de IAM. AWS IoT Device Defender informa sobre configuraciones que no cumplen con los procedimientos recomendados de seguridad, como las políticas poco restrictivas, que podrían permitir que un dispositivo lea y actualice los datos de muchos otros dispositi vos.
Rules Detect	AWS IoT Device Defender detecta un comportamiento inusual de los dispositivos que podría indicar peligro; para ello, supervisa continuamente las métricas de seguridad de alto valor del dispositivo y de AWS IoT Core. Puede especificar el comportamiento normal de los dispositivos para un grupo de dispositi vos configurando los comportamientos (reglas) para estas métricas. AWS IoT Device Defender supervisa y evalúa cada punto de datos registrado para estas métricas comparándolo con los comportamientos (reglas) definidos por el usuario y le avisa si se detecta una anomalía.
ML Detect	AWS IoT Device Defender establece automátic amente el comportamiento de los dispositi vos mediante modelos de machine learning (ML) que utilizan los datos del dispositivo en seis métricas de la nube y siete métricas del lado del dispositivo para los últimos catorce días. Luego, reorganiza los modelos todos los

	días (siempre y cuando haya datos suficient es para entrenar el modelo) para actualizar el comportamiento esperado de los dispositivos en función de los últimos catorce días después de la creación de los modelos iniciales. AWS IoT Device Defender supervisa e identifica los puntos de datos anómalos de estas métricas con los modelos de machine learning y activa una alarma si se detecta una anomalía.
Alertas	AWS IoT Device Defender publica las alarmas en la consola de AWS IoT, Amazon CloudWatc h y Amazon SNS.
Mitigación	AWS IoT Device Defender se puede utilizar para investigar problemas proporcionando información contextual e histórica sobre el dispositivo, como metadatos, estadísticas y alertas históricas del dispositivo. También puede utilizar las acciones de mitigación integradas en AWS IoT Device Defender para mitigar las alarmas de Audit y Detect; por ejemplo, añadir elementos a un grupo de objetos, sustituir la versión predeterminada de la política y actualizar el certificado del dispositi vo.

Cómo comenzar con AWS IoT Device Defender

Si desea obtener ayuda para empezar a usar AWS IoT Device Defender, consulte los siguientes tutoriales.

- Configuración
- Guía de ML Detect
- Guía de Audit

- Personalizar cuándo y cómo ver los resultados de auditoría de AWS IoT Device Defender

Servicios relacionados

- AWS IoT Greengrass:AWS IoT Greengrass proporciona una integración prediseñada con AWS IoT Device Defender para monitorizar los comportamientos de los dispositivos de forma continua.
- AWS IoT Device Management: Puede utilizar la indexación de flotas de AWS IoT Device Management para indexar, buscar y agregar las infracciones de AWS IoT Device Defender Detect.

Acceso a AWS IoT Device Defender

Puede usar la consola AWS IoT Device Defender o la API para acceder a AWS IoT Device Defender.

Precios de AWS IoT Device Defender

Con AWS IoT Device Defender, solo paga por lo que usa. No se requieren cuotas mínimas ni hay ningún uso obligatorio del servicio. Sin embargo, las características Audit y Detect se facturan por separado. El precio de Audit se calcula por número de dispositivos por mes. Al activar Audit, se le cobrará en función de la cantidad de dispositivos activos principales en un mes. Por lo tanto, agregar o eliminar comprobaciones de auditoría no afectaría a la factura mensual al utilizar esta característica. Puede calcular los costes de arquitectura y AWS IoT Device Defender en una sola estimación mediante la Calculadora de precios de AWS.

- Calculadora de precios de AWS

Introducción a AWS IoT Device Defender

Puede utilizar los siguientes aprendizajes para trabajar con AWS IoT Device Defender.

Temas

- Configuración
- Guía de auditoría
- Guía de ML Detect
- Personalizar cuándo y cómo ver los resultados de auditoría de AWS IoT Device Defender

Configuración

Antes de usar AWS IoT Device Defender por primera vez, realice las siguientes tareas:

Temas

- Registro en una Cuenta de AWS
- Creación de un usuario con acceso administrativo

Registro en una Cuenta de AWS

Si no dispone de una Cuenta de AWS, siga estos pasos para crear una.

Procedimiento para registrarse en Cuenta de AWS

1. Abra https://portal.aws.amazon.com/billing/signup.
2. Siga las instrucciones que se le indiquen.

   Parte del procedimiento de registro consiste en recibir una llamada telefónica e indicar un código de verificación en el teclado del teléfono.

   Al registrarse en una Cuenta de AWS, se crea un Usuario raíz de la cuenta de AWS. El usuario raíz tendrá acceso a todos los Servicios de AWS y recursos de esa cuenta. Como práctica recomendada de seguridad, asigne acceso administrativo a un usuario y utilice únicamente el usuario raíz para realizar tareas que requieren acceso de usuario raíz.

AWS le enviará un email de confirmación cuando complete el proceso de registro. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de registrarse para obtener una Cuenta de AWS, proteja su Usuario raíz de la cuenta de AWS, habilite AWS IAM Identity Center y cree un usuario administrativo para no utilizar el usuario raíz en las tareas cotidianas.

Protección de Usuario raíz de la cuenta de AWS

1. Inicie sesión en AWS Management Console como propietario de la cuenta; para ello, elija Usuario raíz e introduzca el correo electrónico de su Cuenta de AWS. En la siguiente página, escriba su contraseña.

   Para obtener ayuda para iniciar sesión con el usuario raíz, consulte Iniciar sesión como usuario raíz en la Guía del usuario de AWS Sign-In.
2. Active la autenticación multifactor (MFA) para el usuario raíz.

   Para obtener instrucciones, consulte Habilitación de un dispositivo MFA virtual para su usuario raíz de la Cuenta de AWS (consola) en la Guía del usuario de IAM.

Creación de un usuario con acceso administrativo

1. Activar IAM Identity Center.

   Consulte las instrucciones en Activar AWS IAM Identity Center en la Guía del usuario de AWS IAM Identity Center.
2. En IAM Identity Center, conceda acceso administrativo a un usuario.

   Para ver un tutorial sobre cómo utilizar Directorio de IAM Identity Center como origen de identidad, consulte Configuración del acceso de los usuarios con el Directorio de IAM Identity Center predeterminado en la Guía del usuario de AWS IAM Identity Center.

Iniciar sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, utilice la URL de inicio de sesión que se envió a la dirección de correo electrónico cuando creó el usuario de IAM Identity Center.

Para obtener ayuda para iniciar sesión con un usuario del IAM Identity Center, consulte Inicio de sesión en el portal de acceso de AWS en la Guía del usuario de AWS Sign-In.

Concesión de acceso a usuarios adicionales

1. En IAM Identity Center, cree un conjunto de permisos que siga la práctica recomendada de aplicar permisos de privilegios mínimos.

   Para conocer las instrucciones, consulte Create a permission set en la Guía del usuario de AWS IAM Identity Center.

2. Asigne usuarios a un grupo y, a continuación, asigne el acceso de inicio de sesión único al grupo.

   Para conocer las instrucciones, consulte Add groups en la Guía del usuario de AWS IAM Identity Center.

Estas tareas crean una Cuenta de AWS y un usuario con privilegios de administrador en la cuenta.

Guía de auditoría

Este tutorial proporciona instrucciones sobre cómo configurar una auditoría periódica, configurar alarmas, revisar los resultados y mitigar los problemas.

Temas

- Requisitos previos
- Habilitación de comprobaciones de auditoría
- Visualización de los resultados de auditoría
- Creación de acciones de mitigación de auditoría
- Aplicación de acciones de mitigación a los resultados de la auditoría
- Creación de un rol de IAM de auditoría de AWS IoT Device Defender (opcional)
- Habilitación de notificaciones de SNS (opcional)
- Habilitación del registro (opcional)

Requisitos previos

Necesitará lo siguiente para completar este tutorial:

- Una Cuenta de AWS. Si no tiene una, consulte Configuración.

Habilitación de comprobaciones de auditoría

En el siguiente procedimiento, habilite las comprobaciones de auditoría que analizan la configuración y las políticas de la cuenta y el dispositivo para garantizar que se apliquen las medidas de seguridad. En este tutorial le indicamos que habilite todas las comprobaciones de auditoría, pero podrá seleccionar las que desee.

Los precios de las auditorías se calculan por número de dispositivos al mes (dispositivos de la flota conectados a AWS IoT). Por lo tanto, agregar o eliminar comprobaciones de auditoría no afectaría a la factura mensual al utilizar esta característica.

1. Abra la consola de AWS IoT. En el panel de navegación, elija Seguridad e Intro.
2. Seleccione Automatizar auditoría de seguridad de AWS IoT. Las comprobaciones de auditoría se activan automáticamente.
3. Expanda Auditoría y seleccione Configuración para ver las comprobaciones de auditoría. Seleccione un nombre de comprobación de auditoría para obtener información sobre lo que hace la comprobación de auditoría. Para obtener más información sobre las comprobaciones de auditoría, consulte Comprobaciones de auditoría.
4. (Opcional) Si ya tiene un rol que quiere usar, elija Administrar permisos de servicio, seleccione el rol en la lista y, a continuación, elija Actualizar.

Visualización de los resultados de auditoría

En el siguiente procedimiento se muestra cómo ver los resultados de auditoría. En este tutorial, verá los resultados de las comprobaciones de auditoría configuradas en el tutorial Habilitación de comprobaciones de auditoría.

Para ver los resultados de auditoría

1. Abra la consola de AWS IoT. En el panel de navegación, expanda Seguridad, Auditoría y, a continuación, seleccione Resultados.

2. Seleccione el nombre de la programación de auditoría que desee investigar.
3. En Comprobaciones no compatibles, en Mitigación, seleccione los botones de información para obtener información sobre los motivos por los que no son compatibles. Para obtener información sobre cómo hacer que las comprobaciones no compatibles sí lo sean, consulte Comprobaciones de auditoría.

Creación de acciones de mitigación de auditoría

En el siguiente procedimiento, creará una acción de mitigación de auditoría de AWS IoT Device Defender para habilitar el registro de AWS IoT. Cada comprobación de auditoría ha asignado las acciones de mitigación que afectarán al tipo de acción que elija para la comprobación de auditoría que quiera corregir. Para obtener más información, consulte Acciones de mitigación.

Para utilizar la consola de AWS IoT para crear acciones de mitigación

1. Abra la consola de AWS IoT. En el panel de navegación, expanda Seguridad, Detectar y, a continuación, seleccione Acciones de mitigación.
2. En la página Acciones de mitigación, elija Crear.
3. En la página Crear una acción de mitigación, en Nombre de la acción, escriba un nombre único para la acción de mitigación, por ejemplo, *`EnableErrorLoggingAction`*.
4. En Tipo de acción, seleccione Habilitar registro de AWS IoT.
5. En Permisos, seleccione Crear rol. Para el nombre del rol, use *`IoTMitigationActionErrorLoggingRole`*. A continuación, elija Crear.
6. En Parámetros, en Rol para el registro, elija `IoTMitigationActionErrorLoggingRole`. En Nivel de registro, elija `Error`.
7. Seleccione Crear.

Aplicación de acciones de mitigación a los resultados de la auditoría

En el siguiente procedimiento se muestra cómo aplicar acciones de mitigación a los resultados de auditoría.

Para mitigar los resultados de la auditoría no compatibles

1. Abra la consola de AWS IoT. En el panel de navegación, expanda Seguridad, Auditoría y, a continuación, seleccione Resultados.

2. Elija un resultado de auditoría al que quiera responder.
3. Compruebe los resultados.
4. Seleccione Iniciar las acciones de mitigación.
5. En Registro desactivado, elija la acción de mitigación que creó anteriormente, `EnableErrorLoggingAction`. Puede seleccionar las acciones adecuadas para cada resultado no compatible con el fin de abordar los problemas.
6. En Seleccionar códigos de motivo, elija el código de motivo que devolvió la comprobación de auditoría.
7. Seleccione Iniciar tarea. La acción de mitigación puede tardar varios minutos en ejecutarse.

Para comprobar que la acción de mitigación ha funcionado

1. En el panel de navegación de la consola de AWS IoT, seleccione Configuración.
2. En Registro de servicio, confirme que el nivel de registro es `Error (least verbosity)`.

Creación de un rol de IAM de auditoría de AWS IoT Device Defender (opcional)

En el siguiente procedimiento, se crea un rol de IAM de auditoría de AWS IoT Device Defender que proporcione acceso de lectura de AWS IoT Device Defender a AWS IoT.

Para crear un rol de servicio para AWS IoT Device Defender (consola de IAM)

1. Inicie sesión en la AWS Management Console y abra la consola de IAM en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, seleccione Crear rol.
3. Elija el tipo de rol Servicio de AWS.
4. En Casos de uso para otros servicios de AWS, elija AWS IoT y, a continuación, elija Auditoría de IoT - Device Defender.
5. Seleccione Siguiente.
6. (Opcional) Configure un límite de permisos. Se trata de una característica avanzada que está disponible para los roles de servicio, pero no para los roles vinculados a servicios.

Amplíe la sección Límite de permisos y seleccione Usar un límite de permisos para controlar los permisos máximos de la función. IAM incluye una lista de las políticas administradas por AWS y de las políticas administradas por el cliente de cada cuenta. Seleccione la política que desea utilizar para el límite de permisos o elija Crear política para abrir una pestaña nueva del navegador y crear una política nueva desde cero. Para obtener más información, consulte Creación de políticas de IAM en la Guía del usuario de IAM. Una vez creada la política, cierre la pestaña y vuelva a la pestaña original para seleccionar la política que va a utilizar para el límite de permisos.

7. Seleccione Siguiente.
8. Introduzca un nombre de rol que le sea útil para identificar su propósito. Los nombres de rol deben ser únicos en su Cuenta de AWS. No distinguen entre mayúsculas y minúsculas. Por ejemplo, no puede crear funciones denominado tanto **`PRODROLE`** como **`prodrole`**. Dado que varias entidades pueden hacer referencia al rol, no puede editar el nombre del rol después de crearlo.
9. (Opcional) En Descripción, ingrese una descripción para el nuevo rol.
10. Seleccione Editar en las secciones Paso 1: seleccionar entidades de confianza o Paso 2: seleccionar permisos para editar los casos de uso y los permisos del rol.
11. (Opcional) Asocie etiquetas como pares de clave-valor para agregar metadatos al rol. Para obtener más información sobre el uso de etiquetas en IAM, consulte Etiquetado de recursos de IAM en la Guía de usuario de IAM .
12. Revise el rol y, a continuación, seleccione Crear rol.

Habilitación de notificaciones de SNS (opcional)

En el siguiente procedimiento, habilite las notificaciones de Amazon SNS (SNS) para que le avisen cuando sus auditorías identifiquen recursos no compatibles. En este tutorial, configurará las notificaciones para las comprobaciones de auditoría habilitadas en el tutorial Habilitación de comprobaciones de auditoría.

1. Si aún no lo ha hecho, asocie una política que proporcione acceso a SNS a través de AWS Management Console. Para ello, siga las instrucciones de Asociación de una política a un grupo de usuarios de IAM en la Guía del usuario de IAM y seleccione la política AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction.
2. Abra la consola de AWS IoT. En el panel de navegación, expanda Seguridad, Auditoría y, a continuación, seleccione Configuración.

3. En la parte inferior de la página Configuración de auditoría de Device Defender, seleccione Habilitar alertas de SNS.
4. Elija Enabled (Habilitado).
5. En Tema, elija Crear nuevo tema. Asigne al tema el nombre `IoTDDNotifications` y elija Crear. En Rol, elija el rol que creó en Creación de un rol de IAM de auditoría de AWS IoT Device Defender (opcional).
6. Seleccione Actualizar.
7. Si desea recibir correos electrónicos o mensajes de texto en sus plataformas Ops a través de Amazon SNS, consulte Uso de Amazon SNS para notificaciones de usuario.

Habilitación del registro (opcional)

En este procedimiento se describe cómo habilitar AWS IoT para registrar información en los registros de CloudWatch. Esto le permitirá ver los resultados de auditoría. Habilitar el registro puede llevar cargos asociados.

Para habilitar el registro

1. Abra la consola de AWS IoT. En el panel de navegación, seleccione Configuración.
2. En Registros, elija Administrar registros.
3. En Seleccionar rol, elija Crear rol. Asigne al rol el nombre `AWSIoTLoggingRole` y elija Crear. Se asocia automáticamente una política.
4. En Nivel de registro, elija Depurar (máximo detalle).
5. Seleccione Actualizar.

Guía de ML Detect

En esta guía de introducción, creará un perfil de seguridad de ML Detect que utiliza el machine learning (ML) para crear modelos del comportamiento esperado basados en los datos métricos históricos de sus dispositivos. Mientras ML Detect crea el modelo de ML, puede monitorizar su avance. Una vez creado el modelo de machine learning, puede ver e investigar las alarmas de forma continua y mitigar los problemas identificados.

Para obtener más información sobre ML Detect y sus comandos de API y de la CLI, consulte ML Detect.

El capítulo contiene las siguientes secciones:

- Requisitos previos
- Cómo utilizar ML Detect en la consola
- Cómo usar ML Detect con la CLI

Requisitos previos

- Una Cuenta de AWS. Si no tiene una, consulte Configuración.

Cómo utilizar ML Detect en la consola

Tutoriales

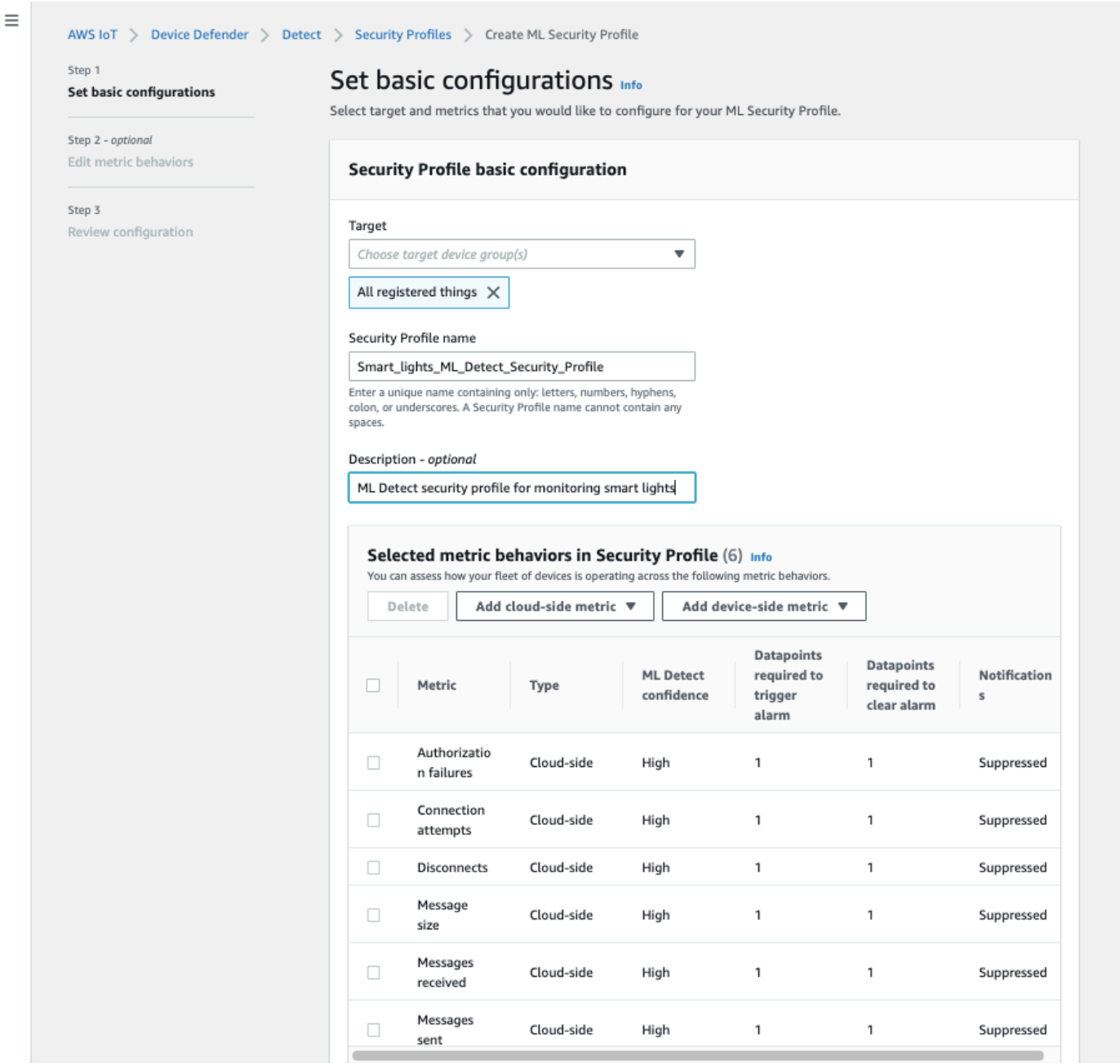
- Habilitar ML Detect
- Monitorizar el estado de su modelo de machine learning
- Revisar las alarmas de ML Detect
- Ajustar sus alarmas de machine learning
- Marcar el estado de verificación de su alarma
- Mitigar los problemas identificados en los dispositivos

Habilitar ML Detect

Los siguientes procedimientos detallan cómo configurar ML Detect en la consola.

1. En primer lugar, asegúrese de que sus dispositivos creen los puntos de datos mínimos necesarios, tal como se definen en los requisitos mínimos de ML Detect para la formación continua y la actualización del modelo. Para que la recopilación de datos progrese, asegúrese de que su perfil de seguridad esté asociado a un objetivo, que puede ser un objeto o un grupo de objetos.
2. En la consola de AWS IoT, en el panel de navegación, amplíe Defend. Seleccione Detectar, Perfiles de seguridad, Crear perfil de seguridad y, a continuación, Crear perfil de detección de anomalías de machine learning.
3. En la página Establecer configuraciones básicas, haga lo siguiente.
   - En Destino, seleccione los grupos de dispositivos de destino.

- En Nombre del perfil de seguridad, escriba un nombre para el perfil de seguridad.
- (Opcional) En Descripción, puede escribir una breve descripción del perfil de machine learning.
- En Comportamientos de métricas seleccionados en el perfil de seguridad, elija las métricas que quiera monitorizar.

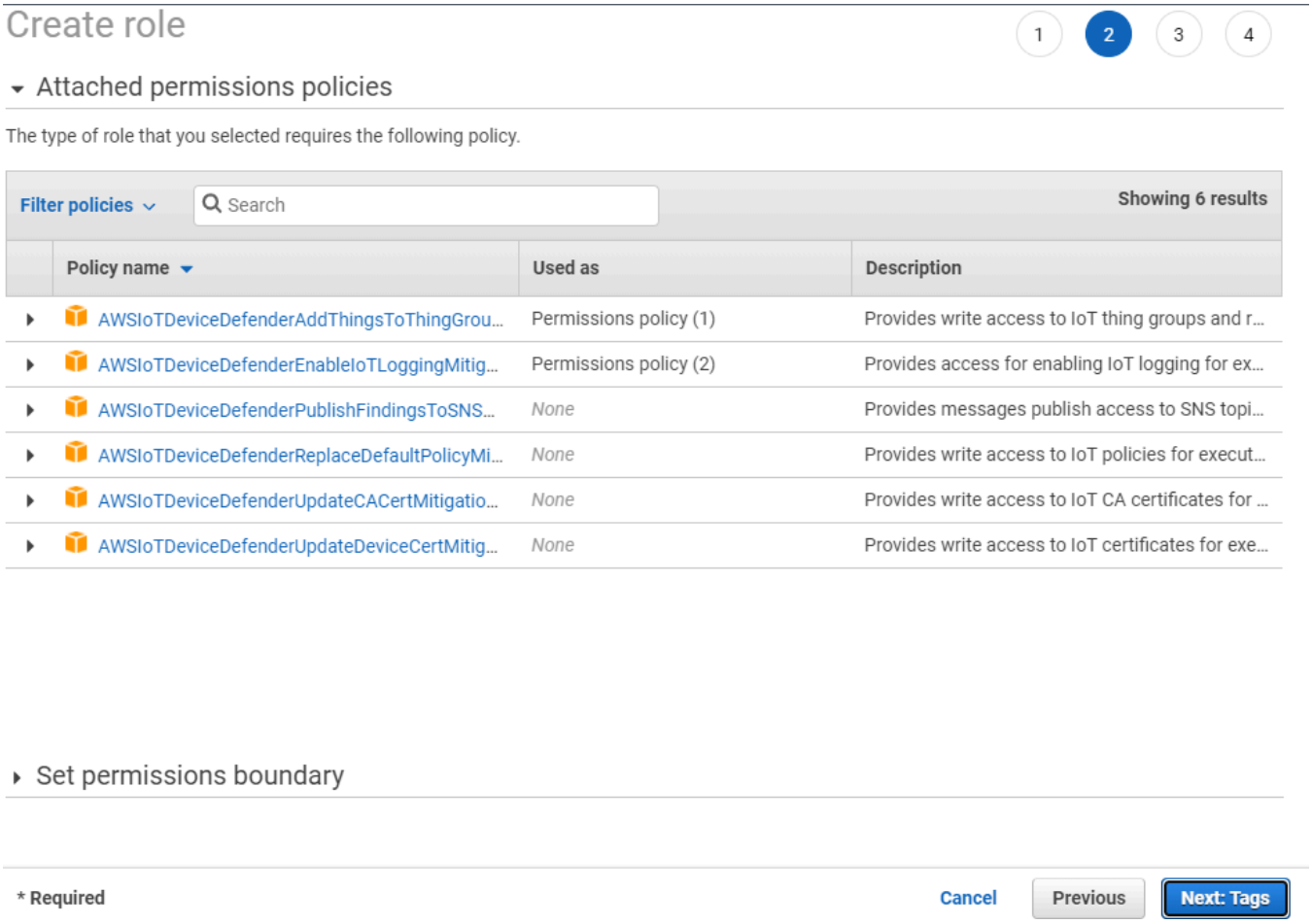


Cuando haya terminado, elija Siguiente.

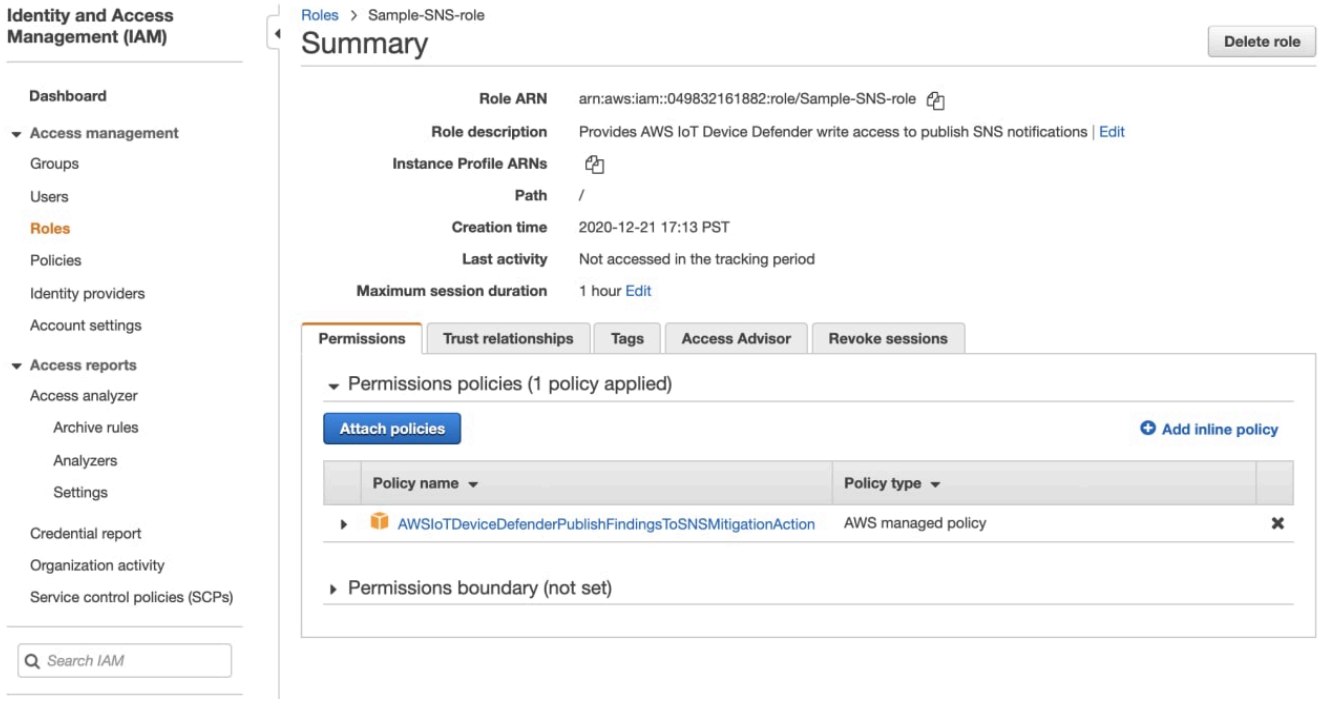
4. En la página Establecer SNS (opcional), especifique un tema de SNS para las notificaciones de alarma cuando un dispositivo infrinja un comportamiento de su perfil. Elija un rol de IAM que utilizará para publicar en el tema de SNS seleccionado.

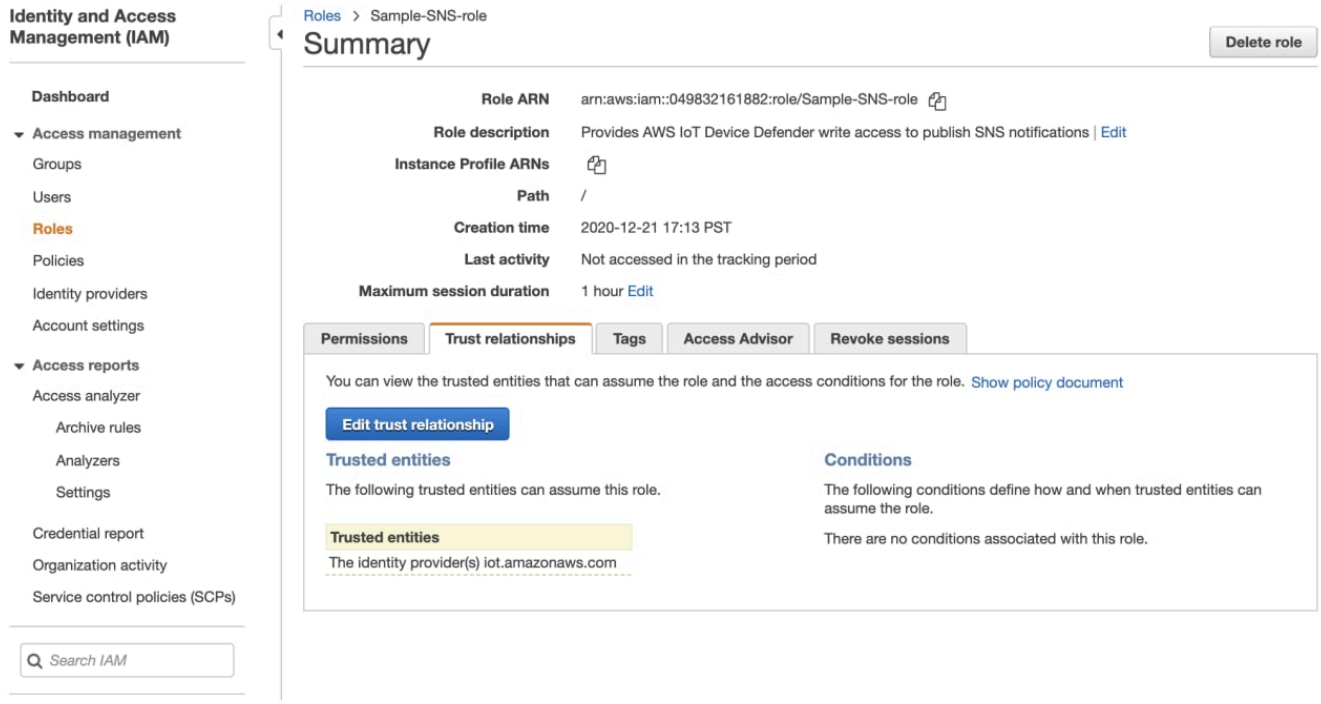
   Si aún no tiene un rol de SNS, siga los siguientes pasos para crear uno con los permisos y las relaciones de confianza adecuados necesarios.

   - Desplácese hasta la consola de IAM. En el panel de navegación, seleccione Roles y, a continuación, seleccione Crear rol.
   - En Seleccionar tipo de entidad de confianza, elija Servicio de AWS. A continuación, en Elija un caso de uso, elija IoT y, en Seleccione su caso de uso, elija IoT: Device Defender Mitigation Actions. Cuando haya terminado, seleccione Siguiente: Permisos.
   - En Políticas de permisos asociadas, asegúrese de que AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction esté seleccionada y, a continuación, elija Siguiente: Etiquetas.

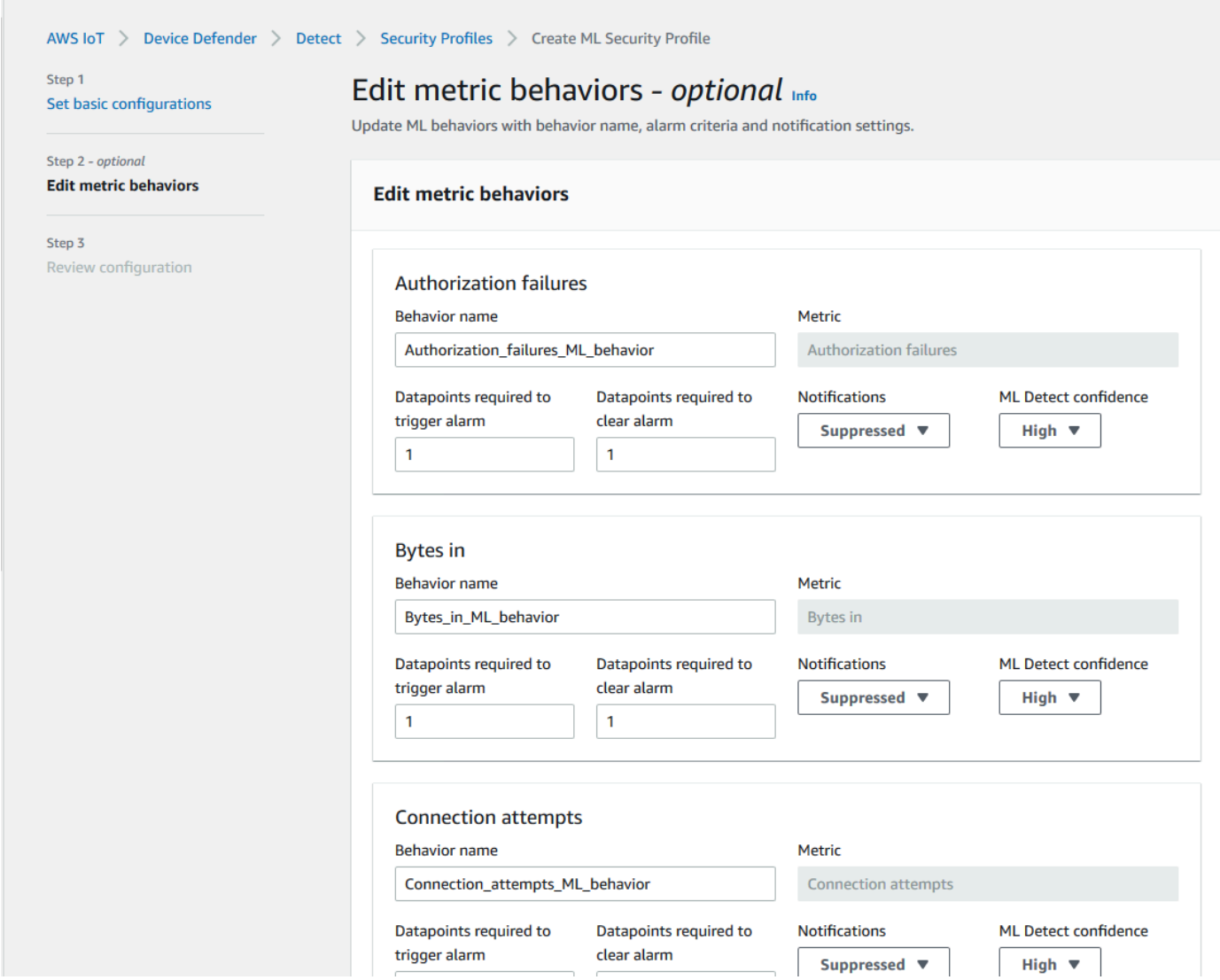


- En Agregar etiquetas (opcional), puede agregar cualquier etiqueta que quiera asociar a su rol. Cuando haya terminado, elija Siguiente: revisar.
- En Revisar, asigne un nombre a su rol y asegúrese de que AWSIoTDeviceDefenderPublishFindingsToSNSMitigationAction aparezca en Permisos y Servicio AWS: iot.amazonaws.com aparezca en Relaciones de confianza. Cuando haya terminado, elija Crear rol.



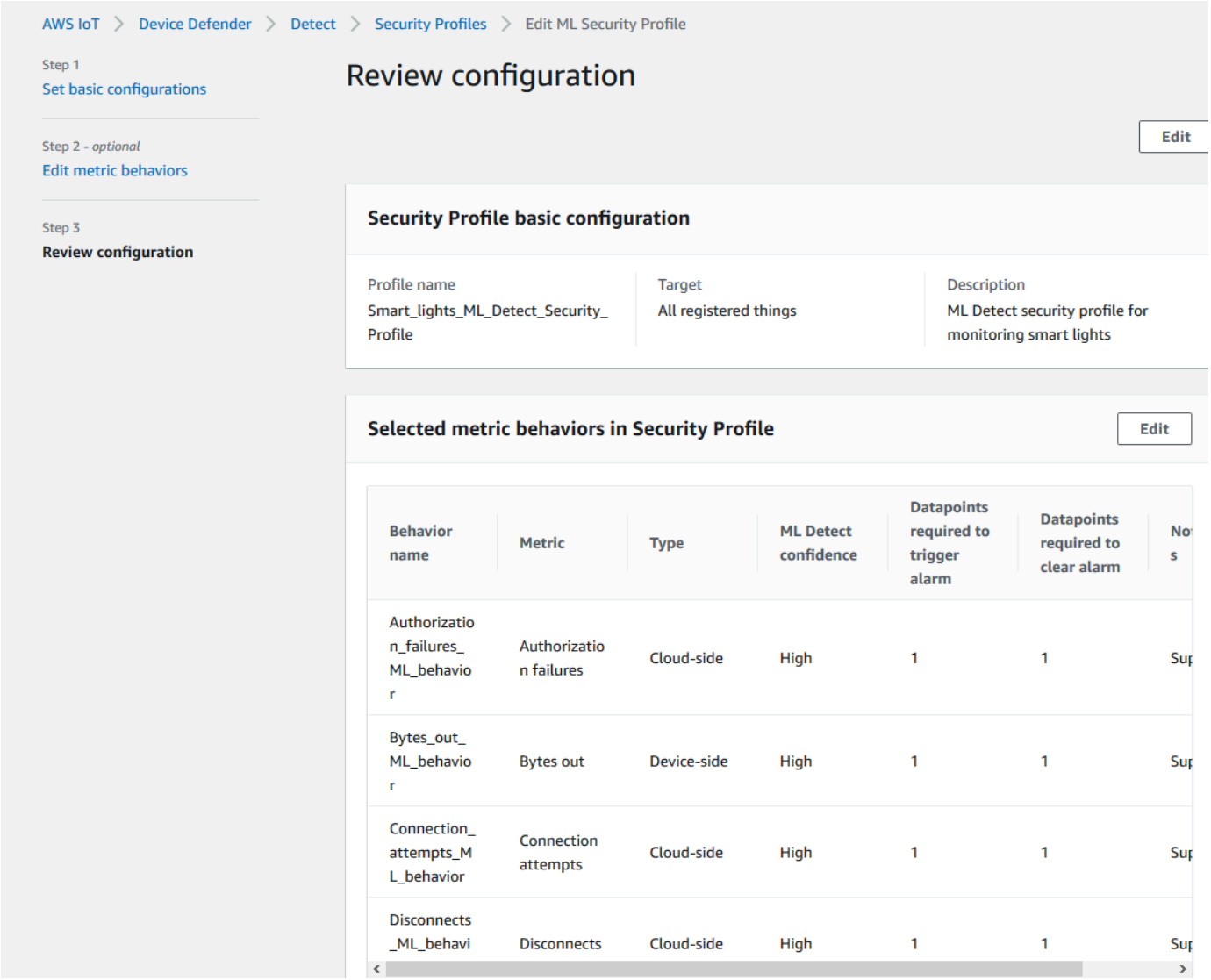


5. En la página Editar los comportamientos de las métricas, puede personalizar la configuración del comportamiento del machine learning.



6. Cuando haya terminado, elija Siguiente.

7. En la página Revisar la configuración, compruebe los comportamientos que quiera que monitorice el machine learning y, a continuación, seleccione Siguiente.



8. Una vez creado el perfil de seguridad, se le redirigirá a la página Perfiles de seguridad, donde aparecerá el perfil de seguridad recién creado.

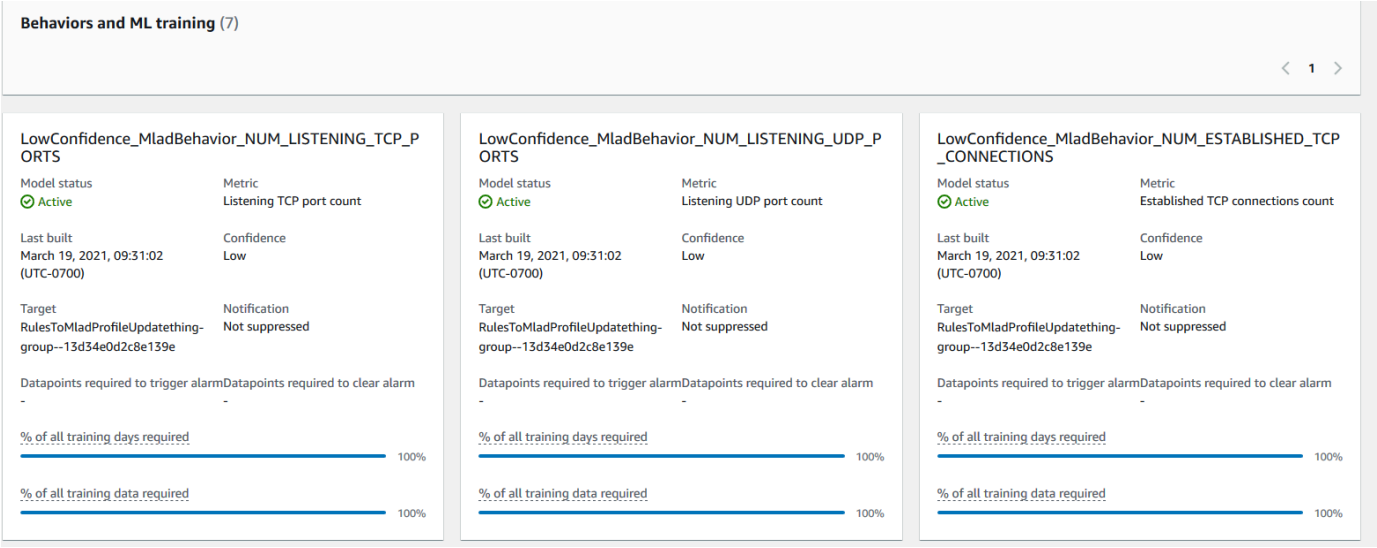
> **Note**
>
> La formación y la creación iniciales del modelo de machine learning tardan 14 días en completarse. Si hay alguna actividad anómala en sus dispositivos, verá las alarmas una vez que se haya completado el proceso.

Monitorizar el estado de su modelo de machine learning

Mientras sus modelos de machine learning se encuentran en el período de formación inicial, puede monitorizar su progreso en cualquier momento siguiendo estos pasos.

1. En la consola de AWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Detect, Perfiles de seguridad.
2. En la página Perfiles de seguridad, elija el perfil de seguridad que quiera revisar. A continuación, seleccione Comportamientos y entrenamiento de machine learning.
3. En la página Comportamientos y entrenamiento de machine learning, compruebe el progreso del entrenamiento de sus modelos de machine learning.

   Cuando el estado del modelo sea Activo, empezará a tomar decisiones de detección en función de su uso y actualizará el perfil todos los días.

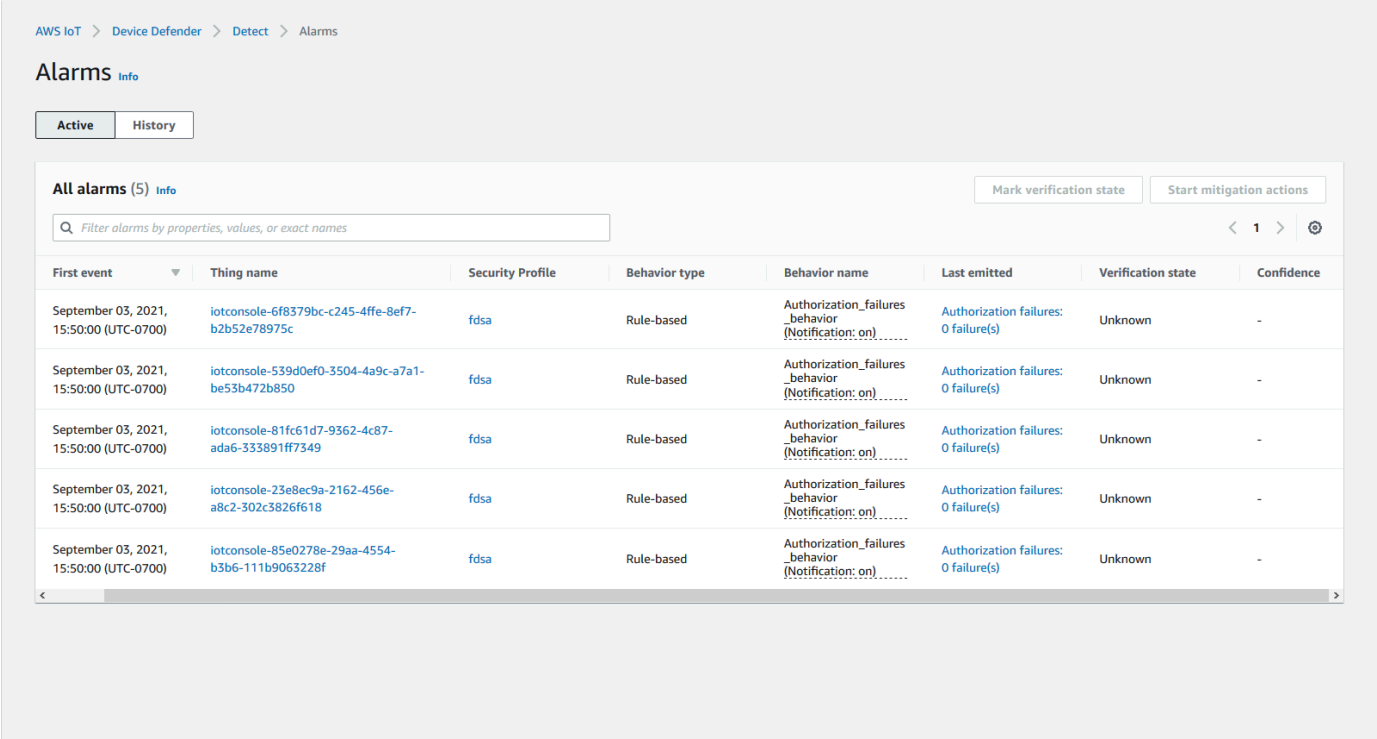


> **Note**
>
> Si su modelo no progresa según lo esperado, asegúrese de que tus dispositivos cumplen los Requisitos mínimos.

Revisar las alarmas de ML Detect

Una vez que sus modelos de machine learning estén diseñados y listos para la inferencia de datos, podrá ver e investigar periódicamente las alarmas que identifiquen los modelos.

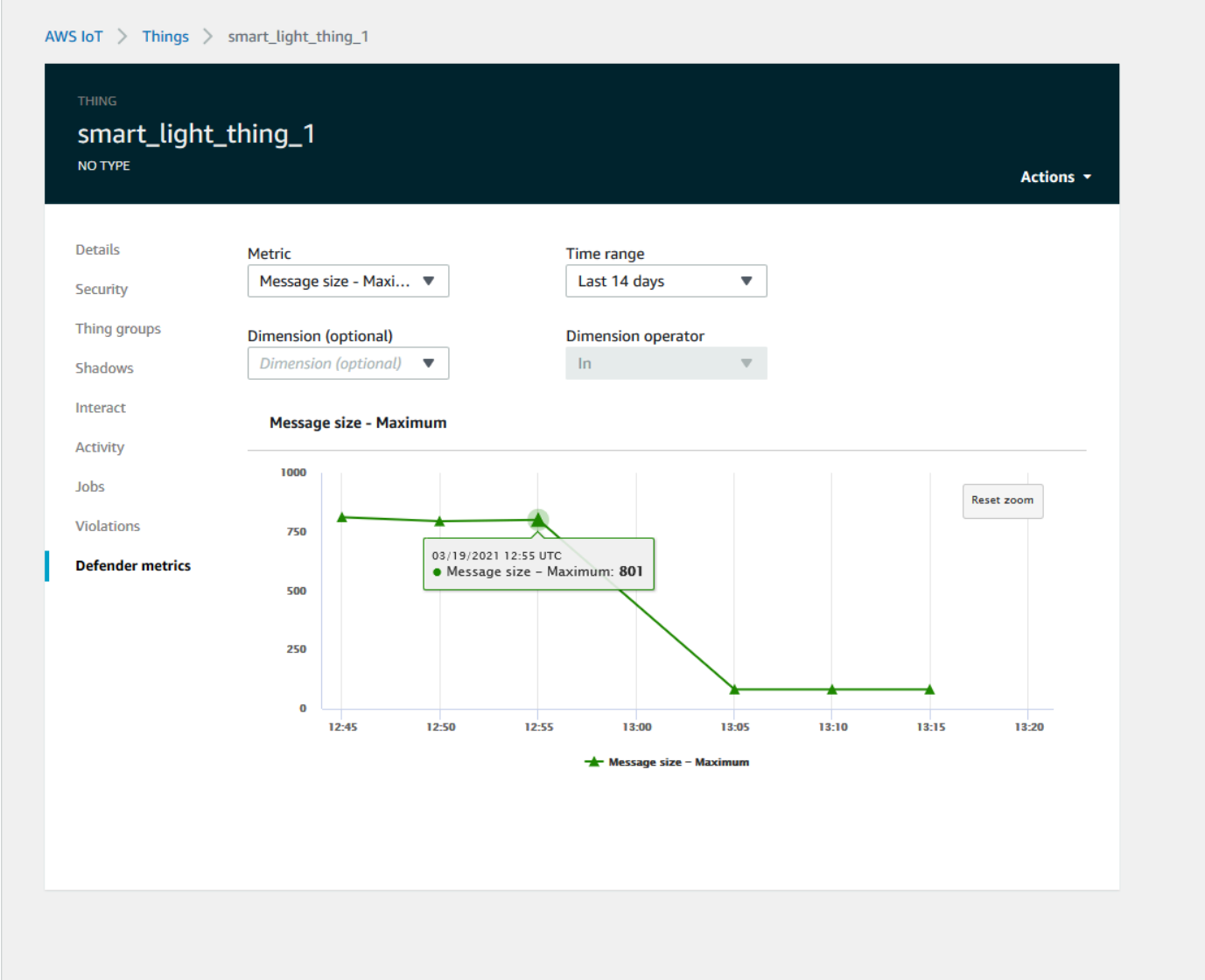
1. En la consola deAWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Detect y luego elija Alarmas.



2. Si accede a la pestaña Historial, también puede ver los detalles de los dispositivos que ya no aparecen en las alarmas.

Para obtener más información, en Administrar, seleccione Objetos, elija el objeto del que quiera ver más detalles y, a continuación, vaya hasta Métricas de Defender. Desde la pestaña Activo,

puede acceder al gráfico de métricas de Defender e investigar cualquier cosa que dé señales de alarma. En este caso, el gráfico muestra un aumento en el tamaño del mensaje, lo que provocó la alarma. Puede ver que la alarma se borró posteriormente.

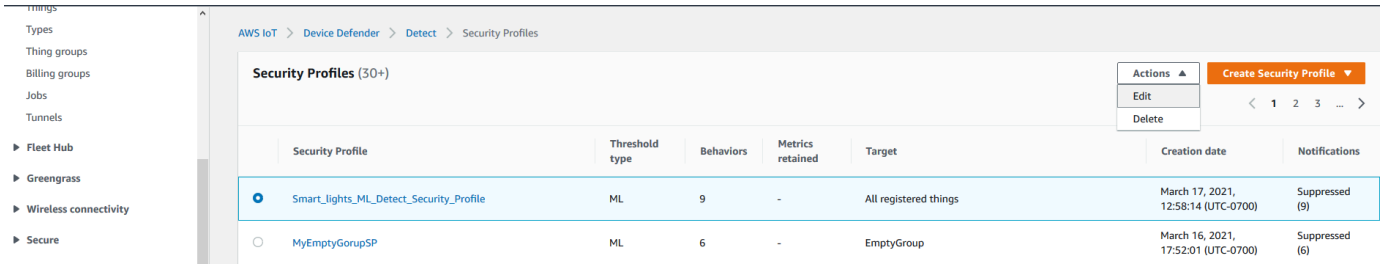


Ajustar sus alarmas de machine learning

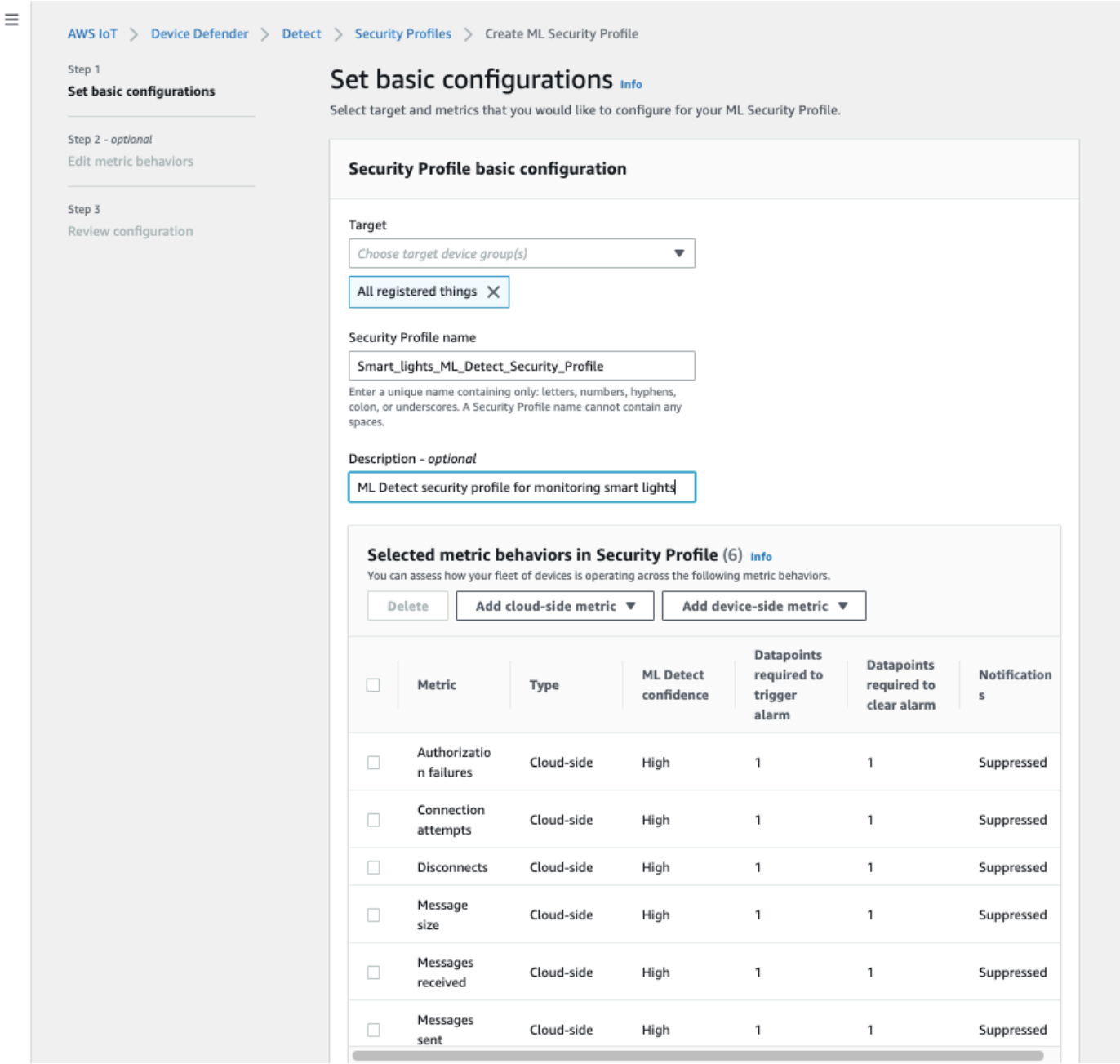
Una vez que sus modelos de machine learning estén diseñados y listos para la evaluación de los datos, puede actualizar los ajustes de comportamiento del machine learning de su perfil de seguridad para cambiar la configuración. En el siguiente procedimiento se muestra cómo actualizar la configuración de comportamiento de machine learning del perfil de seguridad en la AWS CLI.

1. En la consola de AWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Detect, Perfiles de seguridad.

2. En la página Perfiles de seguridad, marque la casilla situada junto al perfil de seguridad que quiera revisar. Luego elija Acciones y Editar.

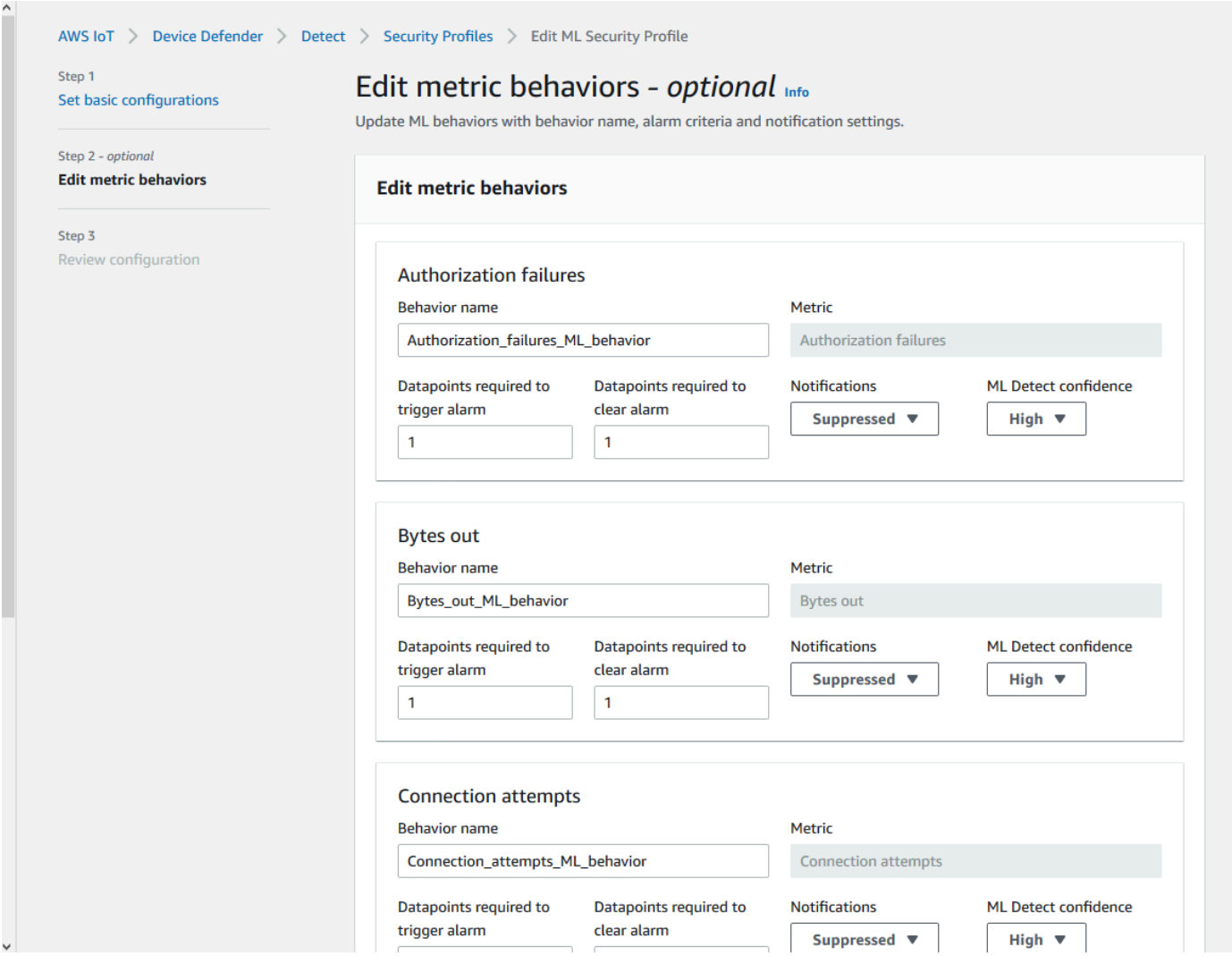


3. En Establecer configuraciones básicas, puede ajustar los grupos de destino de los perfiles de seguridad o cambiar las métricas que quiera monitorizar.



4. Para actualizar cualquiera de las siguientes opciones, vaya a Editar los comportamientos de las métricas.

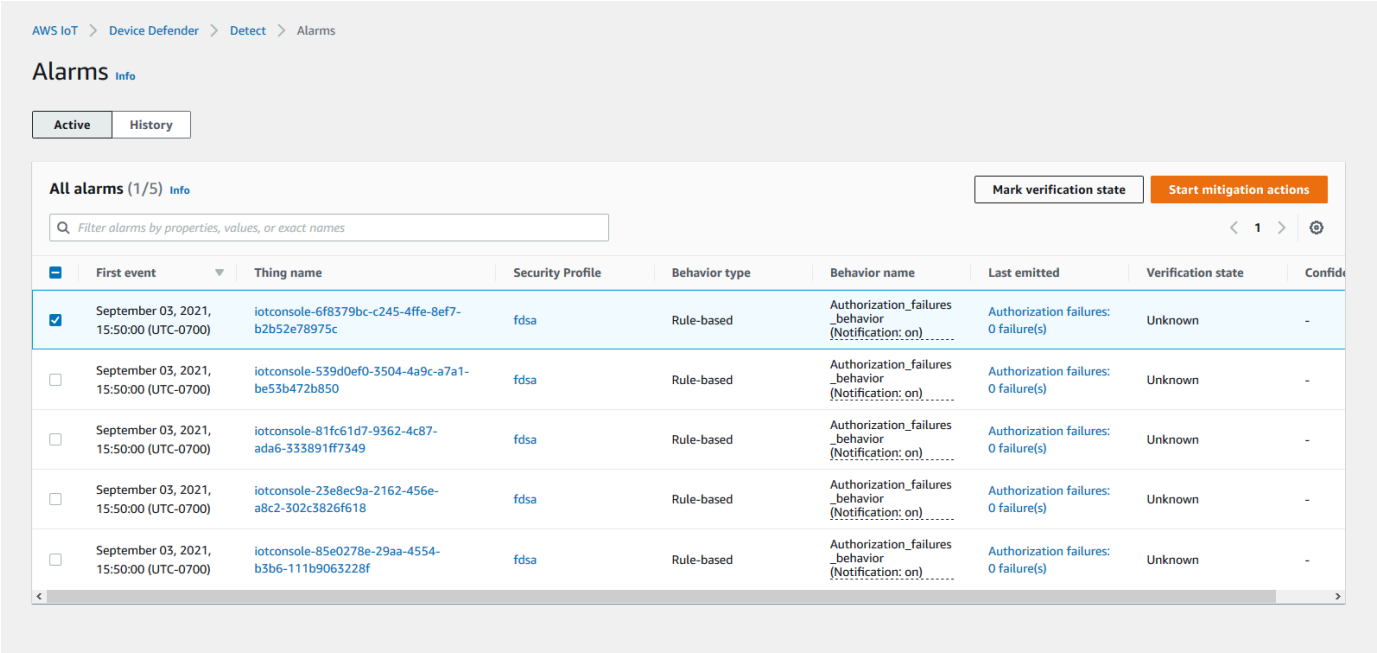
   - Los puntos de datos de su modelo de machine learning son necesarios para iniciar la alarma
   - Los puntos de datos de su modelo de machine learning son necesarios para borrar la alarma
   - Su nivel de confianza en ML Detect
   - Sus notificaciones de ML Detect (por ejemplo, No suprimidas, Suprimidas)



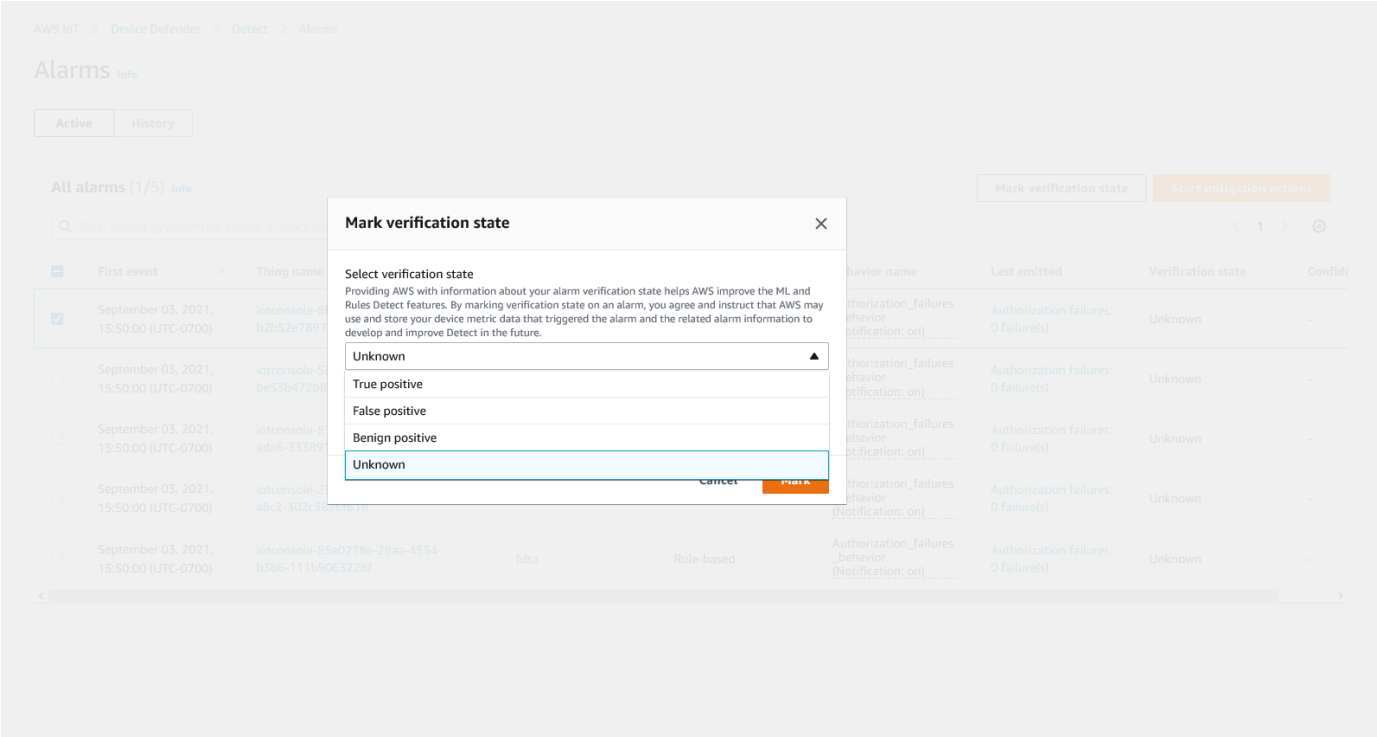
Marcar el estado de verificación de su alarma

Marque sus alarmas configurando el estado de verificación y proporcionando una descripción de ese estado de verificación. Esto le ayudará a usted y a su equipo a identificar las alarmas a las que no tengan que responder.

1. En la consola deAWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Detect y luego elija Alarmas. Seleccione una alarma para marcar su estado de verificación.



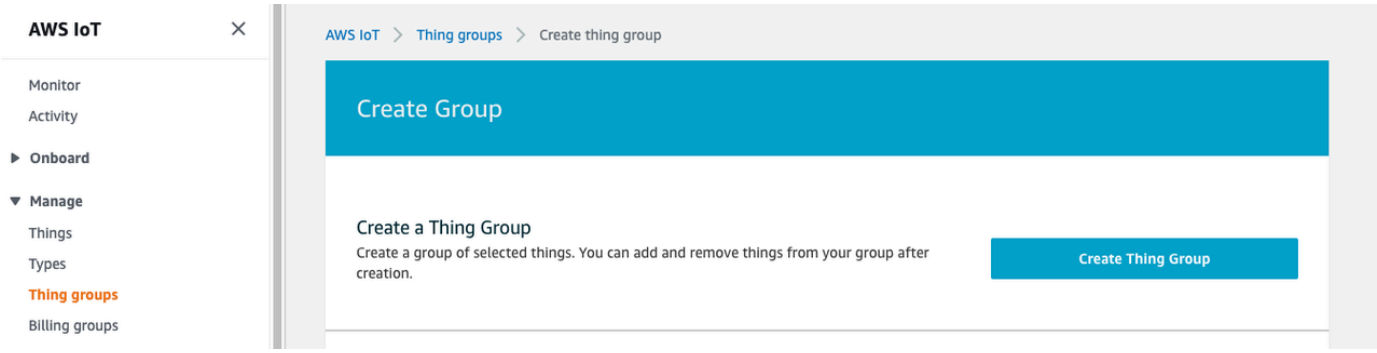
2. Seleccione Marcar el estado de verificación. Se abre la ventana emergente de estado de verificación.
3. Elija el estado de verificación adecuado, introduzca una descripción de verificación (opcional) y, a continuación, seleccione Marcar. Esta acción asigna un estado de verificación y una descripción a la alarma elegida.



Mitigar los problemas identificados en los dispositivos

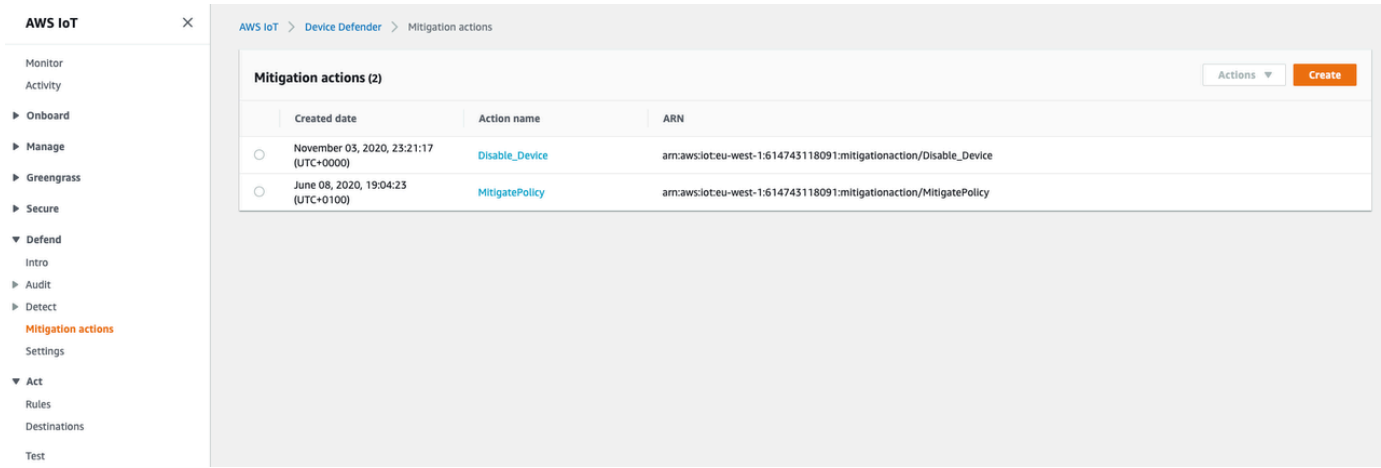
1. (Opcional) Antes de configurar las acciones de mitigación de la cuarentena, vamos a configurar un grupo de cuarentena al que trasladaremos el dispositivo que infrinja la norma. También puede utilizar un grupo que ya exista.
2. Vaya a Administrar, Grupos de objetos y, a continuación, Crear grupo de objetos. Asigne un nombre al grupo de objetos. En este tutorial, asignaremos un nombre a nuestro grupo de objetos `Quarantine_group`. En Grupo de objetos, Seguridad, aplique la siguiente política al grupo de objetos.

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



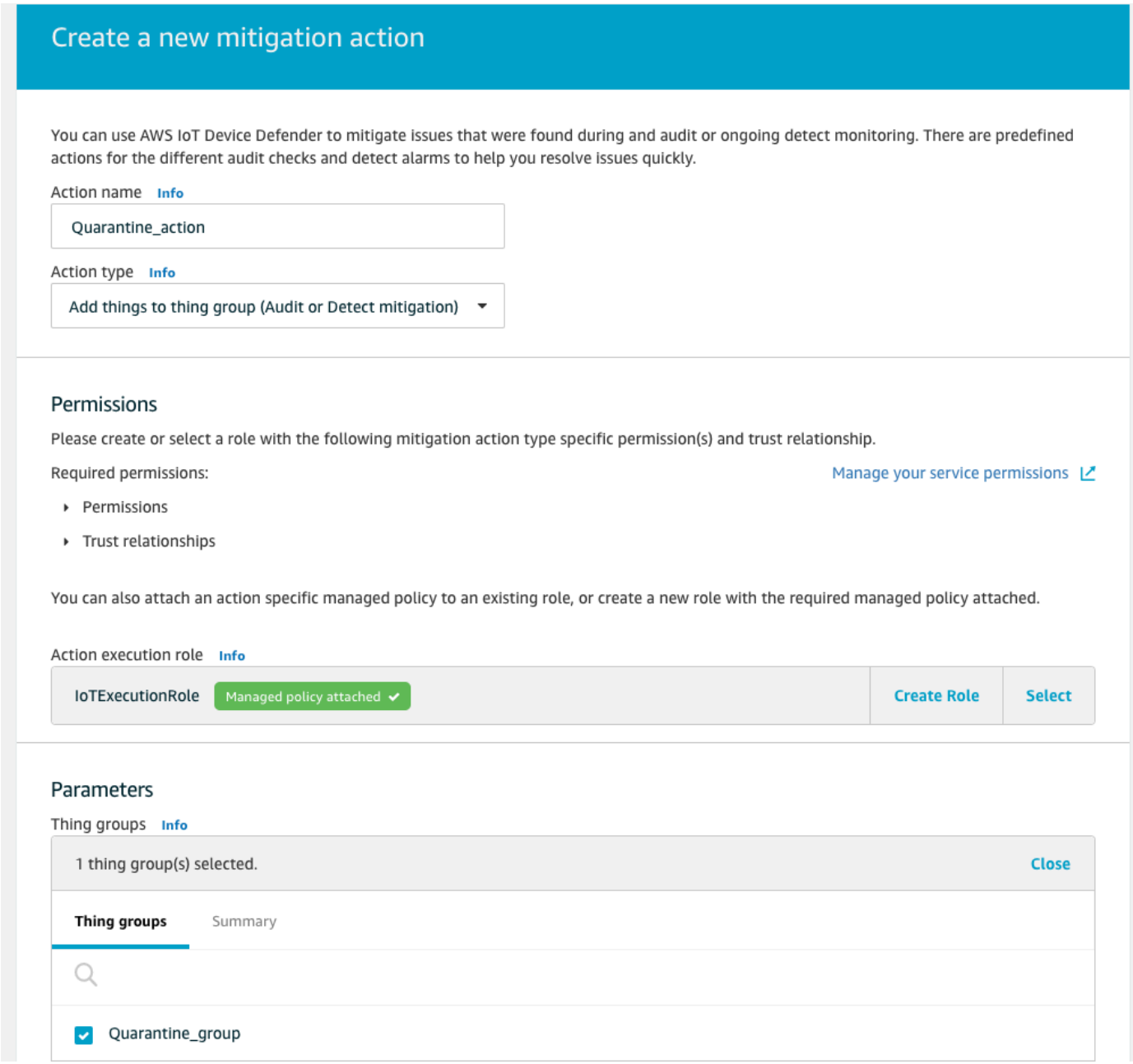
   Cuando haya terminado, elija Crear grupo de objetos.
3. Ahora que hemos creado un grupo de objetos, vamos a crear una acción de mitigación que mueva los dispositivos que estén en estado de alarma a `Quarantine_group`.

   En Defender, Acciones de mitigación, seleccione Crear.



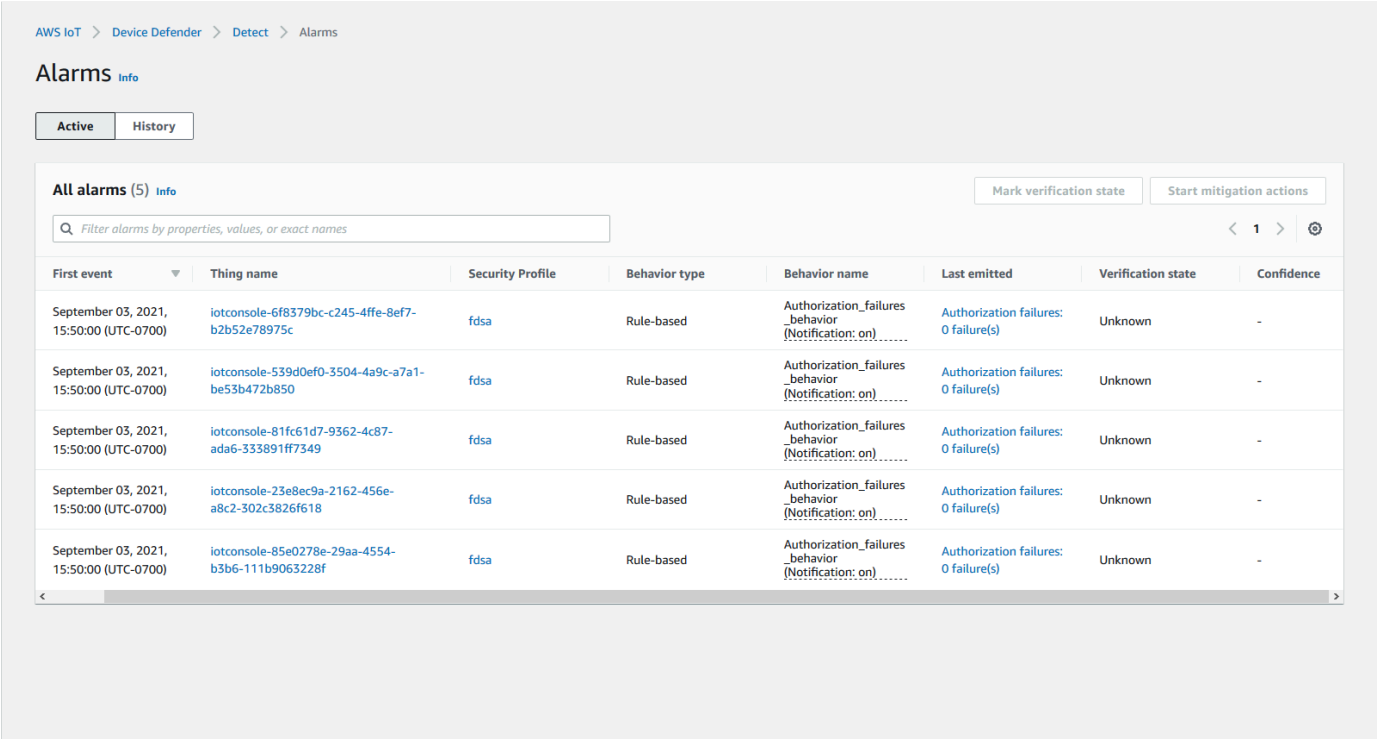
4. En la página Crear una nueva acción de mitigación, especifique la siguiente información.

   - Nombre de acción: asigne un nombre a la acción de mitigación, por ejemplo, **`Quarantine_action`**.
   - Tipo de acción: elija el tipo de acción. Vamos a elegir Agregar objetos al grupo de objetos (mitigación de auditoría o detección).
   - Papel de ejecución de acción: cree un rol o elija uno existente si ya lo creó anteriormente.
   - Parámetros: elija un grupo de objetos. Podemos usar el `Quarantine_group` que hemos creado anteriormente.



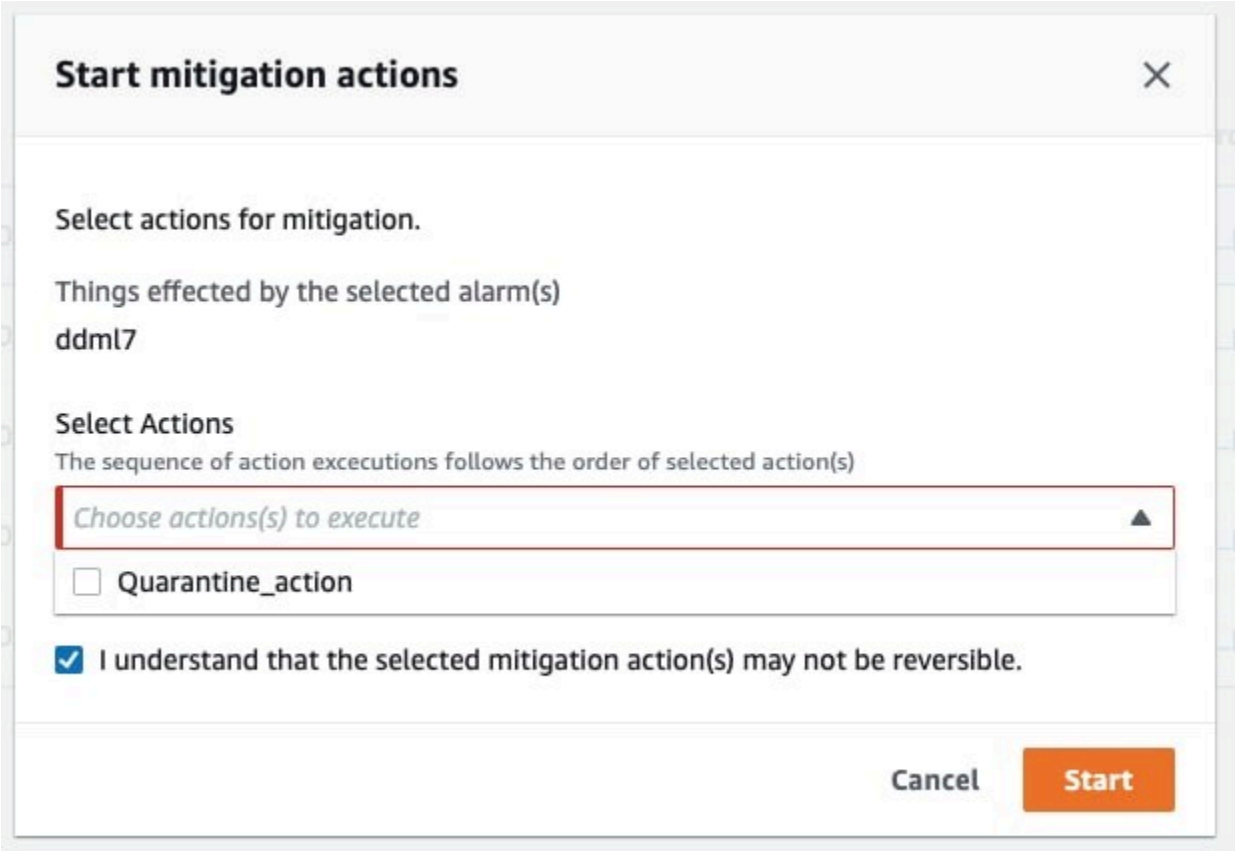
Cuando haya terminado, elija Guardar. Ahora dispone de una acción de mitigación que traslada los dispositivos en estado de alarma a un grupo de cuarentena y de una acción de mitigación que aísla el dispositivo mientras investiga.

5. Vaya a Defend, Detect y Alarmas. Puede ver qué dispositivos están en estado de alarma en Activo.

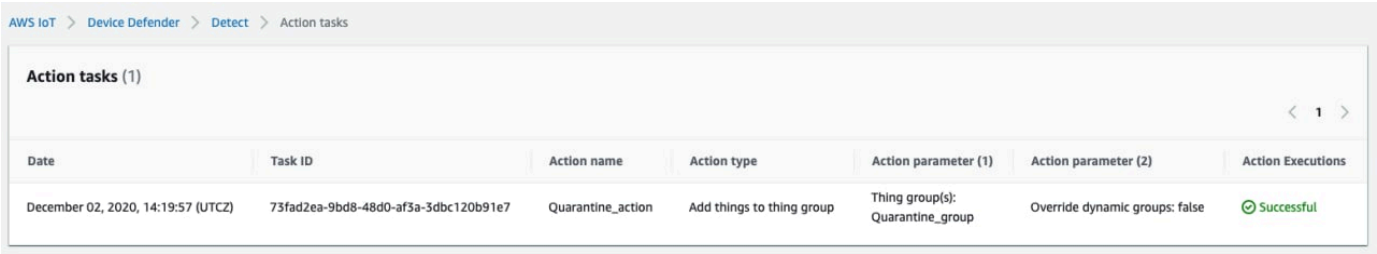


Seleccione el dispositivo que quiera mover al grupo de cuarentena y elija Iniciar acciones de mitigación.

6. En Iniciar acciones de mitigación, Iniciar acciones, seleccione la acción de mitigación que creó anteriormente. Por ejemplo, elegiremos **`Quarantine_action`** y, a continuación, seleccionaremos Iniciar. Se abrirá la página Tareas de acción.



7. El dispositivo ahora está aislado en **`Quarantine_group`** y puede investigar la causa raíz del problema que activó la alarma. Una vez finalizada la investigación, puede sacar el dispositivo del grupo de objetos o tomar otras medidas.



Cómo usar ML Detect con la CLI

A continuación, se muestra cómo configurar ML Detect mediante la CLI.

Tutoriales

- Habilitar ML Detect
- Monitorizar el estado de su modelo de machine learning

- Revisar las alarmas de ML Detect
- Ajustar sus alarmas de machine learning
- Marcar el estado de verificación de su alarma
- Mitigar los problemas identificados en los dispositivos

Habilitar ML Detect

En el siguiente procedimiento se muestra cómo habilitar ML Detect en la AWS CLI.

1. Asegúrese de que sus dispositivos creen los puntos de datos mínimos necesarios, tal como se definen en los requisitos mínimos de ML Detect para la formación continua y la actualización del modelo. Para que la recopilación de datos progrese, asegúrese de que sus objetos están en un grupo de objetos asociado a un perfil de seguridad.
2. Cree un perfil de seguridad de ML Detect utilizando el comando `create-security-profile`. El siguiente ejemplo crea un perfil de seguridad denominado *`security-profile-for-smart-lights`* que comprueba el número de mensajes enviados, el número de errores de autorización, el número de intentos de conexión y el número de desconexiones. El ejemplo utiliza `mlDetectionConfig` para establecer que la métrica utilizará el modelo de 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
  }]'
```

Salida:

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

3. A continuación, asocie su perfil de seguridad a uno o varios grupos de objetos. Utilice el comando `attach-security-profile` para asociar un grupo de objetos a su perfil de seguridad. El siguiente ejemplo asocia un grupo de objetos denominado

ML_Detect_beta_static_group con el perfil de seguridad *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
```

Salida:

Ninguna.

4. Una vez que haya creado su perfil de seguridad completo, el modelo de machine learning comienza a entrenarse. La formación y la creación iniciales del modelo de machine learning tardan 14 días en completarse. Después de 14 días, si hay actividad anómala en su dispositivo puede esperar ver alarmas.

Monitorizar el estado de su modelo de machine learning

En el siguiente procedimiento se muestra cómo monitorizar el entrenamiento en curso de modelos de machine learning.

- Utilice el comando `get-behavior-model-training-summaries` para ver el progreso de su modelo de machine learning. En el siguiente ejemplo, se obtiene el resumen del progreso del entrenamiento del modelo de machine learning para el perfil de seguridad *security-profile-for-smart-lights*. `modelStatus` muestra si un modelo ha completado el entrenamiento o aún está pendiente de crearse para un comportamiento en particular.

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

Salida:

```
{
    "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**
>
> Si su modelo no progresa según lo esperado, asegúrese de que tus dispositivos cumplen los Requisitos mínimos.

Revisar las alarmas de ML Detect

Una vez que sus modelos de machine learning estén construidos y listos para las evaluaciones de datos, podrá ver periódicamente las alarmas inferidas por los modelos. El siguiente procedimiento le muestra cómo ver sus alarmas en la AWS CLI.

- Para ver todas las alarmas activas, utilice el comando `list-active-violations`.

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

  Salida:

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

  Como alternativa, puede ver todas las infracciones descubiertas durante un período de tiempo determinado mediante el comando `list-violation-events`. En el siguiente ejemplo se enumeran las infracciones ocurridas entre el 22 de septiembre de 2020 a las 05:42:13 GMT y el 26 de octubre de 2020 a las 5:42:13 GMT.

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

  Salida:

  ```
  {
      "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"
}
```

Ajustar sus alarmas de machine learning

Una vez que sus modelos de machine learning estén diseñados y listos para la evaluación de los datos, puede actualizar los ajustes de comportamiento del machine learning de su perfil de seguridad para cambiar la configuración. En el siguiente procedimiento se muestra cómo actualizar la configuración de comportamiento de machine learning del perfil de seguridad en la AWS CLI.

- Para cambiar la configuración del comportamiento de machine learning de su perfil de seguridad, utilice el comando `update-security-profile`. El siguiente ejemplo actualiza los comportamientos del perfil de seguridad de *`security-profile-for-smart-lights`* cambiando el `confidenceLevel` de algunos de los comportamientos y desactivando las notificaciones de todos los comportamientos.

```
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

  }]'
```

Salida:

```
 {
    "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
}
```

Marcar el estado de verificación de su alarma

Puede marcar sus alarmas con estados de verificación para ayudar a clasificar las alarmas e investigar las anomalías.

- Marque las alarmas con un estado de verificación y una descripción de ese estado. Por ejemplo, para establecer el estado de verificación de una alarma en falso positivo, utilice el siguiente 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
```

Salida:

Ninguna.

Mitigar los problemas identificados en los dispositivos

1. Utilice el comando `create-thing-group` para crear un grupo de objetos para la acción de mitigación. En el siguiente ejemplo vamos a crear un grupo de objetos denominado ThingGroupForDetectMitigationAction.

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

Salida:

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

2. A continuación utilice el comando `create-mitigation-action` para crear una acción de mitigación. En el siguiente ejemplo, creamos una acción de mitigación llamada detect_mitigation_action con el ARN del rol de IAM que se usa para aplicar la acción de mitigación. También definimos el tipo de acción y los parámetros de dicha acción. En este caso, nuestra mitigación moverá los objetos a nuestro grupo de objetos creado anteriormente, denominado ThingGroupForDetectMitigationAction.

```
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
    }
}'
```

Salida:

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

3. Use el comando `start-detect-mitigation-actions-task` para iniciar la tarea de acciones de mitigación. `task-id`, `target` y `actions` son parámetros obligatorios.

```
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
```

Salida:

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

4. (Opcional) Para ver las ejecuciones de las acciones de mitigación incluidas en una tarea, utilice el comando `list-detect-mitigation-actions-executions`.

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

Salida:

```
{
    "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. (Opcional) Utilice el comando `describe-detect-mitigation-actions-task` para obtener información sobre una tarea de acción de mitigación.

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

Salida:

```
{
    "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. (Opcional) Para obtener una lista de sus tareas de acción de mitigación, utilice el 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
```

Salida:

```
{
    "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. (Opcional) Para cancelar una tarea de acciones de mitigación, utilice el comando `cancel-detect-mitigation-actions-task`.

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

Salida:

Ninguna.

Personalizar cuándo y cómo ver los resultados de auditoría de AWS IoT Device Defender

La auditoría de AWS IoT Device Defender proporciona controles de seguridad periódicos para confirmar que los dispositivos y los recursos de AWS IoT siguen las prácticas recomendadas. Para

cada comprobación, los resultados de auditoría se clasifican en conformes o no conformes, mientras que en caso de incumplimiento aparecen iconos de advertencia en la consola. Para reducir el ruido provocado por la repetición de problemas conocidos, la función de supresión de resultados de auditoría permite silenciar temporalmente estas notificaciones de incumplimiento.

Puede suprimir determinadas comprobaciones de auditoría para un recurso o una cuenta específicos durante un período de tiempo predeterminado. El resultado de una comprobación de auditoría que se ha suprimido se clasifica como resultado suprimido, independientemente de las categorías de conformidad y no conformidad. Esta nueva categoría no activa una alarma como si se tratara de un resultado no conforme. Esto le permite reducir las interrupciones en las notificaciones de incumplimiento durante los períodos de mantenimiento conocidos o hasta que esté programada la finalización de una actualización.

Introducción

En las siguientes secciones se detalla cómo puede utilizar las supresiones de los resultados de auditoría para suprimir una comprobación de `Device certificate expiring`en la consola y en la CLI. Si desea seguir alguna de las demostraciones, primero debe crear dos certificados que venzan para que Device Defender los detecte.

Use lo siguiente para crear sus certificados.

- Crear y registrar un certificado de CA, en la Guía para desarrolladores de AWS IoT Core
- Cree un certificado de cliente mediante el certificado de entidad de certificación. En el paso 3, defina su parámetro `days` en **1**.

Si usa la CLI para crear los certificados, escriba el comando siguiente.

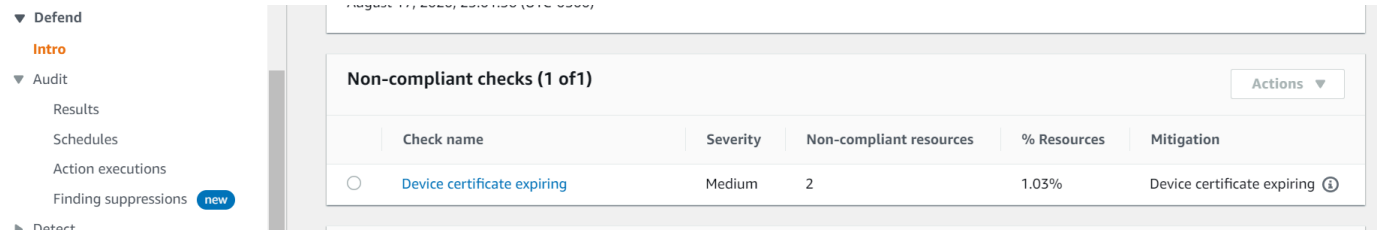
```
openssl x509 -req \
    -in device_cert_csr_filename \
    -CA root_ca_pem_filename \
    -CAkey root_ca_key_filename \
    -CAcreateserial \
    -out device_cert_pem_filename \
    -days 1 -sha256
```

Personalización de los resultados de la auditoría en la consola

En el siguiente tutorial, se utiliza una cuenta con dos certificados de dispositivo caducados que provocan una comprobación de auditoría no conforme. En este escenario, queremos deshabilitar la advertencia porque nuestros desarrolladores están probando una característica que solucionará el problema. Creamos una supresión de resultados de auditoría para cada certificado con el fin de evitar que el resultado de la auditoría no sea conforme durante la semana siguiente.

1. En primer lugar, realizaremos una auditoría bajo demanda para comprobar que la comprobación del certificado del dispositivo caducado no es conforme.

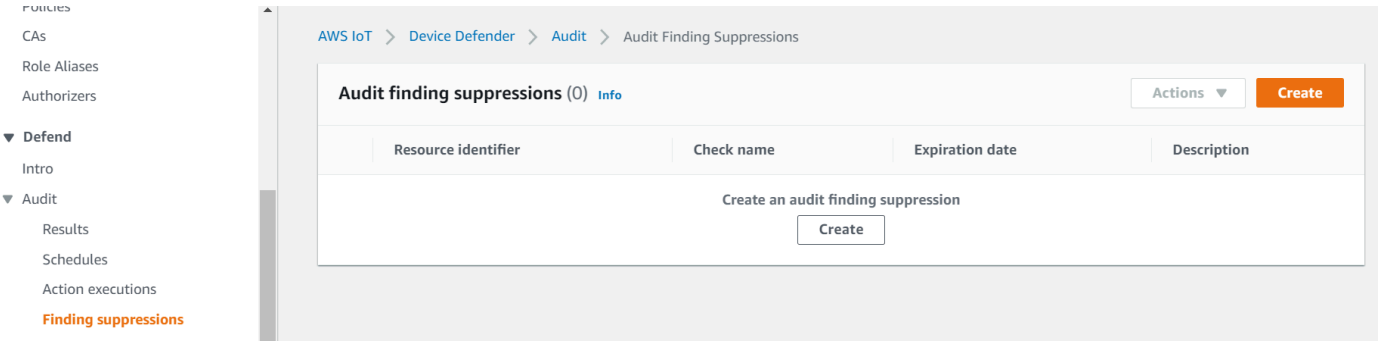
   En la consola de AWS IoT, elija Defend en la barra lateral izquierda, luego Audit y después Resultados. En la página Resultados de auditoría, seleccione Crear. Se abrirá la ventana Crear una auditoría nueva. Seleccione Crear.



   A partir de los resultados de la auditoría bajo demanda, podemos ver que la expresión «El certificado de dispositivo está caducando» no es compatible con dos recursos.

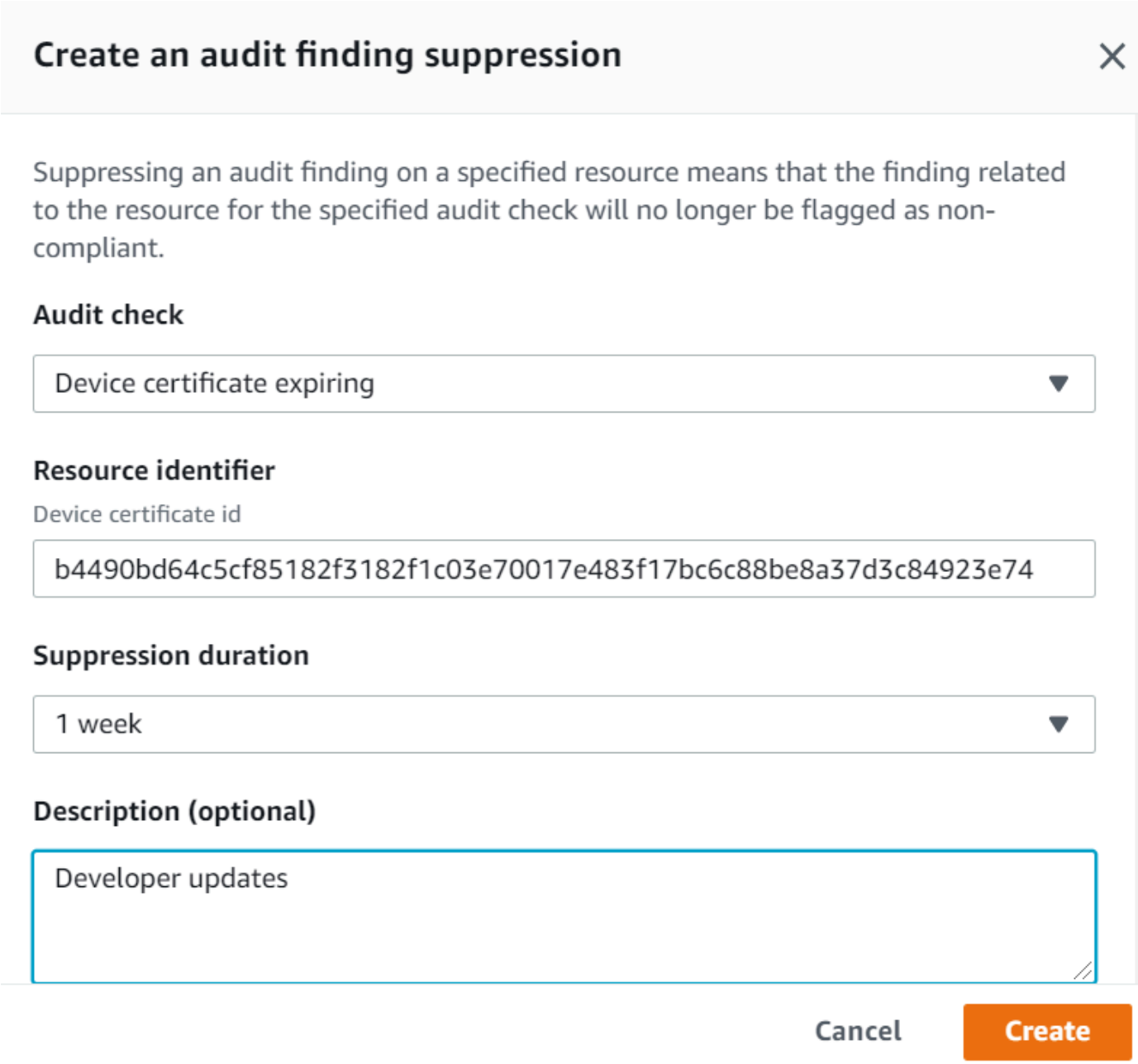
2. Ahora, queremos desactivar la advertencia de verificación de no conformidad que indica que el certificado del dispositivo está caducando, ya que nuestros desarrolladores están probando nuevas características para corregir esta advertencia.

   En la barra lateral izquierda, debajo de Defend, elija Audit y, a continuación, Supresiones de resultados. En la página Supresiones de resultados de la auditoría, seleccione Crear.



3. En la ventana Crear una supresión de resultados de la auditoría, necesitamos rellenar lo siguiente.

- Comprobación de auditoría: seleccionamos `Device certificate expiring` porque es la verificación de auditoría que queremos suprimir.
- Identificador de recursos: introducimos el identificador del certificado del dispositivo de uno de los certificados cuyos resultados de auditoría queremos suprimir.
- Duración de la supresión: seleccionamos `1 week` porque ese es el tiempo durante el que queremos suprimir la comprobación de auditoría de `Device certificate expiring`.
- Descripción (opcional): agregamos una nota que describe por qué estamos suprimiendo este resultado de auditoría.

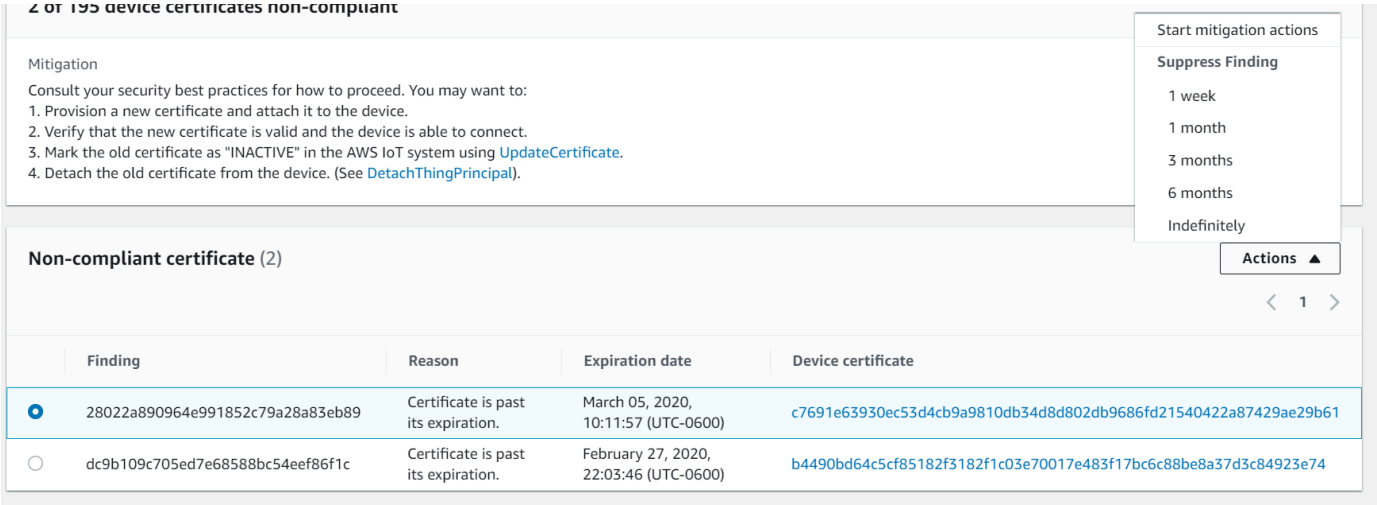


Tras de completar los campos, elija Crear. Vemos un banner indicando que se ha realizado todo correctamente después de que se haya creado la supresión de resultados de la auditoría.

4. Hemos suprimido el resultado de una auditoría para uno de los certificados y ahora necesitamos suprimir el resultado de la auditoría del segundo certificado. Podríamos utilizar el mismo método de supresión que utilizamos en el paso 3, pero utilizaremos un método diferente con fines de demostración.

En la barra lateral izquierda, debajo de Defend, elija Audit y, a continuación, Resultados. En la página Resultados de auditoría, elija la auditoría con el recurso no conforme. A continuación, seleccione el recurso en Comprobaciones de no conformidad. En nuestro caso, seleccionamos «Certificado de dispositivo que va a caducar».

5. En la página Certificado de dispositivo que va a caducar, en Política no conforme, seleccione el botón de opción situado junto al resultado que quiera suprimir. A continuación, seleccione el menú desplegable Acciones y luego elija el tiempo durante el que quiere que se suprima el resultado. En nuestro caso, elegimos `1 week` como hicimos con el otro certificado. En la ventana Confirme la supresión, seleccione Habilite la supresión.



Vemos un banner indicando que se ha realizado todo correctamente después de que se haya creado la supresión de resultados de la auditoría. Ahora, los dos resultados de la auditoría se han ocultado durante una semana mientras nuestros desarrolladores trabajan en una solución que aborde la advertencia.

Personalización de los resultados de la auditoría en la CLI

En el siguiente tutorial, se utiliza una cuenta con un certificado de dispositivo caducado que provoca una comprobación de auditoría no conforme. En este escenario, queremos deshabilitar la advertencia porque nuestros desarrolladores están probando una característica que solucionará el problema. Creamos una supresión de resultados de auditoría para el certificado con el fin de evitar que el resultado de la auditoría no sea conforme durante la semana siguiente.

Utilizamos los siguientes comandos de la CLI.

- create-audit-suppression

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

1. Utilice el siguiente comando para activar la auditoría.

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

   Salida:

   Ninguna.

2. Utilice el siguiente comando para ejecutar una auditoría bajo demanda dirigida a la comprobación de auditoría de `DEVICE_CERTIFICATE_EXPIRING_CHECK`.

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

   Salida:

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

3. Utilice el comando describe-account-audit-configuration para describir la configuración de la auditoría. Queremos confirmar que hemos activado la comprobación de auditoría para `DEVICE_CERTIFICATE_EXPIRING_CHECK`.

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

   Salida:

```
{
    "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` debe tener un valor de `true`.

4. Utilice el comando list-audit-task para identificar las tareas de auditoría completadas.

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

Salida:

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

El `taskId` de la auditoría que ejecutó en el paso 1 debe tener un `taskStatus` de `COMPLETED`.

5. Utilice el comando describe-audit-task para obtener detalles sobre la auditoría completada utilizando el resultado `taskId` del paso anterior. Este comando muestra los detalles de la auditoría.

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

Salida:

```
{
```

```
    "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. Utilice el comando list-audit-findings para buscar el identificador de certificado que no cumple los requisitos para que podamos suspender las alertas de auditoría de este recurso.

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

Salida:

```
{
    "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. Utilice el comando create-audit-suppression para suprimir las notificaciones de la comprobación de auditoría de `DEVICE_CERTIFICATE_EXPIRING_CHECK` de un certificado de dispositivo con el identificador *`c7691e<shortened>`* hasta el *`20-08-2022`*

```
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. Utilice el comando list-audit-suppression para confirmar la configuración de supresión de la auditoría y obtener detalles sobre la supresión.

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

Salida:

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

9. El comando update-audit-suppression se puede utilizar para actualizar la supresión de resultados de la auditoría. En el siguiente ejemplo, se actualiza el `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. El comando delete-audit-suppression se puede utilizar para eliminar la supresión de un resultado de auditoría.

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

Para confirmar la eliminación, utilice el comando list-audit-suppressions.

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

Salida:

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

En este tutorial, le mostramos cómo suprimir una comprobación de `Device certificate expiring` en la consola y en la CLI. Para obtener más información acerca de las supresiones de resultados de la auditoría, consulte Supresiones de resultados de auditoría.

Auditoría

Una auditoría de AWS IoT Device Defender examina la configuración y las políticas relacionadas con una cuenta y dispositivo para garantizar que existen medidas de seguridad. Las auditorías pueden ayudarle a detectar cualquier desviación con respecto a las prácticas recomendadas de seguridad o a las políticas de acceso adecuadas (por ejemplo, cuando varios dispositivos usan la misma identidad o cuando existen políticas excesivamente permisivas que permiten a un dispositivo leer y actualizar datos de muchos otros dispositivos). Puede ejecutar auditorías según sean necesarias (auditorías bajo demanda) o programarlas para que se ejecuten periódicamente (auditorías programadas).

Una auditoría de AWS IoT Device Defender realiza una serie de comprobaciones predefinidas relacionadas con las prácticas recomendadas de seguridad de IoT comunes y las vulnerabilidades de los dispositivos. Entre las comprobaciones se incluyen las políticas que conceden permiso para leer o actualizar datos en varios dispositivos, los dispositivos que comparten una identidad (certificado X.509), o los certificados que van a caducar o que se han revocado pero siguen activos.

Gravedad del problema

La gravedad del problema indica el nivel de gravedad asociado con cada caso identificado de incumplimiento y el tiempo recomendado para remediarlo.

Critico

Las comprobaciones de auditoría no conformes con esta gravedad identifican los problemas que requieren atención inmediata. Los problemas críticos permiten a menudo a los agentes malintencionados obtener fácilmente acceso a sus recursos o controlarlos sin demasiada sofisticación y sin disponer de información privilegiada o credenciales especiales.

Alta

Las comprobaciones de auditoría no conformes con esta gravedad requieren una investigación urgente y una planificación de remediación después de que se resuelvan los problemas críticos. Al igual que los problemas críticos, los problemas con gravedad alta suelen proporcionar los usuarios malintencionados acceso o control de sus recursos. Sin embargo, los problemas con gravedad alta suelen ser más difíciles de aprovechar. Es posible que requieran herramientas especiales, información privilegiada o configuraciones específicas.

Medio

Las comprobaciones de auditoría no conformes con esta gravedad presentan problemas que requieren atención como parte del mantenimiento continuo del estado de seguridad. Los problemas de gravedad media pueden causar un impacto operativo negativo, como interrupciones no planificadas debido a un mal funcionamiento de los controles de seguridad. Estos problemas también pueden proporcionar a los usuarios malintencionados acceso o control limitado a sus recursos, o pueden facilitar algunos pasos de sus acciones maliciosas.

Baja

Las comprobaciones de auditoría no conformes con esta gravedad suelen indicar que las prácticas recomendadas de seguridad se descuidaron o se pasaron por alto. Aunque pueden no causar un impacto inmediato en la seguridad, estos descuidos pueden ser aprovechados por usuarios con malas intenciones. Al igual que los problemas de gravedad media, los problemas de gravedad baja requieren atención como parte del mantenimiento continuo del estado de seguridad.

Siguientes pasos

Para conocer los tipos de comprobaciones de auditoría que se pueden realizar, consulte Comprobaciones de auditoría. Para obtener información sobre las cuotas de servicio que se aplican a las auditorías, consulte la sección Cuotas de servicio.

Comprobaciones de auditoría

> **Note**
>
> Cuando habilita una comprobación, la recopilación de datos comienza inmediatamente. Si tiene que recopilar una gran cantidad de datos en la cuenta, es posible que los resultados de la comprobación no estén disponibles durante cierto tiempo después de habilitarlos.

Es posible realizar las siguientes comprobaciones de auditoría:

- Se ha revocado la entidad de certificación intermedia para comprobar los certificados de los dispositivos activos
- El certificado de entidad de certificación revocado sigue activo

- Certificado de dispositivo compartido
- Calidad de la clave del certificado del dispositivo
- Calidad de la clave del certificado de entidad de certificación
- El rol de Cognito no autenticado es demasiado permisivo
- El rol de Cognito autenticado es demasiado permisivo
- Políticas de AWS IoT demasiado permisivas
- La política de AWS IoT está potencialmente mal configurada
- El alias de rol es demasiado permisivo
- El alias del rol permite el acceso a los servicios no utilizados
- El certificado de entidad de certificación está caducando
- Identificadores de cliente MQTT contradictorios
- El certificado de dispositivo está caducando
- Comprobación de la antigüedad del certificado del dispositivo
- Un certificado del dispositivo revocado sigue activo
- Registro desactivado

Se ha revocado la entidad de certificación intermedia para comprobar los certificados de los dispositivos activos

Utilice esta comprobación para identificar todos los certificados de dispositivos relacionados que siguen activos a pesar de haber revocado una entidad de certificación intermedia.

Esta comprobación aparece como `INTERMEDIATE_CA_REVOKED_FOR_ACTIVE_DEVICE_CERTIFICATES_CHECK` en la CLI y la API.

Gravedad: crítica

Detalles

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra una falta de conformidad:

- INTERMEDIATE_CA_REVOKED_BY_ISSUER

¿Por qué importa?

La entidad de certificación intermedia revocada para los certificados de dispositivo activos comprueba la identidad y la confianza del dispositivo, determinando si hay certificados de dispositivo activos en AWS IoT Core en los que las entidades de certificación intermedias hayan sido revocadas en la cadena de la entidad de certificación.

Una entidad de certificación intermedia revocada ya no debe utilizarse para firmar ningún otro certificado de entidad de certificación o dispositivo de la cadena de entidad de certificación. Los dispositivos recién agregados con certificados firmados con este certificado de entidad de certificación después de que se revoque la entidad de certificación intermedia supondrán una amenaza para la seguridad.

Cómo solucionarlo

Revise la actividad de registro del certificado de entidad de certificación del dispositivo durante el tiempo posterior a la revocación del certificado de entidad de certificación. Siga las prácticas recomendadas de seguridad para mitigar la situación. Es posible que desee:

1. Aprovisione nuevos certificados, firmados por una entidad de certificación diferente, para los dispositivos afectados.
2. Verifique que los nuevos certificados sean válidos y que los dispositivos puedan usarlos para conectarse.
3. Utilice UpdateCertificate para marcar el certificado antiguo como REVOCADO en AWS IoT. También puede utilizar acciones de mitigación para:
   - Aplicar la acción de mitigación `UPDATE_DEVICE_CERTIFICATE` en los resultados de la auditoría para realizar este cambio.
   - Aplicar la acción de mitigación `ADD_THINGS_TO_THING_GROUP` para agregar el dispositivo a un grupo en el que puede tomar medidas.
   - Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una respuesta personalizada en respuesta al mensaje de Amazon SNS.
   - Revise la actividad de registro de certificados de dispositivo realizada después de que se revocara el certificado de entidad de certificación intermedia y considere la posibilidad de revocar los certificados de dispositivo que se hayan podido emitir durante este período. Puede utilizar ListRelatedResourcesForAuditFinding para obtener una lista de los certificados de dispositivo firmados con el certificado de entidad de certificación y UpdateCertificate para revocar un certificado de dispositivo.

- Desvincular el certificado antiguo del dispositivo. (Consulte DetachThingPrincipal.)

Para obtener más información, consulte Acciones de mitigación.

El certificado de entidad de certificación revocado sigue activo

Se revocó un certificado de entidad de certificación pero sigue activo en AWS IoT.

Esta comprobación aparece como `REVOKED_CA_CERTIFICATE_STILL_ACTIVE_CHECK` en la CLI y la API.

Gravedad: crítica

Detalles

Un certificado de entidad de certificación está marcado como revocado en la lista de revocación de certificados mantenida por la entidad emisora, pero sigue marcado como “ACTIVE” o “PENDING_TRANSFER” en AWS IoT.

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra un certificado de entidad de certificación no conforme:

- CERTIFICATE_REVOKED_BY_ISSUER

¿Por qué importa?

Un certificado de entidad de certificación revocado no debe utilizarse nunca más para firmar certificados de dispositivos. Puede que se haya revocado porque ha sufrido un ataque. Los dispositivos agregados recientemente con certificados firmados con este certificado de entidad de certificación pueden constituir una amenaza para la seguridad.

Cómo solucionarlo

1. Utilice UpdateCACertificate para marcar el certificado de entidad de certificación como INACTIVO en AWS IoT. También puede utilizar acciones de mitigación para:
   - Aplicar la acción de mitigación `UPDATE_CA_CERTIFICATE` en los resultados de la auditoría para realizar este cambio.
   - Aplique la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` para implementar una respuesta personalizada al mensaje de Amazon SNS.

Para obtener más información, consulte Acciones de mitigación.

2. Revise la actividad de registro de certificados de dispositivo realizada después de que se revocara el certificado de entidad de certificación y considere la posibilidad de revocar los certificados de dispositivo que se hayan podido emitir durante este período. Puede utilizar ListCertificatesByCA para obtener una lista de los certificados de dispositivo firmados con el certificado de entidad de certificación y UpdateCertificate para revocar un certificado de dispositivo.

Certificado de dispositivo compartido

Varias conexiones simultáneas usan el mismo certificado X.509 para autenticarse con AWS IoT.

Esta comprobación aparece como `DEVICE_CERTIFICATE_SHARED_CHECK` en la CLI y la API.

Gravedad: crítica

Detalles

Cuando se realiza como parte de una auditoría bajo demanda, esta comprobación analiza los certificados y los ID de cliente utilizados por los dispositivos para conectarse durante los 31 días anteriores al inicio de la auditoría hasta 2 horas antes de la ejecución de la comprobación. Para las auditorías programadas, esta comprobación analiza los datos desde 2 horas antes de la última vez que se realizó la auditoría hasta 2 horas antes del momento en que comenzó esta instancia de la auditoría. Si ha tomado medidas para mitigar esta condición durante el periodo de la comprobación, observe cuándo se realizaron las conexiones simultáneas para determinar si el problema persiste.

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra un certificado no conforme:

- CERTIFICATE_SHARED_BY_MULTIPLE_DEVICES

Además, los resultados devueltos con esta comprobación incluyen el ID del certificado compartido, los ID de los clientes que usan el certificado para conectarse y los tiempos de conexión/desconexión. Se muestran primero los resultados más recientes.

¿Por qué importa?

Cada dispositivo debe tener un certificado único para autenticarse con AWS IoT. Cuando varios dispositivos utilizan el mismo certificado, esto podría indicar que un dispositivo ha sufrido un ataque. Puede que su identidad haya sido clonada para realizar nuevos ataques en el sistema.

Cómo solucionarlo

Compruebe que el certificado del dispositivo no ha sufrido un ataque. Si ha sido atacado, siga las prácticas recomendadas de seguridad para mitigar la situación.

Si utiliza el mismo certificado en varios dispositivos, es posible que desee:

1. Aprovisionar nuevo certificados únicos y asociarlos a cada dispositivo.
2. Verificar que los nuevos certificados sean válidos y que los dispositivos puedan usarlos para conectarse.
3. Utilice UpdateCertificate para marcar el certificado antiguo como REVOCADO en AWS IoT. También puede utilizar acciones de mitigación para realizar las siguientes acciones:
   - Aplicar la acción de mitigación `UPDATE_DEVICE_CERTIFICATE` en los resultados de la auditoría para realizar este cambio.
   - Aplicar la acción de mitigación `ADD_THINGS_TO_THING_GROUP` para agregar el dispositivo a un grupo en el que puede tomar medidas.
   - Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una respuesta personalizada en respuesta al mensaje de Amazon SNS.

   Para obtener más información, consulte Acciones de mitigación.
4. Desvincular el certificado antiguo de cada uno de los dispositivos.

Calidad de la clave del certificado del dispositivo

Los clientes de AWS IoT suelen confiar en la autenticación mutua de TLS mediante certificados X.509 para autenticarse en el agente de mensajes de AWS IoT. Estos certificados y los certificados de la entidad de certificación se deben registrar en la cuenta de AWS IoT para poder utilizarlos. AWS IoT realiza comprobaciones de verificación básicas en estos certificados cuando se registran. Estas comprobaciones incluyen:

- Deben tener un formato válido.

- Deben estar firmados por una autoridad de certificación registrada.
- Deben estar dentro del periodo de validez (es decir, no han caducado).
- Los tamaños de la clave criptográfica deben cumplir con un tamaño mínimo requerido (para las claves RSA deben ser de 2048 bits o más).

Esta comprobación de auditoría proporciona las siguientes pruebas adicionales de la calidad de la clave criptográfica:

- CVE-2008-0166: comprueba si la clave se generó usando OpenSSL 0.9.8c-1 hasta versiones anteriores a 0.9.8g-9 en un sistema operativo basado en Debian. Esas versiones de OpenSSL utilizan un generador de números aleatorios que genera números predecibles, lo que permite a los atacantes remotos realizar ataques de adivinación de fuerza bruta contra claves criptográficas.
- CVE-2017-15361: comprueba si la clave se generó mediante la biblioteca Infineon RSA 1.02.013 en el firmware Infineon Trusted Platform Module (TPM), como las versiones anteriores a 0000000000000422 – 4.34, anteriores a 000000000000062b – 6.43 y anteriores a 0000000000008521 – 133.33. Esa biblioteca trata de forma inadecuada la generación de claves RSA, lo que permite a los atacantes frustrar algunos mecanismos de protección criptográfica a través de ataques dirigidos. Algunos ejemplos de tecnologías afectadas son BitLocker con TPM 1.2, generación de claves PGP de YubiKey 4 (anterior a 4.3.5) y la función de cifrado de datos de usuario en caché en el sistema operativo Chrome.

AWS IoT Device Defender registra los certificados como no conformes si no superan estas comprobaciones.

Esta comprobación aparece como `DEVICE_CERTIFICATE_KEY_QUALITY_CHECK` en la CLI y la API.

Gravedad: crítica

Detalles

Esta comprobación se aplica a los certificados de dispositivo ACTIVE o PENDING_TRANSFER.

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra un certificado no conforme:

- CERTIFICATE_KEY_VULNERABILITY_CVE-2017-15361

- CERTIFICATE_KEY_VULNERABILITY_CVE-2008-0166

¿Por qué importa?

Cuando un dispositivo utiliza un certificado vulnerable, los atacantes pueden atacar más fácilmente ese dispositivo.

Cómo solucionarlo

Actualice los certificados de su dispositivo para reemplazar aquellos con vulnerabilidades conocidas.

Si está utilizando el mismo certificado en varios dispositivos, es posible que desee:

1. Aprovisionar nuevo certificados únicos y asociarlos a cada dispositivo.
2. Verificar que los nuevos certificados sean válidos y que los dispositivos puedan usarlos para conectarse.
3. Utilice UpdateCertificate para marcar el certificado antiguo como REVOCADO en AWS IoT. También puede utilizar acciones de mitigación para:
   - Aplicar la acción de mitigación `UPDATE_DEVICE_CERTIFICATE` en los resultados de la auditoría para realizar este cambio.
   - Aplicar la acción de mitigación `ADD_THINGS_TO_THING_GROUP` para agregar el dispositivo a un grupo en el que puede tomar medidas.
   - Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una respuesta personalizada en respuesta al mensaje de Amazon SNS.

   Para obtener más información, consulte Acciones de mitigación.
4. Desvincular el certificado antiguo de cada uno de los dispositivos.

Calidad de la clave del certificado de entidad de certificación

Los clientes de AWS IoT suelen confiar en la autenticación mutua de TLS mediante certificados X.509 para autenticarse en el agente de mensajes de AWS IoT. Estos certificados y los certificados de la entidad de certificación deben registrarse en la cuenta de AWS IoT para poder utilizarlos. AWS IoT realiza comprobaciones de verificación básicas en estos certificados cuando se registran, incluidas las siguientes:

- Los certificados tienen un formato válido.

- Los certificados están dentro de su período de validez (es decir, no han caducado).
- Los tamaños de la clave criptográfica cumplen con un tamaño mínimo requerido (para las claves RSA deben ser de 2048 bits o más).

Esta comprobación de auditoría proporciona las siguientes pruebas adicionales de la calidad de la clave criptográfica:

- CVE-2008-0166: comprueba si la clave se generó usando OpenSSL 0.9.8c-1 hasta versiones anteriores a 0.9.8g-9 en un sistema operativo basado en Debian. Esas versiones de OpenSSL utilizan un generador de números aleatorios que genera números predecibles, lo que permite a los atacantes remotos realizar ataques de adivinación de fuerza bruta contra claves criptográficas.
- CVE-2017-15361: comprueba si la clave se generó mediante la biblioteca Infineon RSA 1.02.013 en el firmware Infineon Trusted Platform Module (TPM), como las versiones anteriores a 0000000000000422 – 4.34, anteriores a 000000000000062b – 6.43 y anteriores a 0000000000008521 – 133.33. Esa biblioteca trata de forma inadecuada la generación de claves RSA, lo que permite a los atacantes frustrar algunos mecanismos de protección criptográfica a través de ataques dirigidos. Algunos ejemplos de tecnologías afectadas son BitLocker con TPM 1.2, generación de claves PGP de YubiKey 4 (anterior a 4.3.5) y la función de cifrado de datos de usuario en caché en el sistema operativo Chrome.

AWS IoT Device Defender registra los certificados como no conformes si no superan estas comprobaciones.

Esta comprobación aparece como `CA_CERTIFICATE_KEY_QUALITY_CHECK` en la CLI y la API.

Gravedad: crítica

Detalles

Esta comprobación se aplica a los certificados de CA ACTIVE o PENDING_TRANSFER.

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra un certificado no conforme:

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

¿Por qué importa?

Los dispositivos agregados recientemente firmados con este certificado de entidad de certificación pueden constituir una amenaza para la seguridad.

Cómo solucionarlo

1. Utilice UpdateCACertificate para marcar el certificado de entidad de certificación como INACTIVO en AWS IoT. También puede utilizar acciones de mitigación para:
   - Aplicar la acción de mitigación `UPDATE_CA_CERTIFICATE` en los resultados de la auditoría para realizar este cambio.
   - Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una respuesta personalizada en respuesta al mensaje de Amazon SNS.

   Para obtener más información, consulte Acciones de mitigación.
2. Revise la actividad de registro de certificados de dispositivo realizada después de que se revocara el certificado de entidad de certificación y considere la posibilidad de revocar los certificados de dispositivo que se hayan podido emitir durante este período. (Utilice ListCertificatesByCA para obtener una lista de los certificados de dispositivos firmados con el certificado de entidad de certificación y UpdateCertificate para revocar un certificado de dispositivos).

El rol de Cognito no autenticado es demasiado permisivo

Una política asociada a un rol de grupo de identidades de Amazon Cognito no autenticado se considera excesivamente permisivo porque otorga permiso para realizar cualquiera de las siguientes acciones de AWS IoT:

- Administrar o modificar objetos
- Leer datos administrativos de objetos
- Administrar datos o recursos relacionados con elementos que no sean objetos

O bien porque otorga permiso para realizar las siguientes acciones de AWS IoT en un amplio conjunto de dispositivos:

- Utilizar MQTT para conectar, publicar o suscribirse a temas reservados (incluidos los datos de ejecución de sombras o de trabajos)
- Utilizar comandos de la API para leer o modificar los datos de ejecución de sombras o de trabajos

En general, los dispositivos que se conectan usando un rol de grupo de identidades de Amazon Cognito no autenticado deben tener solo permisos limitados para publicar y suscribirse a temas de MQTT específicos o usar los comandos de la API para leer y modificar datos específicos de objetos relacionados con los datos de ejecución de sombras o de trabajos.

Esta comprobación aparece como `UNAUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK` en la CLI y la API.

Gravedad: crítica

Detalles

Para esta comprobación, AWS IoT Device Defender realiza auditorías a todos los grupos de identidades de Amazon Cognito que se han utilizado para conectarse al agente de mensajes de AWS IoT durante los 31 días anteriores a la ejecución de la auditoría. En la auditoría se incluyen todos los grupos de identidades de Amazon Cognito a partir de los cuales se ha conectado una identidad de Amazon Cognito autenticada o no autenticada.

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra un rol de grupo de identidades de Amazon Cognito no autenticado no conforme:

- ALLOWS_ACCESS_TO_IOT_ADMIN_ACTIONS
- ALLOWS_BROAD_ACCESS_TO_IOT_DATA_PLANE_ACTIONS

¿Por qué importa?

Debido a que las identidades no autenticadas nunca las autentica el usuario, suponen un riesgo mucho mayor que las identidades de Amazon Cognito autenticadas. Si se ha puesto en riesgo una identidad no autenticada, se podrían usar acciones administrativas para modificar la configuración de la cuenta, eliminar recursos u obtener acceso a información confidencial. O bien, con un amplio acceso a la configuración del dispositivo, se podría obtener acceso a sombras y trabajos de todos los dispositivos de su cuenta o modificarlos. Un usuario invitado podría usar los permisos para poner en riesgo toda su flota o lanzar un ataque DDOS con mensajes.

Cómo solucionarlo

Una política asociada a un rol de grupo de identidades de Amazon Cognito no autenticado debería otorgar solo los permisos necesarios para que un dispositivo haga su trabajo. Recomendamos los siguientes pasos:

1. Crear un nuevo rol conforme.
2. Crear un nuevo grupo de identidades de Amazon Cognito y asociarlo al rol conforme.
3. Verificar que sus identidades puedan obtener acceso a AWS IoT con el nuevo grupo.
4. Una vez que se complete la verificación, asociar el nuevo rol conforme al grupo de identidades de Amazon Cognito marcado como no conforme.

También puede utilizar acciones de mitigación para:

- Aplique la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` para implementar una respuesta personalizada al mensaje de Amazon SNS.

Para obtener más información, consulte Acciones de mitigación.

Administrar o modificar objetos

Las siguientes acciones de la API de AWS IoT se utilizan para administrar o modificar objetos. No se debe conceder permiso para realizar estas acciones a los dispositivos que se conectan a través de un grupo de identidades de Amazon Cognito no autenticado.

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

Cualquier rol que otorgue permiso para realizar estas acciones, incluso en un solo recurso, se considera no conforme.

Leer datos administrativos de objetos

Las siguientes acciones de la API de AWS IoT se utilizan para leer o modificar datos de objetos. Los dispositivos que se conectan a través de un grupo de identidades de Amazon Cognito no autenticado no deben recibir permiso para realizar estas acciones.

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

Example

- no 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"
      ]
    }
  ]
}
```

Esto permite que el dispositivo realice las acciones especificadas incluso aunque se otorgue solo para un objeto.

Administrar elementos que no sean objetos

A los dispositivos que se conectan a través de un grupo de identidades de Amazon Cognito no autenticado no se les debe conceder permiso para realizar acciones de la API de AWS IoT distintas de las que se indican en estas secciones. Puede administrar la cuenta con una aplicación que se conecta a través de un grupo de identidades de Amazon Cognito no autenticado mediante la creación de un grupo de entidades independiente que no utilizan los dispositivos.

Suscribirse/publicar en temas de MQTT

Los mensajes MQTT se envían a través del agente de mensajes de AWS IoT y los dispositivos los usan para realizar muchas acciones, incluido el acceso y la modificación del estado de la sombra y el estado de ejecución del trabajo. Una política que otorga permiso a un dispositivo para conectarse, publicar o suscribirse a mensajes de MQTT debe restringir estas acciones a recursos específicos de la siguiente manera:

Conectar

- no conforme:

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

  El carácter comodín * permite que cualquier dispositivo se conecte a AWS IoT.

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

  A menos que `iot:Connection.Thing.IsAttached` se establezca en true en la claves de condición, es equivalente al carácter comodín * del ejemplo anterior.

- 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 especificación de recursos contiene una variable que coincide con el nombre del dispositivo que se utiliza para conectarse. La instrucción de condición restringe aún más el permiso al comprobar que el certificado utilizado por el cliente de MQTT coincida con el que está asociado al objeto con el nombre utilizado.

Publish

- no conforme:

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

Esto permite que el dispositivo actualice la sombra de cualquier dispositivo (* = todos los dispositivos).

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

Esto permite que el dispositivo lea, actualice o elimine la sombra de cualquier 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 especificación del recurso contiene un comodín, pero solo coincide con cualquier tema relacionado con la sombra para el dispositivo cuyo nombre de objeto se utilice para conectarse.

Suscribirse

- no conforme:

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

Esto permite que el dispositivo se suscriba a temas de sombra o de trabajo reservados para todos los dispositivos.

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

Lo mismo que el ejemplo anterior, pero usando el comodín #.

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

Esto permite que el dispositivo vea las actualizaciones de la sombra en cualquier dispositivo (+ = todos los dispositivos).

- 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/*"
      ],
    }
  ]
}
```

Las especificaciones de recursos contienen caracteres comodín pero solo coinciden con cualquier tema relacionado con la sombra y cualquier tema relacionado con el trabajo para el dispositivo cuyo nombre de objeto se use para conectarse.

Recibir

- conforme:

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

  Esto se permite porque el dispositivo solo puede recibir mensajes de temas en los que tiene permiso para suscribirse.

Leer/modificar los datos de trabajo o sombras

Una política que concede permiso a un dispositivo para realizar una acción de la API para obtener acceso a datos de ejecución de sombras o trabajos o modificarlos debe restringir estas acciones a recursos específicos. Las acciones de la API son las siguientes:

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

Example

- no conforme:

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

  Esto permite al dispositivo realizar la acción especificada en cualquier objeto.

- conforme:

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

```
      "Action": [
          "iot:DeleteThingShadow",
          "iot:GetThingShadow",
          "iot:UpdateThingShadow",
          "iotjobsdata:DescribeJobExecution",
          "iotjobsdata:GetPendingJobExecutions",
          "iotjobsdata:StartNextPendingJobExecution",
          "iotjobsdata:UpdateJobExecution"
      ],
      "Resource": [
        "arn:aws:iot:region:account-id:/thing/MyThing1",
        "arn:aws:iot:region:account-id:/thing/MyThing2"
      ]
    }
  ]
}
```

Esto permite que el dispositivo realice las acciones especificadas en solo dos objetos.

El rol de Cognito autenticado es demasiado permisivo

Una política asociada a un rol de grupo de identidades de Amazon Cognito autenticado se considera excesivamente permisivo porque otorga permiso para realizar las siguientes acciones de AWS IoT:

- Administrar o modificar objetos
- Administrar datos o recursos relacionados con elementos que no sean objetos

O bien porque otorga permiso para realizar las siguientes acciones de AWS IoT en un amplio conjunto de dispositivos:

- Leer datos administrativos de objetos
- Utilizar MQTT para conectar/publicar/suscribirse a temas reservados (incluidos los datos de ejecución de sombras o de trabajos)
- Utilizar comandos de la API para leer o modificar los datos de ejecución de sombras o de trabajos

En general, los dispositivos que se conectan usando un rol de grupo de identidades de Amazon Cognito autenticado solo deben tener permisos limitados para leer datos administrativos específicos de los objetos, publicar y suscribirse a temas de MQTT específicos o usar los comandos de la API

para leer y modificar datos específicos de los objetos relacionados con los datos de ejecución de sombras o de trabajos.

Esta comprobación aparece como `AUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK` en la CLI y la API.

Gravedad: crítica

Detalles

Para esta comprobación, AWS IoT Device Defender realiza auditorías a todos los grupos de identidades de Amazon Cognito que se han utilizado para conectarse al agente de mensajes de AWS IoT durante los 31 días anteriores a la ejecución de la auditoría. En la auditoría se incluyen todos los grupos de identidades de Amazon Cognito a partir de los cuales se ha conectado una identidad de Amazon Cognito autenticada o no autenticada.

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra un rol de grupo de identidades de Amazon Cognito autenticado no conforme:

- 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

¿Por qué importa?

Si se ha puesto en riesgo una identidad autenticada, se podrían usar acciones administrativas para modificar la configuración de la cuenta, eliminar recursos u obtener acceso a información confidencial.

Cómo solucionarlo

Una política asociada a un rol de grupo de identidades de Amazon Cognito autenticado debería otorgar solo los permisos necesarios para que un dispositivo haga su trabajo. Recomendamos los siguientes pasos:

1. Crear un nuevo rol conforme.
2. Crear un nuevo grupo de identidades de Amazon Cognito y asociarlo al rol conforme.
3. Verificar que sus identidades puedan obtener acceso a AWS IoT con el nuevo grupo.

4. Una vez que se complete la verificación, asociar el nuevo rol conforme al grupo de identidades de Amazon Cognito marcado como no conforme.

También puede utilizar acciones de mitigación para:

- Aplique la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` para implementar una respuesta personalizada al mensaje de Amazon SNS.

Para obtener más información, consulte Acciones de mitigación.

Administrar o modificar objetos

Las siguientes acciones de la API de AWS IoT se usan para administrar o modificar objetos, por lo que no se debe otorgar permiso para realizarlas a los dispositivos que se conectan a través de un grupo de identidades de Amazon Cognito autenticado:

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

Cualquier rol que otorgue permiso para realizar estas acciones, incluso en un solo recurso, se considera no conforme.

Administrar elementos que no sean objetos

A los dispositivos que se conectan a través de un grupo de identidades de Amazon Cognito autenticado no se les debe conceder permiso para realizar acciones de la API de AWS IoT distintas

de las que se indican en estas secciones. Para administrar su cuenta con una aplicación que se conecta a través de un grupo de identidades de Amazon Cognito autenticado, cree un grupo de identidades independiente no utilizado por los dispositivos.

Leer datos administrativos de objetos

Las siguientes acciones de la API de AWS IoT se utilizan para leer datos de objetos, por lo que a los dispositivos que se conectan a través de un grupo de identidades de Amazon Cognito autenticado se les debe dar permiso para realizarlas solamente en un conjunto limitado de objetos:

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

- no conforme:

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

  Esto permite al dispositivo realizar la acción especificada en cualquier objeto.
- 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"
      ]
    }
  ]
}
```

Esto permite al dispositivo realizar las acciones especificadas solo en un objeto.

- 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*"
      ]
    }
  ]
}
```

Esto es conforme porque, aunque el recurso se especifica con un carácter comodín (*), va precedido de una cadena específica y esta limita el acceso al conjunto de objetos que tienen el prefijo concreto.

- no conforme:

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

Esto permite al dispositivo realizar la acción especificada en cualquier objeto.

- 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"
        ]
      }
    ]
}
```

Esto permite al dispositivo realizar las acciones especificadas solo en un objeto.

- 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*"
      ]
    }
  ]
}
```

Esto es conforme porque, aunque el recurso se especifica con un carácter comodín (*), va precedido de una cadena específica y esta limita el acceso al conjunto de objetos que tienen el prefijo concreto.

Suscribirse/publicar en temas de MQTT

Los mensajes de MQTT se envían a través del agente de mensajes de AWS IoT y los dispositivos los usan para realizar muchas acciones diferentes, incluido el acceso y la modificación del estado de

la sombra y el estado de ejecución del trabajo. Una política que otorga permiso a un dispositivo para conectarse, publicar o suscribirse a mensajes de MQTT debe restringir estas acciones a recursos específicos de la siguiente manera:

Conectar

- no conforme:

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

  El carácter comodín * permite que cualquier dispositivo se conecte a AWS IoT.

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

  A menos que `iot:Connection.Thing.IsAttached` se establezca en true en la claves de condición, es equivalente al carácter comodín * del ejemplo anterior.

- 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 especificación del recurso contiene una variable que coincide con el nombre del dispositivo utilizado para conectarse, y la instrucción de condición restringe aún más el permiso verificando que el certificado utilizado por el cliente MQTT coincida con el que está asociado al objeto con el nombre utilizado.

Publish

- no conforme:

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

Esto permite que el dispositivo actualice la sombra de cualquier dispositivo (* = todos los dispositivos).

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

Esto permite que el dispositivo lea/actualice/elimine la sombra de cualquier 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 especificación del recurso contiene un comodín, pero solo coincide con cualquier tema relacionado con la sombra para el dispositivo cuyo nombre de objeto se utilice para conectarse.

Suscribirse

- no conforme:

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

Esto permite que el dispositivo se suscriba a temas de sombra o de trabajo reservados para todos los dispositivos.

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

Lo mismo que el ejemplo anterior, pero usando el comodín #.

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

Esto permite que el dispositivo vea las actualizaciones de la sombra en cualquier dispositivo (+ = todos los dispositivos).

- 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/*"
      ],
    }
  ]
}
```

Las especificaciones de recursos contienen caracteres comodín pero solo coinciden con cualquier tema relacionado con la sombra y cualquier tema relacionado con el trabajo para el dispositivo cuyo nombre de objeto se use para conectarse.

Recibir

- conforme:

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

Esto es conforme porque el dispositivo solo puede recibir mensajes de temas en los que tiene permiso para suscribirse.

Leer o modificar datos de trabajo o sombras

Una política que concede permiso a un dispositivo para realizar una acción de la API para obtener acceso a datos de ejecución de sombras o trabajos o modificarlos debe restringir estas acciones a recursos específicos. Las acciones de la API son las siguientes:

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

Ejemplos

- no conforme:

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

  Esto permite al dispositivo realizar la acción especificada en cualquier objeto.

- 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"
      ]
    }
  ]
}
```

Esto permite al dispositivo realizar las acciones especificadas solo en dos objetos.

Políticas de AWS IoT demasiado permisivas

Una política de AWS IoT otorga permisos que son demasiado amplios o no están sujetos a restricciones. Otorga permiso para enviar o recibir mensajes de MQTT para un amplio conjunto de dispositivos, u otorga permiso para obtener acceso a los datos de ejecución de sombras y de trabajos o modificarlos para un amplio conjunto de dispositivos.

En general, una política para un dispositivo debería otorgar acceso a recursos asociados con ese dispositivo y sin otros dispositivos o con muy pocos. Con algunas excepciones, el uso de un carácter comodín (por ejemplo, "*") para especificar recursos en dicha política se considera demasiado amplio o sin restricciones.

Esta comprobación aparece como `IOT_POLICY_OVERLY_PERMISSIVE_CHECK` en la CLI y la API.

Gravedad: crítica

Detalles

Se devuelve el siguiente código de motivo cuando esta comprobación encuentra una política de AWS IoT no conforme:

- ALLOWS_BROAD_ACCESS_TO_IOT_DATA_PLANE_ACTIONS

¿Por qué importa?

Un certificado, una identidad de Amazon Cognito o un grupo de objetos con una política excesivamente permisiva puede, en caso de ponerse en riesgo, afectar a la seguridad de toda su cuenta. Un atacante podría usar un acceso tan amplio para leer o modificar sombras, trabajos o ejecuciones de trabajos para todos sus dispositivos. O un atacante podría usar un certificado atacado para conectar dispositivos maliciosos o lanzar un ataque DDOS en su red.

Cómo solucionarlo

Siga estos pasos para corregir las políticas no conformes asociadas a objetos, grupos de objetos u otras entidades:

1. Utilice CreatePolicyVersion para crear une nueva versión conforme de la política. Establezca la marca `setAsDefault` en true. (Esto hace que esta nueva versión funcione para todas las entidades que utilizan la política).
2. Utilice ListTargetsForPolicy para obtener una lista de destinos (certificados o grupos de objetos) a los que la política está asociada y determinar qué dispositivos están incluidos en los grupos o cuáles utilizan los certificados para conectarse.
3. Verifique que todos los dispositivos asociados puedan conectarse a AWS IoT. Si un dispositivo no puede conectarse, utilice SetPolicyVersion para devolver la política predeterminada a la versión anterior, revisar la política e intentarlo de nuevo.

Puede utilizar acciones de mitigación para:

- Aplicar la acción de mitigación `REPLACE_DEFAULT_POLICY_VERSION` en los resultados de la auditoría para realizar este cambio.
- Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una respuesta personalizada en respuesta al mensaje de Amazon SNS.

Para obtener más información, consulte Acciones de mitigación.

Utilice las variables de política de AWS IoT Core para hacer referencia de forma dinámica a los recursos de AWS IoT en las políticas.

Permisos de MQTT

Los mensajes MQTT se envían a través del agente de mensajes de AWS IoT y los dispositivos los usan para realizar muchas acciones, incluido el acceso y la modificación del estado de la sombra y el estado de ejecución del trabajo. Una política que otorga permiso a un dispositivo para conectarse, publicar o suscribirse a mensajes de MQTT debe restringir estas acciones a recursos específicos de la siguiente manera:

Conectar

- no conforme:

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

El carácter comodín * permite que cualquier dispositivo se conecte a AWS IoT.

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

A menos que `iot:Connection.Thing.IsAttached` se establezca en true en la claves de condición, es equivalente al carácter comodín * del ejemplo anterior.

- 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 especificación de recursos contiene una variable que coincide con el nombre del dispositivo que se utiliza para conectarse. La instrucción de condición restringe aún más el permiso al comprobar que el certificado utilizado por el cliente de MQTT coincida con el que está asociado al objeto con el nombre utilizado.

Publish

- no conforme:

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

Esto permite que el dispositivo actualice la sombra de cualquier dispositivo (* = todos los dispositivos).

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

Esto permite que el dispositivo lea, actualice o elimine la sombra de cualquier 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 especificación del recurso contiene un comodín, pero solo coincide con cualquier tema relacionado con la sombra para el dispositivo cuyo nombre de objeto se utilice para conectarse.

Suscribirse

- no conforme:

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

Esto permite que el dispositivo se suscriba a temas de sombra o de trabajo reservados para todos los dispositivos.

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

Lo mismo que el ejemplo anterior, pero usando el comodín #.

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

Esto permite que el dispositivo vea las actualizaciones de la sombra en cualquier dispositivo (+ = todos los dispositivos).

- 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/*"
      ],
    }
  ]
}
```

  Las especificaciones de recursos contienen caracteres comodín pero solo coinciden con cualquier tema relacionado con la sombra y cualquier tema relacionado con el trabajo para el dispositivo cuyo nombre de objeto se use para conectarse.

Recibir

- conforme:

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

  Esto es conforme porque el dispositivo solo puede recibir mensajes de temas en los que tiene permiso para suscribirse.

Permisos de trabajo y sombras

Una política que concede permiso a un dispositivo para realizar una acción de la API para obtener acceso a datos de ejecución de sombras o trabajos o modificarlos debe restringir estas acciones a recursos específicos. Las acciones de la API son las siguientes:

- `DeleteThingShadow`
- `GetThingShadow`
- `UpdateThingShadow`

- `DescribeJobExecution`
- `GetPendingJobExecutions`
- `StartNextPendingJobExecution`
- `UpdateJobExecution`

Ejemplos

- no conforme:

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

  Esto permite al dispositivo realizar la acción especificada en cualquier objeto.

- conforme:

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

  Esto permite al dispositivo realizar las acciones especificadas solo en dos objetos.

La política de AWS IoT está potencialmente mal configurada

Se identificó una política de AWS IoT potencialmente mal configurada. Las políticas mal configuradas, incluidas las políticas demasiado permisivas, pueden provocar incidentes de seguridad, como permitir que los dispositivos accedan a recursos no deseados.

La comprobación de una política de AWS IoT potencialmente mal configurada es una advertencia para que se asegure de que solo se permiten las acciones previstas antes de actualizar la política.

Esta comprobación aparece como `IOT_POLICY_POTENTIAL_MISCONFIGURATION_CHECK` en la CLI y la API.

Gravedad: media

Detalles

AWS IoT devuelve el siguiente código de motivo cuando esta comprobación encuentra una política de AWS IoT potencialmente mal configurada:

- POLICY_CONTAINS_MQTT_WILDCARDS_IN_DENY_STATEMENT
- TOPIC_FILTERS_INTENDED_TO_DENY_ALLOWED_USING_WILDCARDS

¿Por qué importa?

Las políticas mal configuradas pueden tener consecuencias no deseadas, ya que proporcionan más permisos a los dispositivos de los necesarios. Recomendamos considerar detenidamente la política para limitar el acceso a los recursos y prevenir las amenazas a la seguridad.

La política contiene caracteres comodín de MQTT en el ejemplo de la declaración de denegación

La comprobación de la política de AWS IoT potencialmente mal configurada, inspecciona los caracteres comodín (+ o #) de MQTT en las declaraciones de denegación. Las políticas tratan los caracteres comodín como cadenas literales y pueden hacer que la política de AWS IoT sea demasiado permisiva.

El siguiente ejemplo tiene por objeto denegar la suscripción a temas relacionados con `building/control_room` usando el comodín de MQTT en las políticas de #. Sin embargo, los caracteres comodín de MQTT no tienen un significado comodín en las políticas de AWS IoT y los dispositivos se pueden suscribir a `building/control_room/data1`.

La comprobación de la política de AWS IoT potencialmente mal configurada marcará esta política con un código de 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/*"
    }
  ]
}
```

A continuación se muestra un ejemplo de una política correctamente configurada. Los dispositivos no tienen permiso para suscribirse a subtemas de `building/control_room/` ni para recibir mensajes de subtemas de `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/*"
    }
  ]
}
```

Ejemplo de filtros de temas destinados a denegar el uso de caracteres comodín

La siguiente política de ejemplo pretende denegar la suscripción a temas relacionados con `building/control_room` denegando el recurso de `building/control_room/*`. Sin embargo, los dispositivos pueden enviar solicitudes para suscribirse a `building/#` y recibir mensajes de todos los temas relacionados con `building`, incluidos `building/control_room/data1`.

La comprobación de la política de AWS IoT potencialmente mal configurada marcará esta política con un código de motivo `TOPIC_FILTERS_INTENDED_TO_DENY_ALLOWED_USING_WILDCARDS`.

El siguiente ejemplo de política tiene permisos para recibir mensajes en `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/*"
```

```
    }
  ]
}
```

A continuación se muestra un ejemplo de una política correctamente configurada. Los dispositivos no tienen permiso para suscribirse a subtemas de `building/control_room/` ni para recibir mensajes de subtemas de `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**
>
> Esta comprobación podría arrojar falsos positivos. Le recomendamos que evalúe las políticas marcadas y seleccione los recursos con falsos positivos mediante supresiones de auditoría.

Cómo solucionarlo

Esta comprobación marca las políticas que potencialmente mal configuradas, por lo que podrían producirse falsos positivos. Marque los falsos positivos mediante supresiones de auditoría para que no se detecten en el futuro.

También puede seguir estos pasos para corregir las políticas no conformes asociadas a objetos, grupos de objetos u otras entidades:

1. Utilice CreatePolicyVersion para crear une nueva versión conforme de la política. Establezca la marca `setAsDefault` en true. (Esto hace que esta nueva versión funcione para todas las entidades que utilizan la política).

   Para ver ejemplos de creación de políticas de AWS IoT para casos de uso comunes, consulte los ejemplos de políticas Publish/Subscribe en la Guía para desarrolladores de AWS IoT Core.
2. Verifique que todos los dispositivos asociados puedan conectarse a AWS IoT. Si un dispositivo no puede conectarse, utilice SetPolicyVersion para devolver la política predeterminada a la versión anterior, revisar la política e intentarlo de nuevo.

Puede utilizar acciones de mitigación para:

- Aplicar la acción de mitigación `REPLACE_DEFAULT_POLICY_VERSION` en los resultados de la auditoría para realizar este cambio.
- Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una respuesta personalizada en respuesta al mensaje de Amazon SNS.

Para obtener más información, consulte Acciones de mitigación.

Utilice las variables de política de IoT Core en la Guía para desarrolladores de AWS IoT Core para hacer referencia de forma dinámica a los recursos de AWS IoT en las políticas.

El alias de rol es demasiado permisivo

El alias de rol de AWS IoT proporciona un mecanismo para que los dispositivos conectados se autentiquen en AWS IoT mediante certificados X.509 y obtengan credenciales de AWS de corta duración de un rol de IAM asociado a un alias de rol de AWS IoT. Los permisos para estas credenciales se deben reducir mediante políticas de acceso con variables de contexto de autenticación. Si las políticas no están configuradas correctamente, podría quedar expuesto a una

escalada de ataque de privilegios. Esta comprobación de auditoría garantiza que las credenciales temporales proporcionadas por los alias de rol de AWS IoT no sean excesivamente permisivas.

Esta comprobación se activa si se encuentra una de las siguientes condiciones:

- La política proporciona permisos administrativos a todos los servicios utilizados en el último año por este alias de rol (por ejemplo, "iot:*", "dynamodb:*", "iam:*", etc.).
- La política proporciona un amplio acceso a acciones de metadatos de objetos, acceso a acciones de AWS IoT restringidas o un amplio acceso a acciones del plano de datos de AWS IoT.
- La política proporciona acceso a servicios de auditoría de seguridad como "iam", "cloudtrail", "guardduty", "inspector" o "trustedadvisor".

Esta comprobación aparece como `IOT_ROLE_ALIAS_OVERLY_PERMISSIVE_CHECK` en la CLI y la API.

Gravedad: crítica

Detalles

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra una política de IoT no conforme:

- 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

¿Por qué importa?

Al limitar los permisos a aquellos que se requieren para que un dispositivo realice sus operaciones normales, se reducen los riesgos de su cuenta si un dispositivo es víctima de un ataque.

Cómo solucionarlo

Siga estos pasos para corregir las políticas no conformes asociadas a objetos, grupos de objetos u otras entidades:

1. Siga los pasos que encontrará en Autorización de llamadas directas a los servicios de AWS mediante un proveedor de credenciales de AWS IoT Core para aplicar una política más restrictiva al alias de su rol.

Puede utilizar acciones de mitigación para:

- Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una acción personalizada en respuesta al mensaje de Amazon SNS.

Para obtener más información, consulte Acciones de mitigación.

El alias del rol permite el acceso a los servicios no utilizados

El alias de rol de AWS IoT proporciona un mecanismo para que los dispositivos conectados se autentiquen en AWS IoT mediante certificados X.509 y obtengan credenciales de AWS de corta duración de un rol de IAM asociado a un alias de rol de AWS IoT. Los permisos para estas credenciales se deben reducir mediante políticas de acceso con variables de contexto de autenticación. Si las políticas no están configuradas correctamente, podría quedar expuesto a una escalada de ataque de privilegios. Esta comprobación de auditoría garantiza que las credenciales temporales proporcionadas por los alias de rol de AWS IoT no sean excesivamente permisivas.

Esta comprobación se activa si el alias de rol tiene acceso a servicios que no se han utilizado para el dispositivo de AWS IoT en el último año. Por ejemplo, la auditoría le informa si tiene un rol de IAM vinculado al alias de rol que solo ha utilizado AWS IoT en el último año, pero la política asociada al rol también concede permiso a `"iam:getRole"` y `"dynamodb:PutItem"`.

Esta comprobación aparece como `IOT_ROLE_ALIAS_ALLOWS_ACCESS_TO_UNUSED_SERVICES_CHECK` en la CLI y la API.

Gravedad: media

Detalles

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra una política de AWS IoT no conforme:

- ALLOWS_ACCESS_TO_UNUSED_SERVICES

¿Por qué importa?

Al limitar los permisos a los servicios que se requieren para que un dispositivo realice sus operaciones normales, se reducen los riesgos de su cuenta si un dispositivo es víctima de un ataque.

Cómo solucionarlo

Siga estos pasos para corregir las políticas no conformes asociadas a objetos, grupos de objetos u otras entidades:

1. Siga los pasos que encontrará en Autorización de llamadas directas a los servicios de AWS mediante un proveedor de credenciales de AWS IoT Core para aplicar una política más restrictiva al alias de su rol.

Puede utilizar acciones de mitigación para:

- Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una acción personalizada en respuesta al mensaje de Amazon SNS.

Para obtener más información, consulte Acciones de mitigación.

El certificado de entidad de certificación está caducando

Un certificado de entidad de certificación va a caducar dentro de 30 días o ha caducado.

Esta comprobación aparece como `CA_CERTIFICATE_EXPIRING_CHECK` en la CLI y la API.

Gravedad: media

Detalles

Esta comprobación se aplica a los certificados de CA ACTIVE o PENDING_TRANSFER.

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra un certificado de entidad de certificación no conforme:

- CERTIFICATE_APPROACHING_EXPIRATION
- CERTIFICATE_PAST_EXPIRATION

¿Por qué importa?

Un certificado de entidad de certificación caducado no debe utilizarse para firmar nuevos certificados de dispositivos.

Cómo solucionarlo

Consulte las prácticas recomendadas de seguridad para saber cómo proceder. Es posible que desee:

1. Registrar un nuevo certificado de entidad de certificación en AWS IoT.
2. Verificar que puede firmar certificados de dispositivo con el nuevo certificado de entidad de certificación.
3. Utilice UpdateCACertificate para marcar el antiguo certificado de entidad de certificación como INACTIVO en AWS IoT. También puede utilizar acciones de mitigación para realizar las siguientes acciones:
   - Aplicar la acción de mitigación `UPDATE_CA_CERTIFICATE` en los resultados de la auditoría para realizar este cambio.
   - Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una respuesta personalizada en respuesta al mensaje de Amazon SNS.

   Para obtener más información, consulte Acciones de mitigación.

Identificadores de cliente MQTT contradictorios

Varios dispositivos se conectan con el mismo ID de cliente.

Esta comprobación aparece como `CONFLICTING_CLIENT_IDS_CHECK` en la CLI y la API.

Gravedad: alta

Detalles

Se han realizado varias conexiones con el mismo ID de cliente, lo que ha provocado la desconexión de un dispositivo ya conectado. La especificación de MQTT solo permite una conexión activa por ID de cliente, con lo cual, cuando otro dispositivo se conecta con el mismo ID de cliente, se bloquea la conexión del dispositivo anterior.

Cuando se realiza como parte de una auditoría bajo demanda, esta comprobación analiza cómo se usaban los ID de cliente utilizados por los dispositivos para conectarse durante los 31 días anteriores al inicio de la auditoría. Para las auditorías programadas, esta comprobación analiza los datos desde la última vez que se realizó la auditoría hasta el momento en que comenzó esta instancia de la auditoría. Si ha tomado medidas para mitigar esta condición durante el periodo de la comprobación, observe cuándo se realizaron las conexiones/desconexiones para determinar si el problema persiste.

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra una falta de conformidad:

- DUPLICATE_CLIENT_ID_ACROSS_CONNECTIONS

Además, los resultados devueltos con esta comprobación incluyen el ID de cliente utilizado para conectarse, los identificadores de las entidades principales y los tiempos de desconexión. Se muestran primero los resultados más recientes.

¿Por qué importa?

Los dispositivos con ID en conflicto se ven obligados a volver a conectarse constantemente, lo que puede provocar la pérdida de mensajes o la imposibilidad de que el dispositivo se conecte.

Esto puede indicar que un dispositivo o las credenciales de un dispositivo se han puesto en riesgo y podrían ser parte de un ataque DDoS. También es posible que los dispositivos estén mal configurados en la cuenta o que el dispositivo tenga una mala conexión y se vea obligado a volver a conectarse varias veces por minuto.

Cómo solucionarlo

Registre cada dispositivo como un objeto único en AWS IoT y use el nombre de objeto como ID de cliente para la conexión. O use un UUID como ID de cliente al conectar el dispositivo a través de MQTT. También puede utilizar acciones de mitigación para:

- Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una respuesta personalizada en respuesta al mensaje de Amazon SNS.

Para obtener más información, consulte Acciones de mitigación.

El certificado de dispositivo está caducando

Un certificado de dispositivo va a caducar en el periodo de umbral configurado o ha caducado. El umbral de comprobación de la caducidad del certificado puede configurarse entre 30 días (mínimo) y 3652 días (10 años, máximo) con un valor predeterminado de 30 días.

Esta comprobación aparece como `DEVICE_CERTIFICATE_EXPIRING_CHECK` en la CLI y la API.

Gravedad: media

Detalles

Esta comprobación se aplica a los certificados de dispositivo ACTIVE o PENDING_TRANSFER.

Cuando esta comprobación encuentra un certificado de dispositivo no conforme se devuelven los siguientes códigos de motivo:

- CERTIFICATE_APPROACHING_EXPIRATION
- CERTIFICATE_PAST_EXPIRATION

¿Por qué importa?

Un certificado de dispositivo no debe utilizarse una vez que caduque.

Configuración de la comprobación de caducidad del certificado del dispositivo

Esta configuración le permite supervisar y recibir alertas de los certificados que se acercan a la fecha de caducidad en toda la flota de dispositivos. Por ejemplo, si desea que se le notifique cuándo los certificados están a menos de 30 días de caducar, puede configurar la comprobación del siguiente modo:

```
{
    "roleArn": "your-audit-role-arn",
    "auditCheckConfigurations": {
        "DEVICE_CERTIFICATE_EXPIRING_CHECK": {
            "enabled": true,
            "configuration": {
                "CERT_EXPIRATION_THRESHOLD_IN_DAYS": "30"
            }
```

```
        }
    }
}
```

Cómo solucionarlo

Consulte las prácticas recomendadas de seguridad para saber cómo proceder. Es posible que desee:

1. Aprovisionar un nuevo certificado y asociarlo al dispositivo.
2. Verificar que el nuevo certificado sea válido y que el dispositivo pueda usarlo para conectarse.
3. Utilice UpdateCertificate para marcar el certificado antiguo como INACTIVO en AWS IoT. También puede utilizar acciones de mitigación para:
   - Aplicar la acción de mitigación `UPDATE_DEVICE_CERTIFICATE` en los resultados de la auditoría para realizar este cambio.
   - Aplicar la acción de mitigación `ADD_THINGS_TO_THING_GROUP` para agregar el dispositivo a un grupo en el que puede tomar medidas.
   - Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una respuesta personalizada en respuesta al mensaje de Amazon SNS.

   Para obtener más información, consulte Acciones de mitigación.
4. Desvincular el certificado antiguo del dispositivo. (Consulte DetachThingPrincipal.)

Comprobación de la antigüedad del certificado del dispositivo

Esta comprobación de auditoría le avisa cuando el certificado de un dispositivo ha estado activo durante un número de días superior o igual al número que especifique. Esta comprobación lo ayuda a mantenerse informado sobre el estado de los certificados, lo que permite actuar a tiempo de forma periódica, independientemente de cuándo llegue el certificado al final de su vida útil, y mejora la seguridad al reducir el riesgo de que los certificados se vean comprometidos.

El umbral de comprobación de la antigüedad del certificado puede configurarse entre 30 días (mínimo) y 3652 días (10 años, máximo) con un valor predeterminado de 365 días.

Esta comprobación aparece como `DEVICE_CERTIFICATE_AGE_CHECK` en la CLI y la API. Esta comprobación está desactivada de forma predeterminada Gravedad: baja

Detalles

Esta comprobación se aplica a los certificados de dispositivo ACTIVE o PENDING_TRANSFER. Cuando esta comprobación encuentra un certificado de dispositivo no conforme se devuelven los siguientes códigos de motivo:

- CERTIFICATE_PAST_AGE_THRESHOLD

Configuración de la comprobación de la antigüedad del certificado del dispositivo

Esta configuración le permite adaptar las alertas de rotación de certificados a las necesidades específicas de la flota, lo que lo ayuda a mantener una sólida posición de seguridad en todos los dispositivos. Puede configurar esta comprobación mediante la API `UpdateAccountAuditConfiguration`. Por ejemplo, si desea recibir una alerta cuando los certificados lleven activos más de 365 días, puede configurar la comprobación del siguiente modo:

```
{
    "roleArn": "your-audit-role-arn",
    "auditCheckConfigurations": {
        "DEVICE_CERTIFICATE_AGE_CHECK": {
            "enabled": true,
            "configuration": {
                "CERT_AGE_THRESHOLD_IN_DAYS": "365"
            }
        }
    }
}
```

Un certificado del dispositivo revocado sigue activo

Un certificado del dispositivo revocado sigue activo.

Esta comprobación aparece como `REVOKED_DEVICE_CERTIFICATE_STILL_ACTIVE_CHECK` en la CLI y la API.

Gravedad: media

Detalles

Un certificado de dispositivo no está en la lista de revocación de certificados de CA, pero sigue activo en AWS IoT.

Esta comprobación se aplica a los certificados de dispositivo ACTIVE o PENDING_TRANSFER.

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra una falta de conformidad:

- CERTIFICATE_REVOKED_BY_ISSUER

¿Por qué importa?

Un certificado de dispositivo generalmente se revoca porque ha sufrido un ataque. Es posible que aún no se haya revocado en AWS IoT debido a un error o un descuido.

Cómo solucionarlo

Compruebe que el certificado del dispositivo no ha sufrido un ataque. Si ha sido atacado, siga las prácticas recomendadas de seguridad para mitigar la situación. Es posible que desee:

1. Aprovisionar un nuevo certificado para el dispositivo.
2. Verificar que el nuevo certificado sea válido y que el dispositivo pueda usarlo para conectarse.
3. Utilice UpdateCertificate para marcar el certificado antiguo como REVOCADO en AWS IoT. También puede utilizar acciones de mitigación para:
   - Aplicar la acción de mitigación `UPDATE_DEVICE_CERTIFICATE` en los resultados de la auditoría para realizar este cambio.
   - Aplicar la acción de mitigación `ADD_THINGS_TO_THING_GROUP` para agregar el dispositivo a un grupo en el que puede tomar medidas.
   - Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una respuesta personalizada en respuesta al mensaje de Amazon SNS.

   Para obtener más información, consulte Acciones de mitigación.
4. Desvincular el certificado antiguo del dispositivo. (Consulte DetachThingPrincipal.)

Registro desactivado

Los registros de AWS IoT no están habilitados en Amazon CloudWatch. Verifica los registros de la V1 y la V2.

Esta comprobación aparece como `LOGGING_DISABLED_CHECK` en la CLI y la API.

Gravedad: baja

Detalles

Se devuelven los siguientes códigos de motivo cuando esta comprobación encuentra una falta de conformidad:

- LOGGING_DISABLED

¿Por qué importa?

Los registros de AWS IoT en CloudWatch proporcionan visibilidad sobre los comportamientos de AWS IoT, incluidos los errores de autenticación y las desconexiones que podrían indicar que un dispositivo ha sufrido un ataque.

Cómo solucionarlo

Habilite los registros de AWS IoT en CloudWatch. Consulte Registro y supervisión en la Guía para desarrolladores de AWS IoT Core. También puede utilizar acciones de mitigación para:

- Aplicar la acción de mitigación `ENABLE_IOT_LOGGING` en los resultados de la auditoría para realizar este cambio.
- Aplicar la acción de mitigación `PUBLISH_FINDINGS_TO_SNS` si desea implementar una respuesta personalizada en respuesta al mensaje de Amazon SNS.

Para obtener más información, consulte Acciones de mitigación.

Comandos de auditoría

Administrar la configuración de auditorías

Utilice `UpdateAccountAuditConfiguration` para configurar los ajustes de auditoría de su cuenta Este comando le permite habilitar las comprobaciones que desea que estén disponibles para las auditorías, configurar notificaciones opcionales y configurar permisos.

Compruebe esta configuración con `DescribeAccountAuditConfiguration`.

Utilice `DeleteAccountAuditConfiguration` para eliminar la configuración de auditoría. Esto restaura todos los valores predeterminados y desactiva de manera efectiva las auditorías, ya que todas las comprobaciones están deshabilitadas de manera predeterminada.

UpdateAccountAuditConfiguration

Configura o vuelve a configurar los ajustes de auditoría de Device Defender para esta cuenta. La configuración incluye cómo se envían las notificaciones de auditoría y qué comprobaciones de auditoría se habilitan o deshabilitan.

Sinopsis

```
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]
```

Formato `cli-input-json`

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

```
      "enabled": "boolean"
    }
  }
}
```

Campos **`cli-input-json`**

Nombre	Tipo	Descripción
roleArn	cadena Longitud máx.: 2048; mín.: 20	El ARN del rol que concede permiso a AWS IoT para obtener acceso a la informaci ón sobre sus dispositivos, políticas, certificados y otros elementos al realizar una auditoría.
auditNotificationTargetConf igurations	map	Información sobre los destinos a los que se envían las notificaciones de auditoría.
targetArn	cadena	El ARN del destino (tema SNS) al que se envían las notificaciones de auditoría.
roleArn	cadena Longitud máx.: 2048; mín.: 20	El ARN del rol que concede permiso para enviar notificac iones al destino.
enabled	booleano	True si se habilitan las notificaciones al destino.
auditCheckConfigurations	map	Especifica las comporbac iones de auditoría habilitad as y deshabilitadas para esta cuenta. Utilice `DescribeA ccountAuditConfigu ration` para ver la lista de todas las comprobac

Nombre	Tipo	Descripción
		iones, incluidas las habilitadas actualmente. Parte de la recopilación de datos puede comenzar inmediatamente cuando se habilitan determinadas comprobaciones. Cuando se deshabilita una comprobac ión, se borran todos los datos recopilados hasta el momento relacionados con la comprobación. No puede deshabilitar una comprobación si se utiliza en una auditoría programad a. Primero debe eliminar la comprobación de la auditoría programada o eliminar la propia auditoría programada. En la primera llamada a `UpdateAccountAudit Configuration` se necesita este parámetro y debe especificar al menos una comprobación habilitada.
enabled	booleano	True si está habilitada la comprobación de auditoría para esta cuenta.

Nombre	Tipo	Descripción
configuración	map	(Opcional) Configuraciones personalizadas para comprobaciones de auditoría específicas, como `CERT_AGE_THRESHOLD_IN_DAYS` y `CERT_EXPIRATION_THRESHOLD_IN_DAYS`, que le permiten definir cuándo desea recibir alertas sobre la antigüedad de los certificados y su inminente caducidad.

Output

Ninguno

Errores

`InvalidRequestException`

El contenido de la solicitud no es válido.

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

DescribeAccountAuditConfiguration

Obtiene información sobre la configuración de auditoría de Device Defender para esta cuenta. La configuración incluye cómo se envían las notificaciones de auditoría y qué comprobaciones de auditoría se habilitan o deshabilitan.

Sinopsis

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

Formato `cli-input-json`

```
{
}
```

Output

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

Campos de salida de la CLI

Nombre	Tipo	Descripción
roleArn	cadena Longitud máx.: 2048; mín.: 20	El ARN del rol que concede permiso a AWS IoT para obtener acceso a la informaci ón sobre sus dispositivos, políticas, certificados y otros elementos al realizar una auditoría. En la primera llamada a `UpdateAccountAudit`

Nombre	Tipo	Descripción
		`Configuration` , se necesita este parámetro.
auditNotificationTargetConfigurations	map	Información sobre los destinos a los que se envían las notificaciones de auditoría para esta cuenta.
targetArn	cadena	El ARN del destino (tema SNS) al que se envían las notificaciones de auditoría.
roleArn	cadena Longitud máx.: 2048; mín.: 20	El ARN del rol que concede permiso para enviar notificaciones al destino.
enabled	booleano	True si se habilitan las notificaciones al destino.
auditCheckConfigurations	map	Las verificaciones de auditoría habilitadas y deshabilitadas para esta cuenta.
enabled	booleano	True si está habilitada la comprobación de auditoría para esta cuenta.
configuración	map	(Opcional) Proporciona configuraciones específicas para determinadas comprobaciones de auditoría, como la antigüedad máxima permitida para los certificados o el número de días antes de la caducidad en los que debe desencadenarse una alerta.

Errores

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

DeleteAccountAuditConfiguration

Restaura la configuración predeterminada para las auditorías de Device Defender para esta cuenta. Se eliminarán todos los datos de configuración que haya introducido y todas las comprobaciones de auditoría se restablecerán como deshabilitadas.

Sinopsis

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

Formato `cli-input-json`

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

Campos **`cli-input-json`**

Nombre	Tipo	Descripción
deleteScheduledAudits	booleano	Si es true, se eliminan todas las auditorías programadas.

Output

Ninguno

Errores

`InvalidRequestException`

El contenido de la solicitud no es válido.

`ResourceNotFoundException`

El recurso especificado no existe.

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

Programación de auditorías

Utilice `CreateScheduledAudit` para crear una o varias auditorías programadas. Este comando permite especificar las comprobaciones que desea realizar durante una auditoría y con qué frecuencia deben ejecutarse.

Mantenga un registro de sus auditorías programadas con `ListScheduledAudits` y `DescribeScheduledAudit`.

Cambie una auditoría programada existente con `UpdateScheduledAudit` o elimínela con `DeleteScheduledAudit`.

CreateScheduledAudit

Crea una auditoría programada que se ejecuta en un intervalo de tiempo especificado.

Sinopsis

```
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]
```

Formato `cli-input-json`

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

Campos **`cli-input-json`**

Nombre	Tipo	Descripción
frequency	cadena	Frecuencia con la que se lleva a cabo la auditoría. Puede ser DAILY, WEEKLY, BIWEEKLY o MONTHLY. El sistema determina la hora de inicio real de cada auditoría. enum: DAILY | WEEKLY | BIWEEKLY | MONTHLY
dayOfMonth	cadena patrón: ^([1-9]|[12][0-9]|3[01])$\|^LAST$	El día del mes en que tiene lugar la auditoría programada. Puede ser de 1 a 31 o LAST. Este campo es obligatorio si el parámetro `frequency` se establece en MONTHLY. Si se especifican los días 29-31 y el mes no tiene tantos días, la

Nombre	Tipo	Descripción
		auditoría se realizará el último (LAST) día del mes.
dayOfWeek	cadena	El día de la semana en que tiene lugar la auditoría programada. Puede ser SUN, MON, TUE,WED, THU, FRI o SAT. Este campo es obligatorio si el parámetro `frequency` se establece en WEEKLY o BIWEEKLY. enum: SUN | MON | TUE | WED | THU | FRI | SAT
targetCheckNames	list miembro: AuditCheckName	Controles que se realizan durante la auditoría programada. Las comprobaciones deben activarse para su cuenta. (Utilice `DescribeAccountAuditConfiguration` para ver la lista de todas las comprobaciones, incluidas las habilitadas o `UpdateAccountAuditConfiguration` para seleccionar las comprobaciones habilitadas).
etiquetas	list member: Tag Clase de Java: java.util.List	Los metadatos que se pueden utilizar para administrar la auditoría programada.
Clave	cadena	La clave de la etiqueta.

Nombre	Tipo	Descripción
Valor	cadena	El valor de la etiqueta.
scheduledAuditName	cadena Longitud máx.: 128; mín.: 1 Patrón: [a-zA-Z0-9_-]+	El nombre que desea asignar a la auditoría programada. (Máximo de 128 caracteres)

Output

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

Campos de salida de la CLI

Nombre	Tipo	Descripción
scheduledAuditArn	cadena	El ARN de la auditoría programada.

Errores

`InvalidRequestException`

El contenido de la solicitud no es válido.

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

`LimitExceededException`

Se ha superado un límite.

ListScheduledAudits

Muestra una lista de las auditorías programadas.

Sinopsis

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

Formato `cli-input-json`

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

Campos **`cli-input-json`**

Nombre	Tipo	Descripción
nextToken	cadena	El token del conjunto siguiente de resultados.
maxResults	entero Rango máx.: 250; mín.: 1	El número máximo de resultados que devolver a la vez. El valor predeterminado es 25.

Output

```
{
  "scheduledAudits": [
    {
      "scheduledAuditName": "string",
      "scheduledAuditArn": "string",
      "frequency": "string",
```

```
      "dayOfMonth": "string",
      "dayOfWeek": "string"
    }
  ],
  "nextToken": "string"
}
```

Campos de salida de la CLI

Nombre	Tipo	Descripción
scheduledAudits	list miembro: ScheduledAuditMetadata Clase de Java: java.util.List	La lista de auditorías programadas.
scheduledAuditName	cadena Longitud máx.: 128; mín.: 1 Patrón: [a-zA-Z0-9_-]+	El nombre de la auditoría programada.
scheduledAuditArn	cadena	El ARN de la auditoría programada.
frequency	cadena	Frecuencia con la que se lleva a cabo la auditoría. enum: DAILY | WEEKLY | BIWEEKLY | MONTHLY
dayOfMonth	cadena patrón: ^([1-9]|[12][0-9]|3[01])$\|^LAST$	El día del mes en que se ejecuta la auditoría programada (si `frequency` es MONTHLY). Si se especifican los días 29-31 y el mes no tiene tantos días, la auditoría se realizará el último (LAST) día del mes.

Nombre	Tipo	Descripción
dayOfWeek	cadena	El día de la semana en que se ejecuta la auditoría programada (si `frequency` es WEEKLY o BIWEEKLY). enum: SUN | MON | TUE | WED | THU | FRI | SAT
nextToken	cadena	Un token que se puede utilizar para recuperar el siguiente conjunto de resultados o `null` si no hay resultados adicionales.

Errores

`InvalidRequestException`

El contenido de la solicitud no es válido.

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

DescribeScheduledAudit

Obtiene información acerca de una auditoría programada.

Sinopsis

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

Formato `cli-input-json`

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

Campos **`cli-input-json`**

Nombre	Tipo	Descripción
scheduledAuditName	cadena Longitud máx.: 128; mín.: 1 Patrón: [a-zA-Z0-9_-]+	El nombre de la auditoría programada cuya información desea obtener.

Output

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

Campos de salida de la CLI

Nombre	Tipo	Descripción
frequency	cadena	Frecuencia con la que se lleva a cabo la auditoría. Uno entre DAILY, WEEKLY, BIWEEKLY o MONTHLY. El sistema determina la hora de inicio real de cada auditoría.

Nombre	Tipo	Descripción
		enum: DAILY | WEEKLY | BIWEEKLY | MONTHLY
dayOfMonth	cadena patrón: ^([1-9]|[12][0-9]|3[01])$\|^LAST$	El día del mes en que tiene lugar la auditoría programada. Puede ser de 1 a 31 o LAST. Si se especifican los días 29-31 y el mes no tiene tantos días, la auditoría se realizará el último (LAST) día del mes.
dayOfWeek	cadena	El día de la semana en que tiene lugar la auditoría programada. Uno entre SUN, MON, TUE, WED, THU, FRI o SAT. enum: SUN | MON | TUE | WED | THU | FRI | SAT
targetCheckNames	list miembro: AuditCheckName	Controles que se realizan durante la auditoría programada. Las comprobaciones deben activarse para su cuenta. (Utilice `DescribeAccountAuditConfiguration` para ver la lista de todas las comprobaciones, incluidas las habilitadas o `UpdateAccountAuditConfiguration` para seleccionar las comprobaciones habilitadas).

Nombre	Tipo	Descripción
scheduledAuditName	cadena Longitud máx.: 128; mín.: 1 Patrón: [a-zA-Z0-9_-]+	El nombre de la auditoría programada.
scheduledAuditArn	cadena	El ARN de la auditoría programada.

Errores

`InvalidRequestException`

El contenido de la solicitud no es válido.

`ResourceNotFoundException`

El recurso especificado no existe.

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

UpdateScheduledAudit

Actualiza una auditoría programada, que incluye las comprobaciones que se realizan y con qué frecuencia se lleva a cabo la auditoría.

Sinopsis

```
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]
```

Formato `cli-input-json`

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

Campos **`cli-input-json`**

Nombre	Tipo	Descripción
frequency	cadena	Frecuencia con la que se lleva a cabo la auditoría. Puede ser DAILY, WEEKLY, BIWEEKLY o MONTHLY. El sistema determina la hora de inicio real de cada auditoría. enum: DAILY | WEEKLY | BIWEEKLY | MONTHLY
dayOfMonth	cadena patrón: ^([1-9]|[12][0-9]|3[01])$\|^LAST$	El día del mes en que tiene lugar la auditoría programada. Puede ser de 1 a 31 o LAST. Este campo es obligatorio si el parámetro `frequency` se establece en MONTHLY. Si se especifican los días 29-31 y el mes no tiene tantos días, la auditoría se realizará el último (LAST) día del mes.

Nombre	Tipo	Descripción
dayOfWeek	cadena	El día de la semana en que tiene lugar la auditoría programada. Puede ser SUN, MON, TUE,WED, THU, FRI o SAT. Este campo es obligatorio si el parámetro `frequency` se establece en WEEKLY o BIWEEKLY. enum: SUN | MON | TUE | WED | THU | FRI | SAT
targetCheckNames	list miembro: AuditCheckName	Controles que se realizan durante la auditoría programada. Las comprobaciones deben activarse para su cuenta. (Utilice `DescribeAccountAuditConfiguration` para ver la lista de todas las comprobaciones, incluidas las habilitadas o `UpdateAccountAuditConfiguration` para seleccionar las comprobaciones habilitadas).
scheduledAuditName	cadena Longitud máx.: 128; mín.: 1 Patrón: [a-zA-Z0-9_-]+	El nombre de la auditoría programada. (Máximo de 128 caracteres)

Output

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

```
}
```

Campos de salida de la CLI

Nombre	Tipo	Descripción
scheduledAuditArn	cadena	El ARN de la auditoría programada.

Errores

`InvalidRequestException`

El contenido de la solicitud no es válido.

`ResourceNotFoundException`

El recurso especificado no existe.

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

DeleteScheduledAudit

Elimina una auditoría programada.

Sinopsis

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

Formato `cli-input-json`

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

```
}
```

Campos **`cli-input-json`**

Nombre	Tipo	Descripción
scheduledAuditName	cadena Longitud máx.: 128; mín.: 1 Patrón: [a-zA-Z0-9_-]+	El nombre de la auditoría programada que desea borrar.

Output

Ninguno

Errores

`InvalidRequestException`

El contenido de la solicitud no es válido.

`ResourceNotFoundException`

El recurso especificado no existe.

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

Ejecutar una auditoría bajo demanda

Utilice `StartOnDemandAuditTask` para especificar las comprobaciones que desea realizar y comenzar una auditoría de inmediato.

StartOnDemandAuditTask

Comienza una auditoría de Device Defender bajo demanda.

Sinopsis

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

Formato `cli-input-json`

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

Campos **`cli-input-json`**

Nombre	Tipo	Descripción
targetCheckNames	list miembro: AuditCheckName	Controles que se realizan durante la auditoría. Las comprobaciones que especifiq ue deben estar habilitadas para su cuenta o se producirá una excepción. Utilice `DescribeAccountAuditConfiguration` para ver la lista de todas las comprobaciones, incluidas las habilitadas o `UpdateAccountAuditConfiguration` para seleccionar las comprobaciones habilitadas.

Output

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

```
}
```

Campos de salida de la CLI

Nombre	Tipo	Descripción
taskId	cadena Longitud máx.: 40; mín.: 1 Patrón: [a-zA-Z0-9-]+	El ID de la auditoría bajo demanda que comenzó.

Errores

`InvalidRequestException`

El contenido de la solicitud no es válido.

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

`LimitExceededException`

Se ha superado un límite.

Administrar instancias de auditoría

Utilice `DescribeAuditTask` para obtener información sobre una instancia de auditoría específica. Si ya se ha ejecutado, los resultados incluyen las comprobaciones fallidas y las correctas, aquellas que el sistema no ha podido completar y, si la auditoría aún está en curso, aquellas en las que todavía está trabajando.

Utilice `ListAuditTasks` para buscar las auditorías que se ejecutaron durante un intervalo de tiempo específico.

Utilice `CancelAuditTask` para parar una auditoría en curso.

DescribeAuditTask

Obtiene información acerca de una auditoría de Device Defender.

Sinopsis

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

Formato `cli-input-json`

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

Campos **`cli-input-json`**

Nombre	Tipo	Descripción
taskId	cadena Longitud máx.: 40; mín.: 1 Patrón: [a-zA-Z0-9-]+	El ID de la auditoría cuya información desea obtener.

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"
    }
  }
}
```

Campos de salida de la CLI

Nombre	Tipo	Descripción
taskStatus	cadena	El estado de la auditoría: uno entre IN_PROGRESS, COMPLETED, FAILED o CANCELED. enum: IN_PROGRESS | COMPLETED | FAILED | CANCELED
taskType	cadena	El tipo de auditoría: ON_DEMAND_AUDIT_TASK r SCHEDULED_AUDIT_TASK. enum: ON_DEMAND _AUDIT_TASK | SCHEDULED _AUDIT_TASK
taskStartTime	marca de tiempo	La hora a la que se inició la auditoría.
taskStatistics	TaskStatistics	Información estadística sobre la auditoría.

Nombre	Tipo	Descripción
totalChecks	entero	El número de comprobaciones de esta auditoría.
inProgressChecks	entero	El número de comprobaciones en curso.
waitingForDataCollectionChecks	entero	El número de comprobaciones en espera de recopilación de datos.
compliantChecks	entero	El número de comprobaciones que encontraron recursos conformes.
nonCompliantChecks	entero	El número de comprobaciones que encontraron recursos no conformes.
failedChecks	entero	El número de comprobac iones.
canceledChecks	entero	El número de comprobaciones no ejecutadas debido a la cancelación de la auditoría.
scheduledAuditName	cadena Longitud máx.: 128; mín.: 1 Patrón: [a-zA-Z0-9_-]+	El nombre de la auditoría programada (solo si la auditoría era una auditoría programada).
auditDetails	map	Información detallada sobre cada comprobación realizada durante esta auditoría.

Nombre	Tipo	Descripción
checkRunStatus	cadena	El estado de finalización de esta comprobación, una entre IN_PROGRESS, WAITING_FOR_DATA_COLLECTION, CANCELED, COMPLETED_COMPLIANT, COMPLETED_NON_COMPLIANT o FAILED. enum: IN_PROGRESS | WAITING_FOR_DATA_COLLECTION | CANCELED | COMPLETED_COMPLIANT | COMPLETED_NON_COMPLIANT | FAILED
checkCompliant	booleano	True si se ha completado la comprobación y se ha detectado que todos los recursos son conformes.
totalResourcesCount	long	El número de recursos en los que se ha realizado la comprobación.
nonCompliantResourcesCount	long	El número de recursos que la comprobación ha encontrado que no son conformes.
errorCode	cadena	El código de cualquier error encontrado al realizar esta comprobación durante esta auditoría. Uno entre INSUFFICIENT_PERMISSIONS o AUDIT_CHECK_DISABLED.

Nombre	Tipo	Descripción
message	cadena Longitud máx.: 2048	El mensaje asociado con cualquier error encontrado al realizar esta comprobación durante esta auditoría.

Errores

`InvalidRequestException`

El contenido de la solicitud no es válido.

`ResourceNotFoundException`

El recurso especificado no existe.

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

ListAuditTasks

Muestra una lista de las auditorías de Device Defender que se han realizado durante un periodo de tiempo determinado.

Sinopsis

```
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]
```

Formato `cli-input-json`

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

Campos **`cli-input-json`**

Nombre	Tipo	Descripción
startTime	marca de tiempo	El comienzo del periodo de tiempo. La información de auditoría se conserva durante un tiempo limitado (180 días). Si se solicita una hora de inicio anterior al tiempo de retención, se produce la excepción `InvalidRequestException` .
endTime	marca de tiempo	El final del periodo de tiempo.
taskType	cadena	Un filtro para limitar el resultado al tipo de auditoría especificado: puede ser uno entre ON_DEMAND_AUDIT_TASK o SCHEDULED__AUDIT_TASK. enum: ON_DEMAND_AUDIT_TASK | SCHEDULED_AUDIT_TASK

Nombre	Tipo	Descripción
taskStatus	cadena	Un filtro para limitar el resultado a las auditorías con el estado de finalizac ión especificado: puede ser uno entre IN_PROGRESS, COMPLETED, FAILED o CANCELED. enum: IN_PROGRESS | COMPLETED | FAILED | CANCELED
nextToken	cadena	El token del conjunto siguiente de resultados.
maxResults	entero Rango máx.: 250; mín.: 1	El número máximo de resultados que devolver a la vez. El valor predeterminado es 25.

Output

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

Campos de salida de la CLI

Nombre	Tipo	Descripción
tareas	list miembro: AuditTaskMetadata Clase de Java: java.util.List	Las auditorías que se realizaron durante el periodo de tiempo especificado.
taskId	cadena Longitud máx.: 40; mín.: 1 Patrón: [a-zA-Z0-9-]+	El ID de esta auditoría.
taskStatus	cadena	El estado de esta auditoría: uno entre IN_PROGRESS, COMPLETED, FAILED o CANCELED. enum: IN_PROGRESS | COMPLETED | FAILED | CANCELED
taskType	cadena	El tipo de esta auditoría: uno entre ON_DEMAND_AUDIT_TASK o SCHEDULED_AUDIT_TASK. enum: ON_DEMAND_AUDIT_TASK | SCHEDULED_AUDIT_TASK
nextToken	cadena	Un token que se puede utilizar para recuperar el siguiente conjunto de resultados o `null` si no hay resultados adicionales.

Errores

`InvalidRequestException`

El contenido de la solicitud no es válido.

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

CancelAuditTask

Cancela una auditoría que está en curso. La auditoría puede ser programada o bajo demanda. Si la auditoría no está en curso, se produce la excepción `InvalidRequestException`.

Sinopsis

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

Formato `cli-input-json`

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

Campos **`cli-input-json`**

Nombre	Tipo	Descripción
taskId	cadena Longitud máx.: 40; mín.: 1 Patrón: [a-zA-Z0-9-]+	ID de la auditoría que desea cancelar. Solo puede cancelar una auditoría que esté IN_PROGRESS.

Output

Ninguno

Errores

`ResourceNotFoundException`

El recurso especificado no existe.

`InvalidRequestException`

El contenido de la solicitud no es válido.

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

Comprobar resultados de auditoría

Utilice `ListAuditFindings` para ver los resultados de una auditoría. Puede filtrar los resultados por el tipo de comporbación, por recurso específico o por la hora de la auditoría. Puede utilizar esta información para mitigar cualquier problema que se encuentre.

Puede definir acciones de mitigación y aplicarlas a los resultados de su auditoría. Para obtener más información, consulte Acciones de mitigación.

ListAuditFindings

Muestra una lista de los resultados (resultados) de una auditoría de Device Defender o de las auditorías realizadas durante un periodo de tiempo especificado. (Los resultados se conservan durante 180 días).

Sinopsis

```
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]
```

Formato `cli-input-json`

```
{
  "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"
}
```

Campos **`cli-input-json`**

Nombre	Tipo	Descripción
taskId	cadena Longitud máx.: 40; mín.: 1 Patrón: [a-zA-Z0-9-]+	Un filtro para limitar los resultados a la auditoría que tiene el ID especificado. Debe especificar taskId o startTime y endTime, pero no ambos.
checkName	cadena	Un filtro para limitar los resultados a los resultados

Nombre	Tipo	Descripción
		de la verificación de auditoría especificada.
resourceIdentifier	ResourceIdentifier	La información que identifica el recurso no conforme.
deviceCertificateId	cadena Longitud máx.: 64; mín.: 64 Patrón: (0x)?[a-fA-F0-9]+	El ID del certificado asociado al recurso.
caCertificateId	cadena Longitud máx.: 64; mín.: 64 Patrón: (0x)?[a-fA-F0-9]+	El ID del certificado de entidad de certificación utilizado para autorizar el certificado.
cognitoIdentityPoolId	cadena	El ID del grupo de identidades de Amazon Cognito.
clientId	cadena	El ID de cliente.
policyVersionIdentifier	PolicyVersionIdentifier	La versión de la política asociada a este recurso.
policyName	cadena Longitud máx.: 128; mín.: 1 patrón: [w+=,.@-]+	El nombre de la política de .
policyVersionId	cadena Patrón: [0-9]+	El ID de la versión de la política asociada a este recurso.

Nombre	Tipo	Descripción
roleAliasArn	cadena	El ARN del alias de rol que tiene acciones excesivamente permisivas. Longitud: máx.: 2048; mín.: 1
inscrita	cadena Longitud máx.: 12; mín.: 12 Patrón: [0-9]+	La cuenta a la que está asociado el recurso.
maxResults	entero Rango máx.: 250; mín.: 1	El número máximo de resultados que devolver a la vez. El valor predeterminado es 25.
nextToken	cadena	El token del conjunto siguiente de resultados.
startTime	marca de tiempo	Un filtro para limitar los resultados a los encontrad os después de la hora especificada. Debe especificar startTime y endTime o taskId, pero no ambos.
endTime	marca de tiempo	Un filtro para limitar los resultados a los encontrados antes de la hora especificada. Debe especificar startTime y endTime o taskId, pero no ambos.

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"
}
```

Campos de salida de la CLI

Nombre	Tipo	Descripción
findings	list miembro: AuditFinding	Los resultados (resultados) de la auditoría.
taskId	cadena Longitud máx.: 40; mín.: 1 Patrón: [a-zA-Z0-9-]+	El ID de la auditoría que generó este resultado (resultado).
checkName	cadena	La comprobación de auditoría que generó este resultado.
taskStartTime	marca de tiempo	La hora a la que se inició la auditoría.
findingTime	marca de tiempo	La hora a la que se descubrió el resultado (resultado).
severity	cadena	La gravedad del resultado (resultado). enum: CRÍTICA | ALTA | MEDIA | BAJA

Nombre	Tipo	Descripción
nonCompliantResource	NonCompliantResource	El recurso que se ha comprobado que no cumple los requisitos de una comprobación de auditoría.
resourceType	cadena	El tipo del recurso no conforme. enum: DEVICE_CERTIFICATE | CA_CERTIFICATE | IOT_POLICY | COGNITO_IDENTITY_POOL | CLIENT_ID | ACCOUNT_SETTINGS
resourceIdentifier	ResourceIdentifier	La información que identifica el recurso no conforme.
deviceCertificateId	cadena Longitud máx.: 64; mín.: 64 Patrón: (0x)?[a-fA-F0-9]+	El ID del certificado asociado al recurso.
caCertificateId	cadena Longitud máx.: 64; mín.: 64 Patrón: (0x)?[a-fA-F0-9]+	El ID del certificado de entidad de certificación utilizado para autorizar el certificado.
cognitoIdentityPoolId	cadena	El ID del grupo de identidades de Amazon Cognito.
clientId	cadena	El ID de cliente.
policyVersionIdentifier	PolicyVersionIdentifier	La versión de la política asociada a este recurso.

Nombre	Tipo	Descripción
policyName	cadena Longitud máx.: 128; mín.: 1 patrón: [w+=,.@-]+	El nombre de la política de .
policyVersionId	cadena Patrón: [0-9]+	El ID de la versión de la política asociada a este recurso.
inscrita	cadena Longitud máx.: 12; mín.: 12 Patrón: [0-9]+	La cuenta a la que está asociado el recurso.
additionalInfo	map	Otra información sobre el recurso no conforme.
relatedResources	list miembro: RelatedResource	La lista de recursos relaciona dos.
resourceType	cadena	El tipo de recurso. enum: DEVICE_CE RTIFICATE | CA_CERTIF ICATE | IOT_POLICY | COGNITO_IDENTITY_POOL | CLIENT_ID | ACCOUNT_S ETTINGS
resourceIdentifier	ResourceIdentifier	Información que identifica el recurso.

Nombre	Tipo	Descripción
deviceCertificateId	cadena Longitud máx.: 64; mín.: 64 Patrón: (0x)?[a-fA-F0-9]+	El ID del certificado asociado al recurso.
caCertificateId	cadena Longitud máx.: 64; mín.: 64 Patrón: (0x)?[a-fA-F0-9]+	El ID del certificado de entidad de certificación utilizado para autorizar el certificado.
cognitoIdentityPoolId	cadena	El ID del grupo de identidades de Amazon Cognito.
clientId	cadena	El ID de cliente.
policyVersionIdentifier	PolicyVersionIdentifier	La versión de la política asociada a este recurso.
iamRoleArn	cadena Longitud máx.: 2048; mín.: 20	El ARN del rol de IAM que tiene acciones excesivamente permisivas.
policyName	cadena Longitud máx.: 128; mín.: 1 patrón: [w+=,.@-]+	El nombre de la política de .
policyVersionId	cadena Patrón: [0-9]+	El ID de la versión de la política asociada a este recurso.
roleAliasArn	cadena Longitud: máx.: 2048; mín.: 1	El ARN del alias de rol que tiene acciones excesivamente permisivas.

Nombre	Tipo	Descripción
inscrita	cadena Longitud máx.: 12; mín.: 12 Patrón: [0-9]+	La cuenta a la que está asociado el recurso.
additionalInfo	map	Otra información sobre el recurso.
reasonForNonCompliance	cadena	El motivo por el que el recurso no era conforme.
reasonForNonCompliance Code	cadena	Un código que indica el motivo por el cual el recurso no era conforme.
nextToken	cadena	Un token que se puede utilizar para recuperar el siguiente conjunto de resultados o `null` si no hay resultados adicionales.

Errores

`InvalidRequestException`

El contenido de la solicitud no es válido.

`ThrottlingException`

El índice supera el límite.

`InternalFailureException`

Se ha producido un error inesperado.

Supresiones de resultados de auditoría

Cuando realiza una auditoría, esta informa de los resultados de todos los recursos no conformes. Esto significa que sus informes de auditoría incluyen los resultados de los recursos en los que está trabajando para mitigar los problemas y también de los recursos que se sabe que no son conformes, como los dispositivos de prueba o los que están averiados. La auditoría sigue informando sobre los resultados de los recursos que siendo no conformes en sucesivas auditorías, lo que puede agregar información no deseada a los informes. La supresión de los resultados de auditoría permite suprimir o filtrar los resultados durante un período de tiempo definido hasta que el recurso se repare, o indefinidamente en el caso de un recurso asociado a una prueba o a un dispositivo averiado.

> **Note**
>
> Las acciones de mitigación no estarán disponibles para los resultados de auditoría suprimidos. Para obtener información sobre las acciones de mitigación, consulte Acciones de mitigación.

Para obtener información sobre las cuotas de supresión de resultados de auditoría, consulte Puntos de enlace y cuotas de AWS IoT Device Defender.

Cómo funcionan las supresiones de resultados de auditoría

Cuando se crea una forma de suprimir los resultados de una auditoría para un recurso no conforme, los informes de auditoría y las notificaciones se comportan de forma diferente.

Los informes de auditoría incluirán una nueva sección en la que se enumeran todos los resultados suprimidos asociados al informe. Los resultados suprimidos no se tendrán en cuenta a la hora de evaluar si una comprobación de auditoría es conforme o no. También se devuelve un recuento de recursos suprimidos para cada comprobación de auditoría cuando se utiliza el comando describe-audit-task en la interfaz de la línea de comandos (CLI).

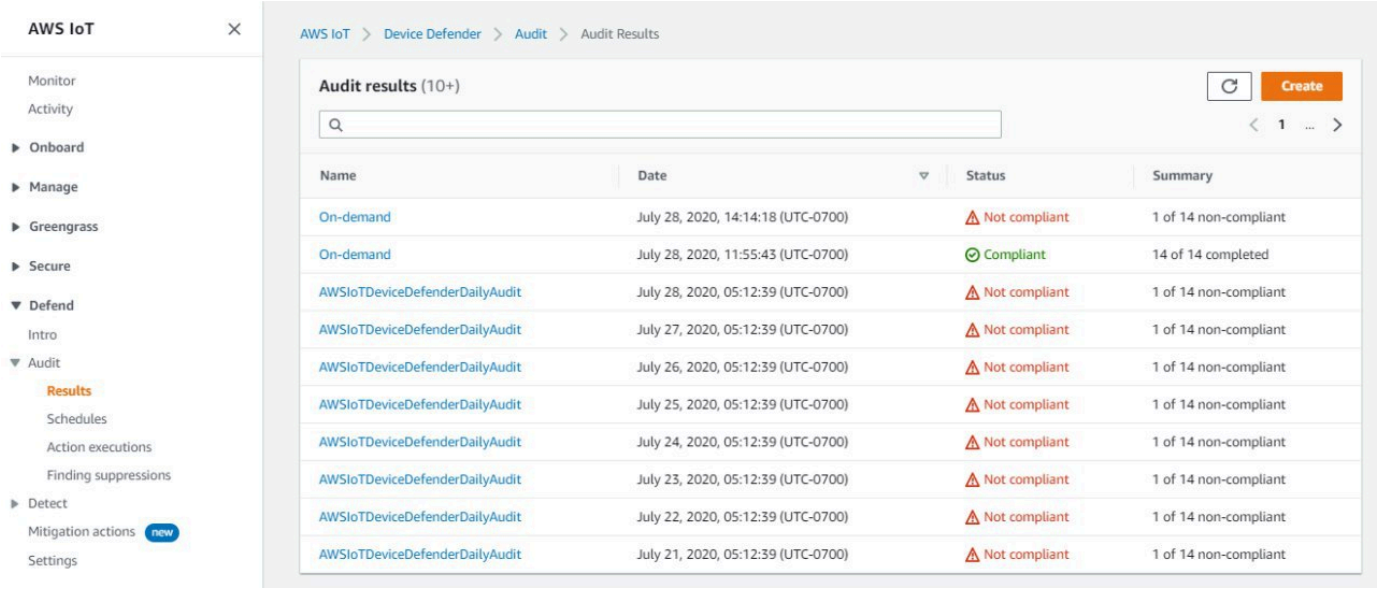
Para las notificaciones de auditoría, los resultados suprimidos no se tienen en cuenta cuando evaluamos si una comprobación de auditoría es conforme o no. También se incluye un recuento de recursos suprimidos en cada notificación de auditoría publicada por AWS IoT Device Defender en Amazon CloudWatch y Amazon Simple Notification Service (Amazon SNS).

Cómo utilizar las supresiones de los resultados de auditoría en la consola

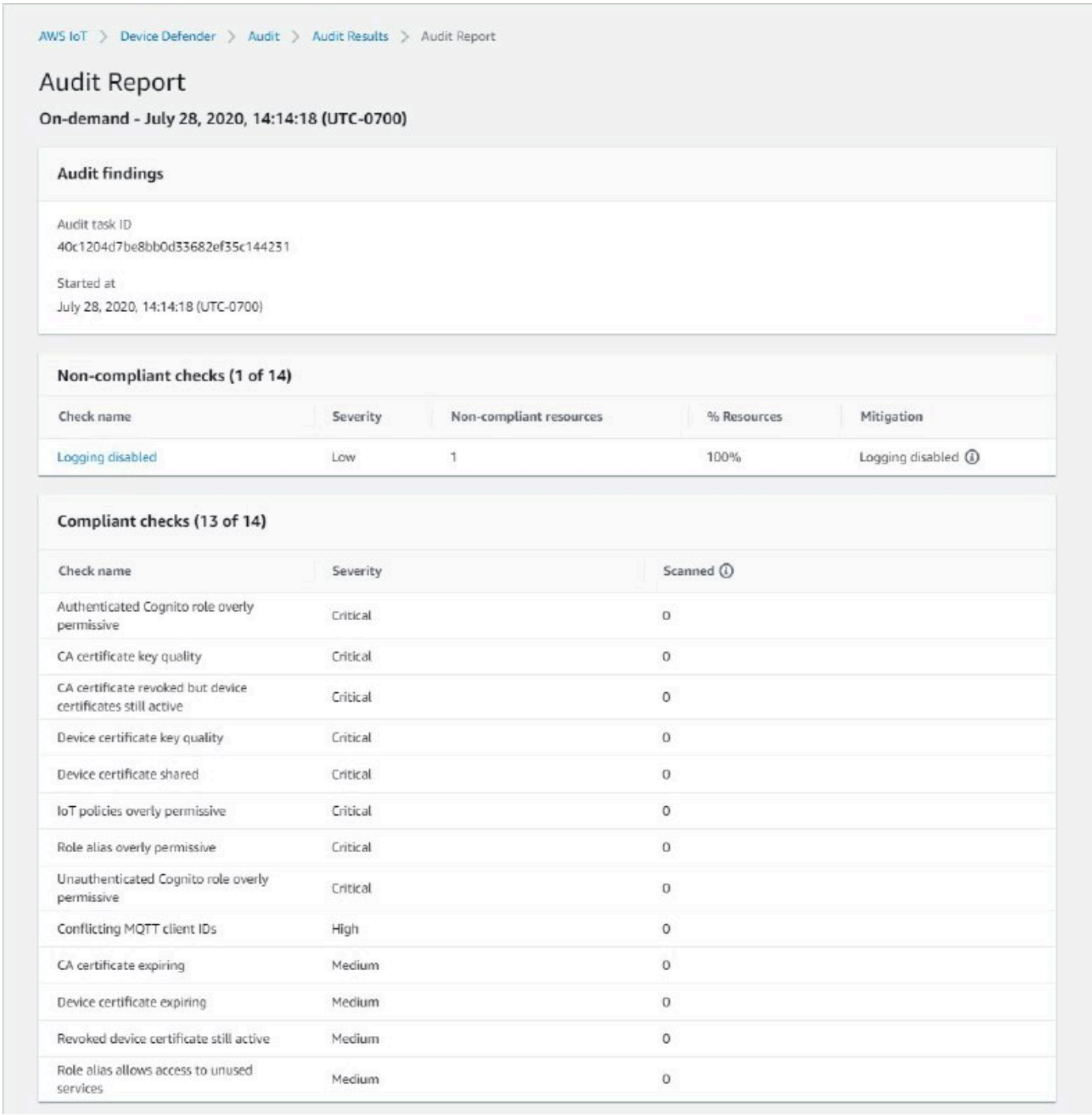
Para suprimir un resultado de un informe de auditoría

El siguiente procedimiento le muestra cómo crear una supresión de resultado de auditoría en la consola de AWS IoT.

1. En la consola deAWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Audit y Resultados.
2. Seleccione un informe de auditoría que quiera revisar.

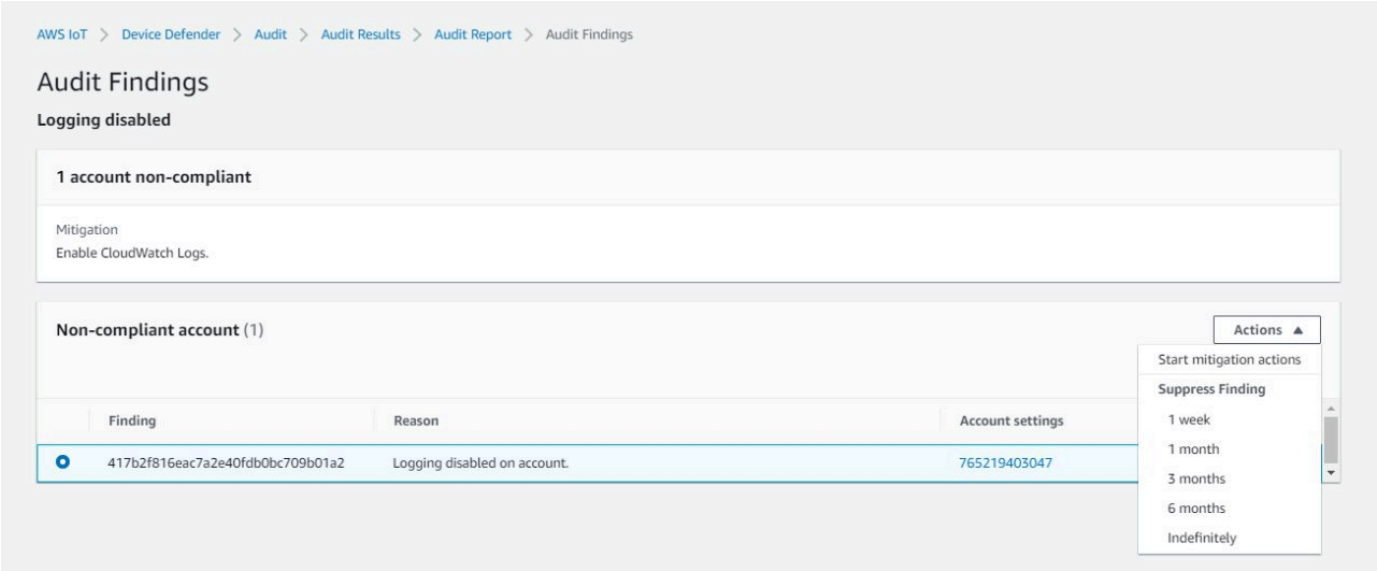


3. En la sección Comprobaciones de no conformidad, en Nombre de comprobación, elija la comprobación de auditoría que le interese.

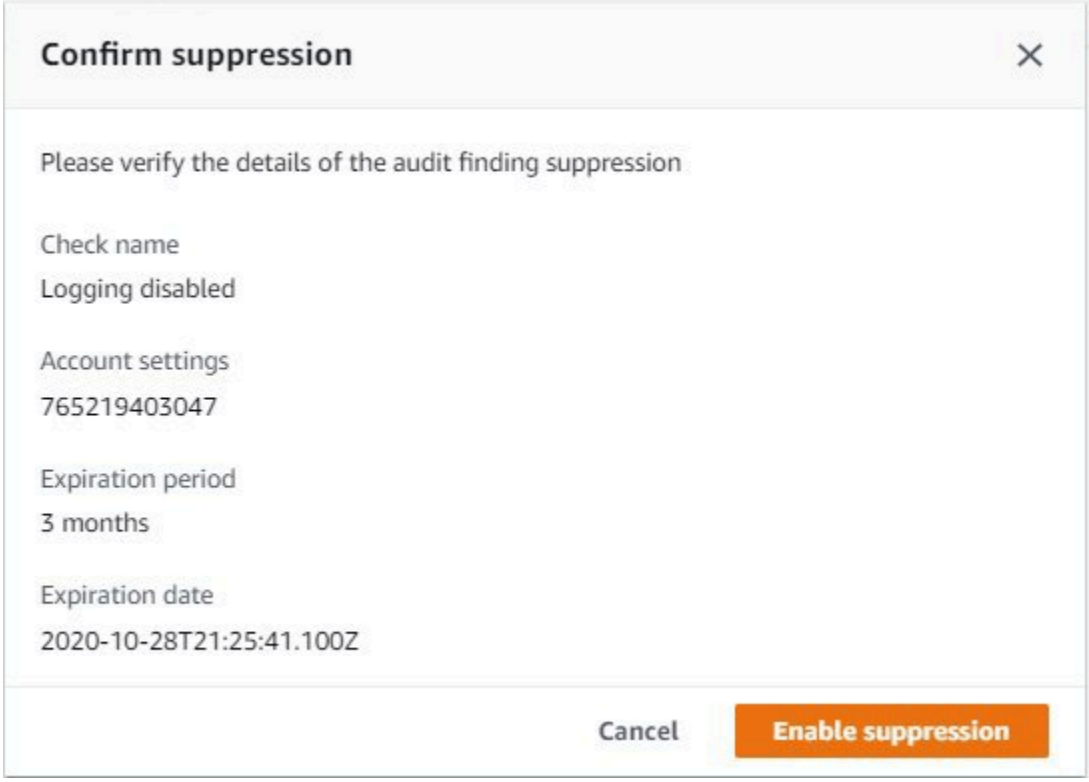


4. En la pantalla de detalles de la comprobación de auditoría, si hay algún resultado que no quiera ver, seleccione el botón de opción situado junto al resultado. A continuación, seleccione Acciones y luego elija el tiempo durante el que quiere que se mantenga la supresión de los resultados de auditoría.

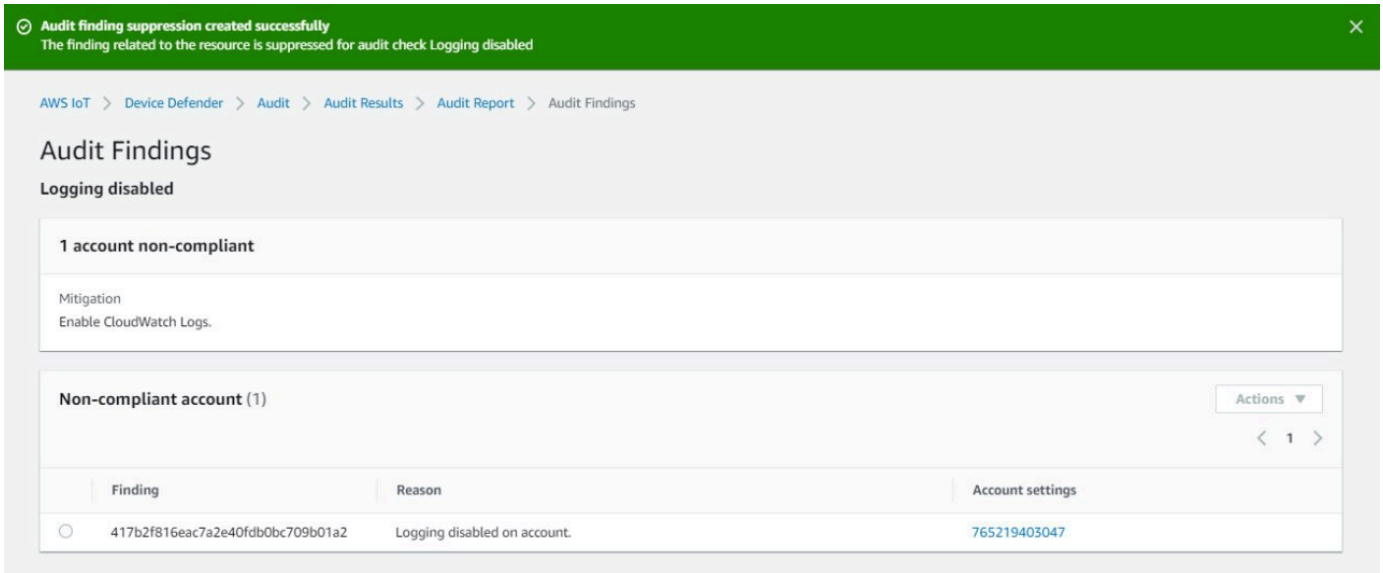
> **Note**
>
> En la consola, puede seleccionar 1 semana, 1 mes, 3 meses, 6 meses o Indefinidamente como fechas de caducidad para la supresión de los resultados de auditoría. Si quiere establecer una fecha de caducidad específica, solo puede hacerlo en la CLI o la API. Las omisiones de los resultados de auditoría también se pueden cancelar en cualquier momento, independientemente de la fecha de caducidad.



5. Confirme los detalles de la supresión y, a continuación, seleccione Habilitar la supresión.



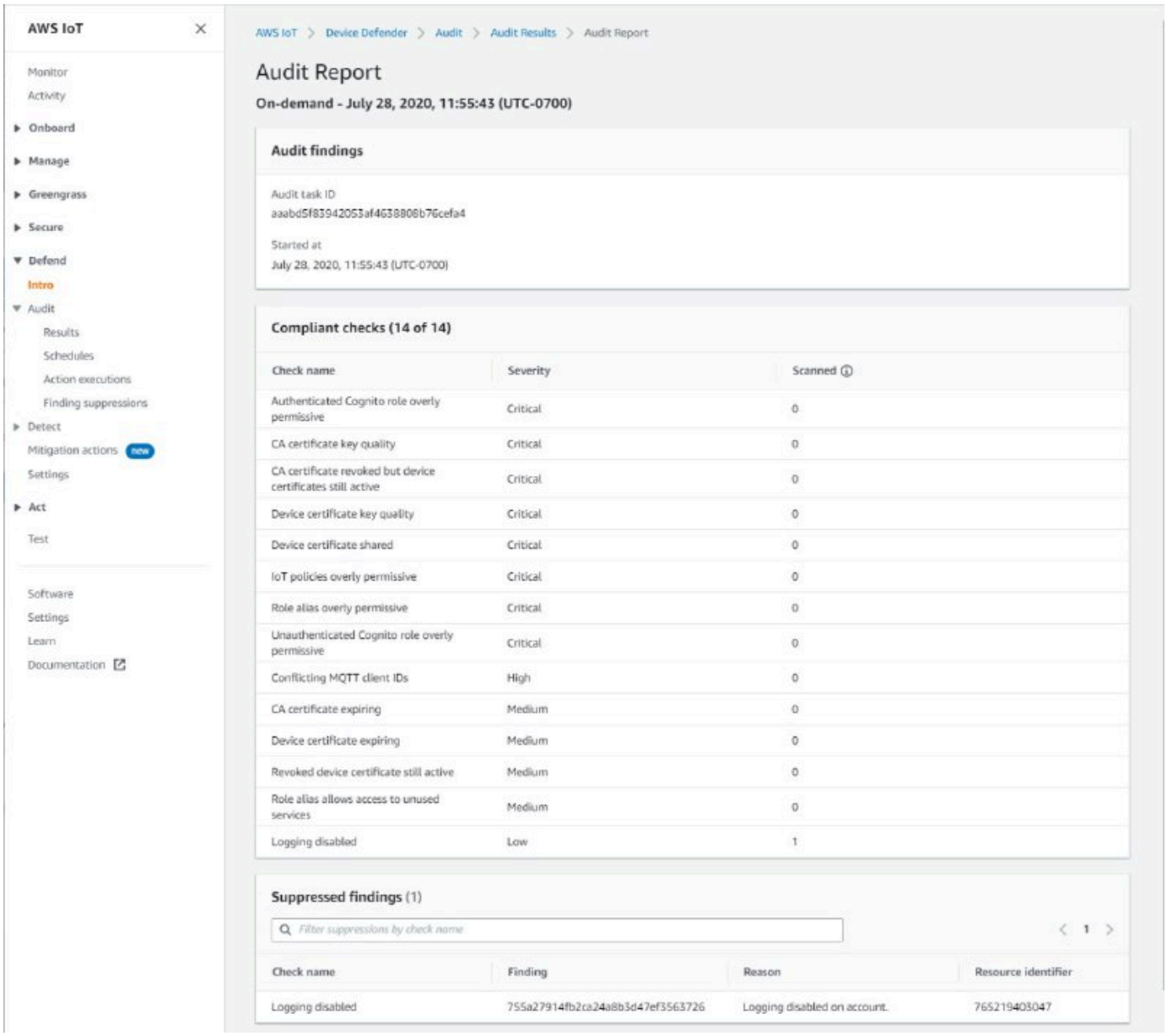
6. Una vez que haya creado la supresión de los resultados de auditoría, aparecerá un banner confirmando que se ha creado la supresión de los resultados de auditoría.



Para ver los resultados suprimidos en un informe de auditoría

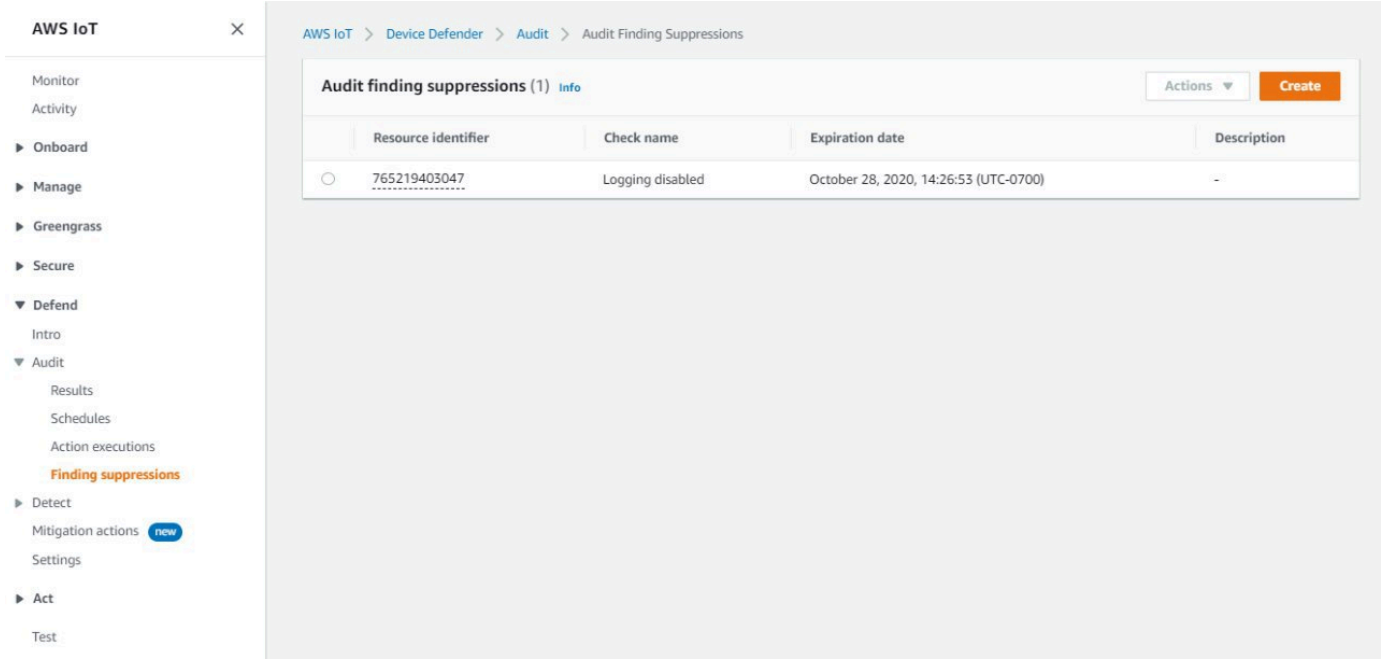
1. En la consola deAWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Audit y Resultados.

2. Seleccione un informe de auditoría que quiera revisar.
3. En la sección Hallazgos suprimidos, consulte qué resultados de auditoría se han suprimido para el informe de auditoría que ha elegido.



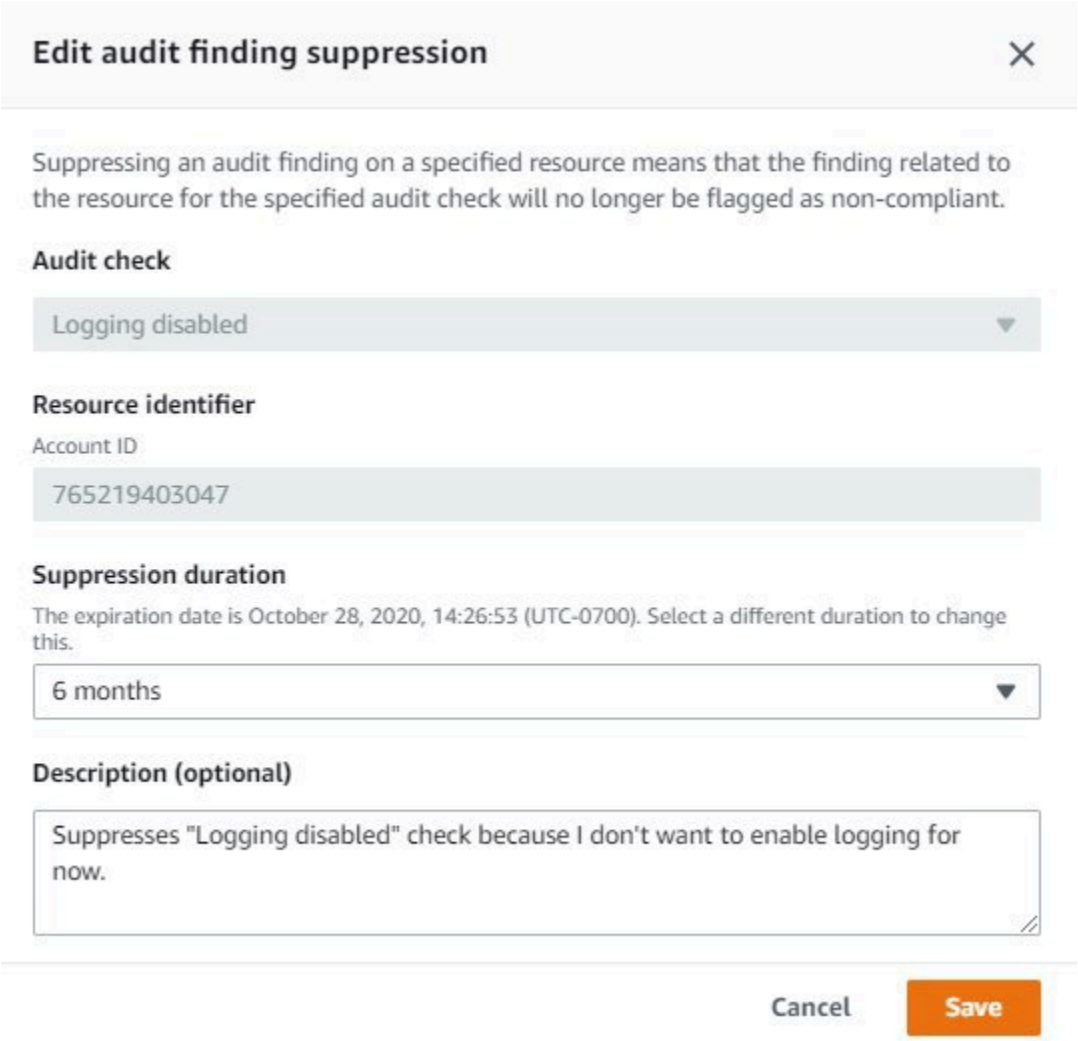
Para enumerar las supresiones de resultados de auditoría

- En la consola deAWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Audit y Supresiones de resultados.



Para editar las supresiones de resultados de auditoría

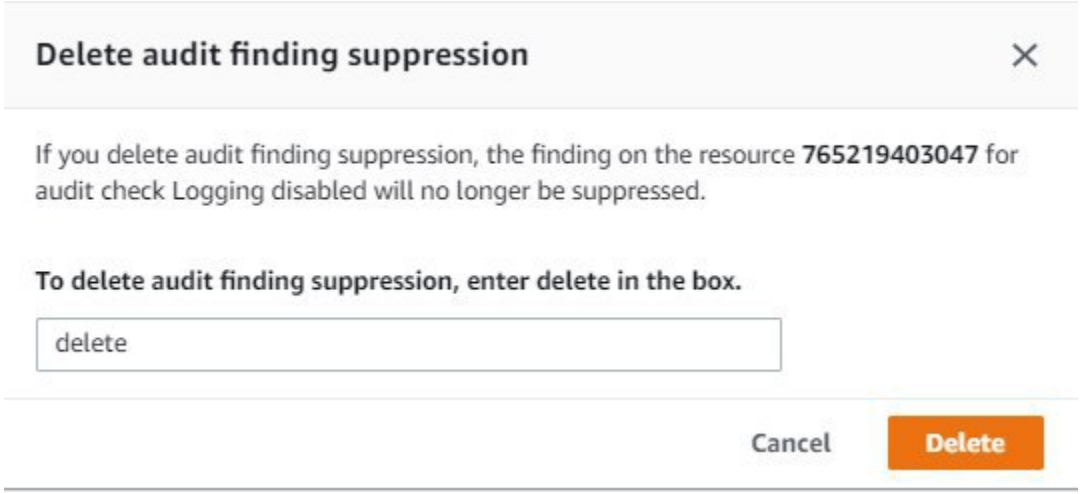
1. En la consola deAWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Audit y Supresiones de resultados.
2. Seleccione el botón de opción situado junto al resultado de auditoría que quiera editar. Luego elija Acciones, Editar.
3. En la ventana Editar las supresiones de resultados de auditoría, puede cambiar la duración de la supresión o la descripción (opcional).



4. Una vez realizados los cambios, elija Guardar. Se abre la ventana Supresiones de resultados.

Para eliminar la supresión de un resultado de auditoría

1. En la consola deAWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Audit y Supresiones de resultados.
2. Seleccione el botón de opción situado junto a la supresión de resultado de auditoría que quiera eliminar y, a continuación, elija Acciones, Eliminar..
3. En la ventana Eliminar supresión de resultado de auditoría, introduzca `delete` en el cuadro de texto para confirmar la eliminación y, a continuación, seleccione Eliminar. Se abre la ventana Supresiones de resultados.



Cómo utilizar las supresiones de resultados de auditoría en la CLI

Puede utilizar los siguientes comandos de la CLI para crear y administrar supresiones de resultados de auditoría.

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

La entrada `resource-identifier` que introduzca dependerá de la `check-name` para la que esté suprimiendo los resultados. En la siguiente tabla se detallan qué comprobaciones requieren qué `resource-identifier` para crear y editar las supresiones.

> **Note**
>
> Los comandos de supresión no indican la desactivación de una auditoría. Las auditorías seguirán ejecutándose en sus dispositivos AWS IoT. Las supresiones solo se aplican a los resultados de la auditoría.

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

Para crear y aplicar una supresión de resultado de auditoría

El siguiente procedimiento le muestra cómo crear una supresión de resultado de auditoría en la AWS CLI.

- Utilice el comando `create-audit-suppression` para crear una supresión de resultados de auditoría. En el siguiente ejemplo, se crea una supresión de resultados de auditoría para Cuenta de AWS *123456789012* en función de la comprobación Registro deshabilitado.

```
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."
```

  No hay ningún resultado para este comando.

API de supresiones de resultados de auditoría

Las siguientes API pueden utilizarse para crear y administrar supresiones de resultados de auditoría.

- CreateAuditSuppression
- DescribeAuditSuppression
- UpdateAuditSuppression
- DeleteAuditSuppression
- ListAuditSuppressions

Para filtrar resultados de auditoría específicos, puede usar la API ListAuditFindings.

Detect

AWS IoT Device Defender Detect permite identificar comportamientos inusuales que podrían indicar que un dispositivo se ha visto comprometido cuando se monitoriza el comportamiento de los dispositivos. Si utiliza una combinación de métricas del lado de la nube (procedentes de AWS IoT) y de métricas del lado del dispositivo (procedentes de agentes instalados en los dispositivos), puede detectar:

- Cambios en los patrones de conexión.
- Dispositivos que se comunican con puntos de conexión no autorizados o no reconocidos.
- Cambios en los patrones de tráfico de entrada y salida de los dispositivos.

Cree perfiles de seguridad, que contengan definiciones de comportamientos esperados de los dispositivos y asígnelos a un grupo de dispositivos o a todos los dispositivos de su flota. AWS IoT Device Defender Detect utiliza estos perfiles de seguridad para detectar anomalías y enviar alarmas a través de las métricas de Amazon CloudWatch y las notificaciones de Amazon Simple Notification Service.

AWS IoT Device Defender Detect puede detectar problemas de seguridad que se producen con frecuencia en los dispositivos conectados:

- Tráfico desde un dispositivo a una dirección IP maliciosa conocida o a un punto de conexión no autorizado que indica un posible comando y canal de control maliciosos.
- Tráfico anómalo, como un pico en el tráfico saliente, que indica que un dispositivo participa en un DDoS.
- Dispositivos con puertos e interfaces de administración remota a los que se puede acceder de forma remota.
- Un pico en el índice de mensajes que se envían a la cuenta (por ejemplo, desde un dispositivo fraudulento, lo que podría producir unos gastos excesivos por mensaje).

Casos de uso

Medir la superficie de ataque

Puede usar AWS IoT Device Defender Detect para medir la superficie de ataque de sus dispositivos. Puede, por ejemplo, identificar dispositivos con puertos de servicio que con

frecuencia son objeto de campañas de ataques (el servicio telnet que se ejecuta en los puertos 23/2323, el servicio SSH que se ejecuta en el puerto 22, los servicios HTTP/S que se ejecutan en los puertos 80/443/8080/8081). Aunque estos puertos de servicio pueden tener motivos legítimos para utilizarse en los dispositivos, también suelen formar parte de la superficie de ataque de los adversarios y llevan asociados riesgos. Una vez que AWS IoT Device Defender Detect alerta de la superficie de ataque, esta puede minimizarse (eliminando servicios de red que no se utilizan) o se pueden ejecutar otras evaluaciones para identificar debilidades de seguridad (por ejemplo, un telnet configurado con contraseñas de uso común, predeterminadas o poco seguras).

Detectar anomalías de comportamiento de dispositivos con posibles causas raíces de seguridad

Puede usar AWS IoT Device Defender Detect para alertarle sobre las métricas de comportamiento inesperado del dispositivo (el número de puertos abiertos, el número de conexiones, un puerto abierto inesperado, las conexiones a direcciones IP inesperadas) que pueden indicar una vulneración de la seguridad. Por ejemplo, un número de conexiones TCP más alto de lo esperado puede indicar que un dispositivo se está utilizando para un ataque DDoS. Un proceso que se escucha en un puerto diferente al que espera puede indicar una puerta trasera instalada en un dispositivo para control remoto. Puede usar AWS IoT Device Defender Detect para sondear el estado de las flotas de dispositivos y contrastar los supuestos de seguridad (por ejemplo, que ningún dispositivo está escuchando en el puerto 23 o 2323).

Puede habilitar la detección de amenazas basada en machine learning (ML) para identificar automáticamente posibles amenazas.

Detectar un dispositivo configurado incorrectamente

Un pico en el número o tamaño de los mensajes enviados desde un dispositivo a su cuenta puede indicar un dispositivo configurado incorrectamente. Un dispositivo como este podría aumentar los gastos por mensaje. Del mismo modo, un dispositivo con muchos errores de autorización podría requerir la reconfiguración de una política.

Monitorización del comportamiento de dispositivos no registrados

AWS IoT Device Defender Detect permite identificar comportamientos inusuales en dispositivos que no figuran en el registro de AWS IoT. Puede definir perfiles de seguridad que sean específicos de uno de los siguientes tipos de destino:

- Todos los dispositivos
- Todos los dispositivos registrados (objetos en el registro de AWS IoT)

- Todos los dispositivos no registrados
- Los dispositivos de un grupo de objetos

Un perfil de seguridad define un conjunto de comportamientos esperados para los dispositivos de su cuenta y especifica las acciones que se realizarán cuando se detecte una anomalía. Los perfiles de seguridad deben asociarse al mayor número de destinos específicos para controlar con detalle qué dispositivos se están evaluando en ese perfil.

Los dispositivos no registrados deben proporcionar un identificador de cliente de MQTT o un nombre de objeto coherentes (para los dispositivos que registran métricas de dispositivo) durante todo el ciclo de vida del dispositivo, de forma que todas las infracciones y métricas se atribuyan al mismo dispositivo.

> **Important**
>
> Los mensajes registrados por los dispositivos se rechazan si el nombre del objeto contiene caracteres de control o si el nombre del objeto tiene más de 128 bytes de caracteres con codificación UTF-8.

Casos de uso de seguridad

En esta sección, se describen los diferentes tipos de ataques que amenazan su flota de dispositivos y las métricas recomendadas que puede utilizar para monitorizar estos ataques. Le recomendamos utilizar las anomalías métricas como punto de partida para investigar los problemas de seguridad, pero no debe basar la determinación de cualquier amenaza a la seguridad únicamente en una anomalía métrica.

Para investigar una alarma de anomalía, correlacione los detalles de la alarma con otra información contextual, como los atributos del dispositivo, las tendencias históricas de las métricas del dispositivo, las tendencias históricas de las métricas del perfil de seguridad, las métricas personalizadas y los registros, para determinar si existe una amenaza a la seguridad.

Casos de uso en la nube

Device Defender puede monitorizar los siguientes casos de uso desde la nube de AWS IoT.

Robo de propiedad intelectual:

El robo de propiedad intelectual implica el robo de la propiedad intelectual de una persona o empresa, incluidos los secretos comerciales, el hardware o el software. Suele ocurrir durante la fase de fabricación de los dispositivos. El robo de propiedad intelectual puede adoptar la forma de piratería, robo de dispositivos o robo de certificados de dispositivos. El robo de propiedad intelectual basado en la nube puede ocurrir debido a la presencia de políticas que permiten el acceso no deseado a los recursos de IoT. Debería revisar sus políticas de IoT y activar las comprobaciones de auditoría excesivamente permisivas para identificar las políticas demasiado permisivas.

Métricas relacionadas:

Métrica	Justificación
IP de origen	Si se roba un dispositivo, su dirección IP de origen quedaría fuera del rango de direcciones IP normalmente esperado para los dispositivos que circulan en una cadena de suministro normal.
Número de mensajes recibidos	Como un atacante puede utilizar un dispositivo para robar una IP basada en la nube, las métricas relacionadas con el número o el tamaño de los mensajes enviados al dispositivo desde la nube de AWS IoT pueden aumentar, lo que indica un posible problema de seguridad.
Tamaño del mensaje	

Exfiltración de datos basada en MQTT:

La exfiltración de datos se produce cuando un actor malintencionado lleva a cabo una transferencia de datos no autorizada desde una implementación de IoT o desde un dispositivo. El atacante lanza este tipo de ataques a través de MQTT contra orígenes de datos del lado de la nube.

Métricas relacionadas:

Métrica	Justificación
IP de origen	Si se roba un dispositivo, su dirección IP de origen quedaría fuera del rango de direcciones IP normalmente esperado para los dispositivos que circulan en una cadena de suministro estándar.
Número de mensajes recibidos	Como un atacante puede utilizar un dispositivo de una exfiltración de datos basada en MQTT, las métricas relacionadas con el número o el tamaño de los mensajes enviados al dispositivo desde la nube de AWS IoT pueden aumentar, lo que indica un posible problema de seguridad.
Tamaño del mensaje	

Suplantación de identidad:

Un ataque de suplantación de identidad se produce cuando los atacantes se hacen pasar por entidades conocidas o de confianza en un esfuerzo por acceder a servicios, aplicaciones o datos del lado de la nube de AWS IoT o ejercer el mando y el control de los dispositivos IoT.

Métricas relacionadas:

Métrica	Justificación
Errores de autorización	Cuando los atacantes se hacen pasar por entidades de confianza utilizando identidades robadas, las métricas relacionadas con la conectividad suelen aumentar, ya que es posible que las credenciales ya no sean válidas o que ya las esté utilizando un dispositivo de confianza. Los comportamientos anómalos en los fallos de autorización, los intentos de conexión o las desconexiones
Intentos de conexión	
Desconectar	

Métrica	Justificación
	apuntan a un posible escenario de suplantac ión de identidad.

Abuso de la infraestructura de la nube:

El abuso de los servicios de AWS IoT en la nube se produce al publicar o suscribirse a temas con un gran volumen de mensajes o con mensajes de gran tamaño. Las políticas excesivamente permisivas o el aprovechamiento de las vulnerabilidades de los dispositivos con fines de mando y control también pueden provocar un abuso de la infraestructura de la nube. Uno de los principales objetivos de este ataque es aumentar su factura de AWS. Debería revisar sus políticas de IoT y activar las comprobaciones de auditoría excesivamente permisivas para identificar las políticas demasiado permisivas.

Métricas relacionadas:

Métrica	Justificación
Número de mensajes recibidos	El objetivo de este ataque es aumentar su factura de AWS, y las métricas que monitorizan actividades como el recuento de mensajes, los mensajes recibidos y el tamaño de los mensajes aumentarán.
Número de mensajes enviados	
Tamaño del mensaje	
IP de origen	Pueden aparecer listas de direcciones IP de fuentes sospechosas, a partir de las cuales los atacantes generan su volumen de mensajes.

Casos de uso del lado del dispositivo

Device Defender puede monitorizar los siguientes casos de uso desde el dispositivo.

Ataque de denegación de servicio:

Un ataque de denegación de servicio (DoS) tiene como objetivo cerrar un dispositivo o una red, haciendo que el dispositivo o la red sean inaccesibles para los usuarios previstos. Los ataques

DoS bloquean el acceso inundando el objetivo con tráfico o enviándole solicitudes que inician una ralentización del sistema o provocan un fallo del sistema. Sus dispositivos IoT se pueden utilizar en ataques de DoS.

Métricas relacionadas:

Métrica	Justificación
Paquetes salientes	Los ataques de DoS suelen implicar tasas más altas de comunicación saliente desde un dispositivo determinado y, según el tipo de ataque de DoS, podría producirse un aumento en la cantidad de paquetes salientes y bytes salientes, o en ambas.
Bytes salientes	
IP de destino	Si define los rangos de direcciones IP/CIDR con los que deben comunicarse sus dispositivos, una anomalía en la IP de destino puede indicar una comunicación IP no autorizada desde sus dispositivos.
Puertos TCP de escucha	Por lo general, un ataque DoS requiere una infraestructura de comando y control más grande en la que el malware instalado en los dispositivos reciba comandos e información sobre a quién atacar y cuándo atacar. Por lo tanto, para recibir esa información, el malware normalmente escucha en los puertos que los dispositivos no suelen utilizar.
Recuento de puertos TCP de escucha	
Puertos UDP de escucha	
Recuento de puertos UDP de escucha	

Escalado lateral de amenazas:

Un escalado lateral de amenazas suele comenzar cuando un atacante accede a un punto de la red, por ejemplo, a un dispositivo conectado. A continuación, el atacante intenta aumentar su nivel de privilegios o su acceso a otros dispositivos mediante métodos como el robo de credenciales o la explotación de vulnerabilidades.

Métricas relacionadas:

Métrica	Justificación
Paquetes salientes	En situaciones típicas, el atacante tendría que realizar un escaneo en la red de área local para realizar un reconocimiento e identific ar los dispositivos disponibles con el fin de reducir su selección de objetivos de ataque. Este tipo de análisis podría provocar un aumento en el número de bytes y paquetes descartados.
Bytes salientes	
IP de destino	Si se supone que un dispositivo debe comunicarse con un conjunto conocido de direcciones IP o CIDR, puede identificar si intenta comunicarse con una dirección IP anormal, que suele ser una dirección IP privada de la red local en un caso de aumento lateral de amenazas.
Errores de autorización	A medida que el atacante intenta aumentar su nivel de privilegios en una red de IoT, puede utilizar credenciales robadas que se han revocado o que han caducado, lo que provocaría un aumento de los errores de autorización.

Exfiltración de datos o vigilancia:

La exfiltración de datos se produce cuando un malware o un actor malicioso lleva a cabo una transferencia de datos no autorizada desde un dispositivo o un punto de conexión de la red. La exfiltración de datos normalmente tiene dos propósitos para el atacante: obtener datos o propiedad intelectual o realizar el reconocimiento de una red. La vigilancia significa que se utiliza código malicioso para monitorizar las actividades de los usuarios con el fin de robar credenciales y recopilar información. Las siguientes métricas pueden proporcionar un punto de partida para investigar cualquier tipo de ataque.

Métricas relacionadas:

Métrica	Justificación
Paquetes salientes	Cuando se producen ataques de exfiltración de datos o de vigilancia, el atacante suele duplicar los datos que se envían desde el dispositivo en lugar de simplemente redirigir los, que el defensor identificaría cuando no ve los datos previstos. Estos datos duplicados aumentarían considerablemente la cantidad total de datos enviados desde el dispositi vo, lo que se traduciría en un aumento del número de paquetes y bytes descartados.
Bytes salientes	
IP de destino	Cuando un atacante utiliza un dispositivo para realizar ataques de exfiltración o vigilanci a de datos, los datos deberán enviarse a una dirección IP anormal controlada por el atacante. La monitorización de la IP de destino puede ayudar a identificar un ataque de este tipo.

Minería de criptomonedas

Los atacantes aprovechan la potencia de procesamiento de los dispositivos para extraer criptomonedas. La minería de criptomonedas es un proceso computacionalmente intensivo que, por lo general, requiere una comunicación de red con otros pares y grupos mineros.

Métricas relacionadas:

Métrica	Justificación
IP de destino	La comunicación de red suele ser un requisito durante la minería de criptomonedas. Tener una lista estrictamente controlada de direcciones IP con las que debe comunicar se el dispositivo puede ayudar a identificar las

Métrica	Justificación
	comunicaciones no deseadas en un dispositivo, como la minería de criptomonedas.
Métrica personalizada de uso de la CPU	La minería de criptomonedas requiere una computación intensiva, lo que resulta en una alta utilización de la CPU del dispositivo. Si opta por recopilar y monitorizar esta métrica, un uso de la CPU superior al normal podría ser un indicador de las actividades de minería de criptomonedas.

Mando y control, malware y ransomware

El malware o el ransomware restringen el control sobre los dispositivos y limitan su funcionalidad. En el caso de un ataque de ransomware, se perdería el acceso a los datos debido al cifrado que utiliza el ransomware.

Métricas relacionadas:

Métrica	Justificación
IP de destino	Los ataques de red o remotos representan una gran parte de los ataques a los dispositivos IoT. Una lista estrictamente controlada de direcciones IP con las que debe comunicarse el dispositivo puede ayudar a identificar direcciones IP de destino anormales provocadas por un ataque de malware o ransomware.
Puertos TCP de escucha	Varios ataques de malware implican iniciar un servidor de mando y control que envía comandos para ejecutarlos en un dispositivo. Este tipo de servidor es fundamental para una operación de malware o ransomware, y se puede identificar monitorizando rigurosam
Recuento de puertos TCP de escucha	
Puertos UDP de escucha	
Recuento de puertos UDP de escucha	

Métrica	Justificación
	ente los puertos TCP/UDP abiertos y el número de puertos.

Conceptos

métrica

AWS IoT Device Defender Detect usa métricas para detectar comportamientos anómalos de dispositivos. AWS IoT Device Defender Detect compara el valor registrado de una métrica con el valor esperado que proporciona el usuario. Estas métricas se pueden obtener de dos fuentes: de las métricas del lado de la nube y de las métricas del lado del dispositivo: ML Detect admite 6 métricas del lado de la nube y 7 métricas del lado del dispositivo. Para obtener una lista de las métricas admitidas para ML Detect, consulte Métricas admitidas.

El comportamiento anómalo en la red de AWS IoT se detecta mediante el uso de métricas del lado de la nube, como el número de errores de autorización o el número o el tamaño de mensajes que un dispositivo envía o recibe a través de AWS IoT.

AWS IoT Device Defender Detect también puede recopilar, agregar y monitorizar datos de métricas generados por dispositivos AWS IoT (por ejemplo, los puertos en los que escucha un dispositivo, la cantidad de bytes o paquetes enviados o las conexiones TCP del dispositivo).

Puede usar AWS IoT Device Defender Detect solo con métricas del lado de la nube. Para usar las métricas del lado del dispositivo, primero debe implementar el SDK de AWS IoT en sus dispositivos conectados a AWS IoT o en las gateways de los dispositivos para recopilar las métricas y enviarlas a AWS IoT. Consulte Envío de métricas desde dispositivos.

Perfil de seguridad

Un perfil de seguridad define comportamientos anómalos para un grupo de dispositivos (un grupo de objetos estáticos) o para todos los dispositivos de su cuenta, y especifica qué acciones adoptar cuando se detecta una anomalía. Puede utilizar la consola de AWS IoT o los comandos de la API para crear un perfil de seguridad y asociarlo a un grupo de dispositivos. AWS IoT Device Defender Detect comienza a registrar datos relacionados con la seguridad y utiliza los comportamientos definidos en el perfil de seguridad para detectar anomalías en el comportamiento de los dispositivos.

comportamiento

Un comportamiento indica a AWS IoT Device Defender Detect cómo puede saber cuándo un dispositivo realiza alguna actividad anómala. Todas las acciones del dispositivo que no coinciden con un comportamiento desencadenan una alerta. Un comportamiento de Rules Detect consiste en una métrica y un valor absoluto o un umbral estadístico con un operador (por ejemplo, menor o igual que, mayor o igual a), que describe el comportamiento esperado del dispositivo. El comportamiento de ML Detect consta de una métrica y una configuración de ML Detect, que establecen un modelo de ML para conocer el comportamiento normal de los dispositivos.

modelo de ML

Un modelo de ML es un modelo de machine learning creado para monitorizar cada comportamiento que configura un cliente. El modelo se basa en los patrones de datos métricos de los grupos de dispositivos específicos y genera tres umbrales de confianza en las anomalías (alto, medio y bajo) para el comportamiento basado en métricas. Deduce anomalías en función de los datos métricos ingeridos a nivel de dispositivo. En el contexto de ML Detect, se crea un modelo de machine learning para evaluar un comportamiento basado en métricas. Para obtener más información, consulte ML Detect.

nivel de confianza

ML Detect admite tres niveles de confianza: `High`, `Medium` y `Low`. Un nivel de confianza `High` significa baja sensibilidad en la evaluación del comportamiento anómalo y, con frecuencia, un número menor de alarmas. El nivel de confianza `Medium` significa sensibilidad media y el nivel de confianza `Low` significa sensibilidad alta y, con frecuencia, un número mayor de alarmas.

dimensión

Puede definir una dimensión para ajustar el ámbito de un comportamiento. Por ejemplo, puede definir una dimensión de filtrado de temas que aplique un comportamiento a los temas de MQTT que coincidan con un patrón. Para obtener información sobre la definición de una dimensión para su uso en un perfil de seguridad, consulte CreateDimension.

alarma

Cuando se detecta una anomalía, se puede enviar una notificación de alarma mediante una métrica de CloudWatch (consulte Monitorización de alarmas y métricas de AWS IoT con Amazon CloudWatch, en la Guía para desarrolladores de AWS IoT Core) o una notificación de SNS. También se muestra una notificación de alarma en la consola de AWS IoT junto con información sobre dicha alarma y un historial de las alarmas del dispositivo. También se envía una alarma

cuando un dispositivo monitorizado deja de exhibir un comportamiento anómalo o cuando ha estado generando una alarma, pero deja de informar durante un período prolongado.

estado de verificación de la alarma

Una vez creada una alarma, puede verificar que la alarma tenga los estados Verdadero positivo, Positiva benigno, Falso positivo o Desconocido. También puede agregar una descripción al estado de verificación de la alarma. Puede ver, organizar y filtrar alarmas de AWS IoT Device Defender mediante uno de los cuatro estados de verificación. Puede usar los estados de verificación de las alarmas y las descripciones relacionadas para informar a los miembros de su equipo. Esto ayuda al equipo a tomar medidas de seguimiento, por ejemplo, tomar medidas de mitigación en el caso de las alarmas verdaderas positivas, omitir las alarmas positivas benignas o continuar investigando las alarmas desconocidas. El estado de verificación predeterminado para todas las alarmas es Desconocido.

supresión de alarmas

Administre las notificaciones de SNS de alarma de Detect configurando la notificación de comportamiento en `on` o en `suppressed`. La supresión de las alarmas no impide que Detect evalúe el comportamiento de los dispositivos; Detect sigue marcando los comportamientos anómalos como alarmas de infracción. Sin embargo, las alarmas suprimidas no se reenviarían para ser notificadas por SNS. Solo se puede acceder a ellas a través de la consola de AWS IoT o la API.

Comportamientos

Un perfil de seguridad contiene un conjunto de comportamientos. Cada comportamiento contiene una métrica que especifica el comportamiento normal de un grupo de dispositivos o de todos los dispositivos de la cuenta. Los comportamientos se dividen en dos categorías: reglas que detectan comportamientos y machine learning que detectan comportamientos. Con los comportamientos de Rules Detect, usted define cómo deben comportarse sus dispositivos, mientras que ML Detect utiliza modelos de machine learning basados en datos históricos de los dispositivos para evaluar cómo deben comportarse sus dispositivos.

Un perfil de seguridad puede ser de dos tipos de umbrales: ML o basado en reglas. Los perfiles de seguridad de ML detectan automáticamente las anomalías operativas y de seguridad a nivel de dispositivo en toda su flota al aprender de los datos anteriores. Los perfiles de seguridad basados en reglas requieren que establezca manualmente reglas estáticas para monitorizar el comportamiento de sus dispositivos.

A continuación, se describen algunos de los campos que se utilizan en la definición de un `behavior`:

Comunes a Rules Detect y ML Detect

`name`

El nombre del comportamiento.

`metric`

El nombre de la métrica utilizada (es decir, lo que mide el comportamiento).

`consecutiveDatapointsToAlarm`

Si un dispositivo infringe el comportamiento para el número especificado de puntos de datos consecutivos, se genera una alarma. Si no se especifica, el valor predeterminado es 1.

`consecutiveDatapointsToClear`

Si se genera una alarma y el dispositivo infractor deja de infringir el comportamiento para el número especificado de puntos de datos consecutivos, la alarma se desactiva. Si no se especifica, el valor predeterminado es 1.

`threshold type`

Un perfil de seguridad puede ser de dos tipos de umbrales: ML o basado en reglas. Los perfiles de seguridad de ML detectan automáticamente las anomalías operativas y de seguridad a nivel de dispositivo en toda su flota al aprender de los datos anteriores. Los perfiles de seguridad basados en reglas requieren que establezca manualmente reglas estáticas para monitorizar el comportamiento de sus dispositivos.

`alarm suppressions`

Puede administrar las notificaciones de Amazon SNS de alarma de Detect configurando la notificación de comportamiento en on o en `suppressed`. La supresión de las alarmas no impide que Detect evalúe el comportamiento de los dispositivos; Detect sigue marcando los comportamientos anómalos como alarmas de infracción. Sin embargo, las alarmas suprimidas no se reenvían a las notificaciones de Amazon SNS. Solo se puede acceder a ellas a través de la consola de AWS IoT o la API.

Rules Detect

`dimension`

Puede definir una dimensión para ajustar el ámbito de un comportamiento. Por ejemplo, puede definir una dimensión de filtrado de temas que aplique un comportamiento a los temas de MQTT que coincidan con un patrón. Si desea definir una dimensión para utilizarla en un perfil de seguridad, consulte CreateDimension. Se aplica únicamente a Rules Detect.

`criteria`

Los criterios que determinan si un dispositivo se comporta normalmente con respecto a la `metric`.

> **Note**
>
> En la consola de AWS IoT, puede elegir Recibir alertas para recibir una notificación a través de Amazon SNS cuando AWS IoT Device Defender detecte que un dispositivo se comporta de forma anómala.

`comparisonOperator`

El operador que relaciona el objeto medido (`metric`) con los criterios (`value` o `statisticalThreshold`).

Los valores posibles son: "less-than", "less-than-equals", "greater-than", "greater-than-equals", "in-cidr-set", "not-in-cidr-set", "in-port-set" y "not-in-port-set". No todos los operadores son válidos para todas las métricas. Los operadores para conjuntos y puertos CIDR solo son para usarlos con métricas que impliquen dichas entidades.

`value`

El valor que se va a comparar con la `metric`. En función del tipo de métrica, debe contener `count` (un valor), `cidrs` (una lista de CIDR) o `ports` (una lista de puertos).

`statisticalThreshold`

El umbral estadístico por el que se determina la infracción de un comportamiento. Este campo contiene un campo `statistic` que tiene los siguientes valores posibles: "p0", "p0.1", "p0.01", "p1", "p10", "p50", "p90", "p99", "p99.9", "p99.99" o "p100".

Este campo `statistic` indica un percentil. Da como resultado un valor por el que se determina la conformidad con el comportamiento. Las métricas se recopilan una o varias veces a lo largo de la duración especificada (`durationSeconds`) de todos los dispositivos de informe asociados a este perfil de seguridad y los percentiles se calculan en función de dichos datos. Posteriormente, las medidas se recopilan para un dispositivo y se acumulan a lo largo de la misma duración. Si el valor resultante del dispositivo está por encima o por debajo (`comparisonOperator`) del valor asociado con el percentil especificado, se considera que el dispositivo se ajusta al comportamiento. De lo contrario, el dispositivo infringirá dicho comportamiento.

Un percentil indica el porcentaje de todas las mediciones consideradas que caigan por debajo del valor asociado. Por ejemplo, si el valor asociado a "p90" (el percentil 90.º) es 123, el 90% de todas las mediciones fueron inferiores a 123.

`durationSeconds`

Utilícelo para especificar el periodo de tiempo durante el cual se evalúa el comportamiento, para aquellos criterios que tienen una dimensión de tiempo (por ejemplo, `NUM_MESSAGES_SENT`). Para una comparación de métricas `statisticalThreshhold`, se trata del período de tiempo durante el que se recopilan mediciones para todos los dispositivos a fin de determinar los valores `statisticalThreshold` y, a continuación, para cada dispositivo para determinar cómo se comparta en comparación.

ML Detect

`ML Detect confidence`

ML Detect admite tres niveles de confianza: `High`, `Medium` y `Low`. Un nivel de confianza `High` significa baja sensibilidad en la evaluación del comportamiento anómalo y, con frecuencia, un número menor de alarmas; el nivel de confianza `Medium` significa sensibilidad media y el nivel de confianza `Low` significa sensibilidad alta y, con frecuencia, un número mayor de alarmas.

ML Detect

Con Machine Learning Detect (ML Detect), puede crear perfiles de seguridad que utilizan el machine learning para conocer el comportamiento esperado de los dispositivos mediante la creación automática de modelos basados en los datos históricos de los dispositivos y asignar estos perfiles

a un grupo de dispositivos o a todos los dispositivos de su flota. A continuación, AWS IoT Device Defender identifica las anomalías y activa las alarmas mediante los modelos de machine learning.

Para obtener información sobre cómo empezar a usar ML Detect, consulte Guía de ML Detect.

El capítulo contiene las siguientes secciones:

- Casos de uso de ML Detect
- Cómo funciona ML Detect
- Requisitos mínimos
- Limitaciones
- Marcar los falsos positivos y otros estados de verificación en las alarmas
- Métricas admitidas
- Service Quotas
- Comandos de la CLI de ML Detect
- API ML Detect API
- Pausar o eliminar un perfil de seguridad de ML Detect

Casos de uso de ML Detect

Puede usar ML Detect para monitorizar los dispositivos de su flota cuando sea difícil establecer el comportamiento esperado de los dispositivos. Por ejemplo, para monitorizar la métrica del número de desconexiones, es posible que no quede claro qué se considera un umbral aceptable. En este caso, puede habilitar ML Detect para identificar puntos de datos de métricas de desconexión anómalos en función de los datos históricos notificados por los dispositivos.

Otro caso de uso de ML Detect es monitorizar los comportamientos de los dispositivos que cambian dinámicamente con el tiempo. ML Detect aprende periódicamente los comportamientos dinámicos esperados de los dispositivos en función de los cambios en los patrones de datos de los dispositivos. Por ejemplo, el volumen de mensajes enviados por el dispositivo puede variar entre los días de la semana y los fines de semana, y ML Detect aprenderá este comportamiento dinámico.

Cómo funciona ML Detect

Con ML Detect, puede crear comportamientos para identificar anomalías operativas y de seguridad en 6 métricas del lado de la nube y 7 métricas del lado del dispositivo. Tras el período de formación

inicial del modelo, ML Detect actualiza los modelos a diario en función de los últimos 14 días de datos. Supervisa los puntos de datos de estas métricas con los modelos de machine learning y activa una alarma si se detecta una anomalía.

ML Detect funciona mejor si se asocia un perfil de seguridad a un conjunto de dispositivos con comportamientos esperados similares. Por ejemplo, si algunos de sus dispositivos se utilizan en los hogares de los clientes y otros en las oficinas comerciales, los patrones de comportamiento de los dispositivos pueden diferir considerablemente entre los dos grupos. Puede organizar los dispositivos en un grupo de dispositivos domésticos y un grupo de dispositivos de oficina. Para lograr la máxima eficacia en la detección de anomalías, asocie cada grupo de elementos a un perfil de seguridad de ML Detect independiente.

Mientras ML Detect está creando el modelo inicial, se necesitan 14 días y un mínimo de 25 000 puntos de datos por métrica durante los últimos 14 días para generar un modelo. Después, actualiza el modelo todos los días, siempre que haya un número mínimo de puntos de datos métricos. Si no se cumple el requisito mínimo, ML Detect intenta crear el modelo al día siguiente y lo volverá a intentar todos los días durante los siguientes 30 días antes de interrumpir el modelo para su evaluación.

Requisitos mínimos

Para entrenar y crear el modelo de machine learning inicial, ML Detect tiene los siguientes requisitos mínimos.

Periodo mínimo de formación

Los modelos iniciales tardan 14 días en construirse. Después, el modelo se actualiza todos los días con datos métricos de un período final de 14 días.

Puntos de datos totales mínimos

El número mínimo de puntos de datos necesario para crear un modelo de machine learning es de 25 000 puntos de datos por métrica durante los últimos 14 días. Para una formación continua y una actualización del modelo, ML Detect requiere que los dispositivos monitorizados cumplan con los puntos de datos mínimos. Es aproximadamente el equivalente a las siguientes configuraciones:

- 60 dispositivos que se conectan y tienen actividad en AWS IoT a intervalos de 45 minutos.
- 40 dispositivos a intervalos de 30 minutos.
- 15 dispositivos a intervalos de 10 minutos.
- 7 dispositivos a intervalos de 5 minutos.

Destinos de grupos de dispositivos

Para recopilar datos, debe incluir objetos en los grupos de objetos de destino del perfil de seguridad.

Una vez creado el modelo inicial, los modelos de machine learning se actualizan todos los días y requieren al menos 25 000 puntos de datos durante un período final de 14 días.

Limitaciones

Puede usar ML Detect con dimensiones en las siguientes métricas del lado de la nube:

- Fallos de autorización (aws:num-authorization-failures)
- Mensajes recibidos (aws:num-messages-received)
- Mensajes enviados (aws:num-messages-sent)
- Tamaño del mensaje (aws:message-byte-size)

ML Detect no admite las siguientes métricas.

ML Detect no admite métricas del lado de la nube:

- IP de origen (aws:source-ip-address)

ML Detect no admite métricas del lado del dispositivo:

- IP de destino (`aws:destination-ip-addresses`)
- Puertos TCP de escucha (`aws:listening-tcp-ports`)
- Puertos UDP de escucha (`aws:listening-udp-ports`)

Las métricas personalizadas solo admiten el tipo number.

Marcar los falsos positivos y otros estados de verificación en las alarmas

Si durante la investigación comprueba que una alarma de ML Detect es un falso positivo, puede configurar el estado de verificación de la alarma en falso positivo. Esto puede ayudarlo a usted y a su equipo a identificar las alarmas a las que no tengan que responder. También puede marcar las alarmas como Verdadero positivo, Benigno positivo o Desconocido.

Puede marcar las alarmas con la consola de AWS IoT Device Defender o mediante la acción de la API PutVerificationStateOnViolation.

Métricas admitidas

Puede utilizar las siguientes métricas del lado de la nube con ML Detect:

- Fallos de autorización (aws:num-authorization-failures)
- Intentos de conexión (aws:num-connection-attempts)
- Desconexiones (aws:num-disconnects)
- Tamaño del mensaje (aws:message-byte-size)
- Mensajes enviados (aws:num-messages-sent)
- Mensajes recibidos (aws:num-messages-received)

Puede utilizar las siguientes métricas del lado del dispositivo con ML Detect:

- Bytes salientes (`aws:all-bytes-out`)
- Bytes entrantes (`aws:all-bytes-in`)
- Recuento de puertos TCP de escucha (`aws:num-listening-tcp-ports`)
- Recuento de puertos UDP de escucha (`aws:num-listening-udp-ports`)
- Paquetes salientes (`aws:all-packets-out`)
- Paquetes entrantes (`aws:all-packets-in`)
- Recuento de conexiones TCP establecidas (`aws:num-established-tcp-connections`)

Service Quotas

Para obtener información sobre las cuotas y límites del servicio ML Detect, consulte Puntos de enlace y cuotas de AWS IoT Device Defender.

Comandos de la CLI de ML Detect

Puede utilizar los siguientes comandos de la CLI para crear y administrar 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 ML Detect API

Las siguientes API pueden utilizarse para crear y administrar la exportación de perfiles de seguridad de ML Detect.

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

Pausar o eliminar un perfil de seguridad de ML Detect

Puede pausar su perfil de seguridad de ML Detect para dejar de monitorizar temporalmente el comportamiento de los dispositivos o eliminar su perfil de seguridad de ML Detect para dejar de monitorizar el comportamiento de los dispositivos durante un período prolongado.

Pausar el perfil de seguridad de ML Detect mediante la consola

Para pausar un perfil de seguridad de ML Detect mediante la consola, primero debe tener un grupo de objetos vacío. Para crear un grupo de objetos vacío, consulte Static thing groups en la

Guía para desarrolladores de AWS IoT Core. Si ha creado un grupo de objetos vacío, configúrelo como el destino del perfil de seguridad de ML Detect.

> **Note**
>
> Debe volver a establecer el destino de su perfil de seguridad en un grupo de dispositivos con dispositivos en un plazo de 30 días o no podrá reactivar el perfil de seguridad.

Eliminar el perfil de seguridad de ML Detect mediante la consola

Si desea eliminar un perfil de seguridad, siga estos pasos:

1. En la consola de AWS IoT, vaya a la barra lateral y seleccione la sección Defender.
2. En Defender, elija Detectar y, a continuación, Perfiles de seguridad.
3. Elija el perfil de seguridad de ML Detect que quiera eliminar.
4. Elija Acciones y, a continuación, en las opciones, elija Eliminar.

> **Note**
>
> Después de eliminar un perfil de seguridad de ML Detect, no podrá reactivarlo.

Pausar un el perfil de seguridad de ML Detect mediante la CLI

Para pausar un perfil de seguridad de ML Detect mediante la CLI, utilice el 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**
>
> Esta opción solo está disponible en AWS CLI. Del mismo modo que hizo en el flujo de trabajo de la consola, debe volver a establecer el destino de su perfil de seguridad en un grupo de dispositivos con dispositivos en un plazo de 30 días o no podrá reactivar el perfil

de seguridad. Para asociar un perfil de seguridad a un grupo de dispositivos, utilice el comando `attach-security-profile`.

Eliminar un perfil de seguridad de ML Detect mediante la CLI

Puede eliminar un perfil de seguridad mediante el siguiente comando `delete-security-profile`:

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

> **Note**
>
> Después de eliminar un perfil de seguridad de ML Detect, no podrá reactivarlo.

Métricas personalizadas

Con las métricas personalizadas de AWS IoT Device Defender, puede definir y monitorizar métricas que sean exclusivas de su flota o caso de uso, como la cantidad de dispositivos conectados a las puertas de enlace wifi, los niveles de carga de las baterías o la cantidad de ciclos de alimentación de los enchufes inteligentes. Los comportamientos de las métricas personalizadas se definen en los perfiles de seguridad, que especifican los comportamientos esperados para un grupo de dispositivos (un grupo de objetos) o para todos los dispositivos. Puede monitorizar los comportamientos configurando alarmas, que puede utilizar para detectar y responder a problemas específicos de los dispositivos.

El capítulo contiene las siguientes secciones:

- Cómo usar las métricas personalizadas en la consola
- Cómo usar métricas personalizadas desde la CLI
- Comandos de la CLI para métricas personalizadas
- API de métricas personalizadas

Cómo usar las métricas personalizadas en la consola

Tutoriales

- AWS IoT Device Defender Agent SDK (Python)
- Crear una métrica personalizada y agregarla a un perfil de seguridad
- Ver los detalles de las métricas personalizadas
- Actualizar de una métrica personalizada
- Eliminar una métrica personalizada

AWS IoT Device Defender Agent SDK (Python)

Para empezar, descargue el agente de ejemplo AWS IoT Device Defender Agent SDK (Python). El agente recopila las métricas y publica los informes. Una vez que se publiquen las métricas del dispositivo, podrá ver las métricas que se están recopilando y determinar los umbrales para configurar las alarmas. Las instrucciones para configurar el agente del dispositivo están disponibles en el archivo Readme de AWS IoT Device Defender Agent SDK (Python). Para obtener más información, consulte AWS IoT Device Defender Agent SDK (Python).

Crear una métrica personalizada y agregarla a un perfil de seguridad

El siguiente procedimiento le muestra cómo crear una métrica personalizada en la consola.

1. En la consola deAWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Detect, Métricas.
2. En la página Métricas personalizadas, elija Crear.
3. En la página Crear métrica personalizada, haga lo siguiente:
    1. En Nombre, escriba un nombre para la métrica personalizada. Este nombre no se puede modificar después de haber creado la métrica personalizada.
    2. En Nombre para mostrar (opcional), puede introducir un nombre descriptivo para la métrica personalizada. No tiene por qué ser único y se puede modificar después de la creación.
    3. En Tipo, elija el tipo de métrica que quiera monitorizar. Los tipos de métrica incluyen string-list, ip-address-list, number-list y number. No se puede modificar el tipo después de la creación.

    > **Note**
    >
    > ML Detect solo permite el tipo number.

4. En Etiquetas, puede seleccionar las etiquetas que quiera asociar al recurso.

   Cuando haya terminado, seleccione Confirmar.
4. Una vez creada la métrica personalizada, aparecerá la página Métricas personalizadas, donde podrá ver la métrica personalizada recién creada.
5. A continuación, debe agregar su métrica personalizada a un perfil de seguridad. En la consola de AWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Detect, Perfiles de seguridad.
6. Elija el perfil de seguridad al que quiera agregar su métrica personalizada.
7. Seleccione Acciones, Editar.
8. Seleccione Métricas adicionales que retener y, a continuación, elija su métrica personalizada. Seleccione Siguiente en las siguientes pantallas hasta llegar a la página de confirmación. Elija Guardar y Continuar. Una vez que la métrica personalizada se haya agregado correctamente, aparecerá la página de detalles del perfil de seguridad.

   > **Note**
   >
   > Las estadísticas de percentiles no están disponibles para las métricas cuando alguno de los valores de métricas es un número negativo.

Ver los detalles de las métricas personalizadas

El siguiente procedimiento le muestra cómo ver los detalles de una métrica personalizada en la consola.

1. En la consola deAWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Detect, Métricas.
2. Elija el nombre de la métrica personalizada de la que desea ver los detalles.

Actualizar de una métrica personalizada

El siguiente procedimiento le muestra cómo actualizar una métrica personalizada en la consola.

1. En la consola deAWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Detect, Métricas.

2. Seleccione el botón de opción situado junto a la métrica personalizada que quiera actualizar. En Acciones, seleccione Editar.
3. En la página Actualizar métrica personalizada, puede editar el nombre para mostrar y eliminar o agregar etiquetas.
4. Cuando haya terminado, elija Actualizar. La página Métricas personalizadas.

Eliminar una métrica personalizada

El siguiente procedimiento le muestra cómo eliminar una métrica personalizada en la consola.

1. En primer lugar, elimine la métrica personalizada de cualquier perfil de seguridad en el que se haga referencia. Puede ver qué perfiles de seguridad contienen su métrica personalizada en la página de detalles de la métrica personalizada. En la consola deAWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Detect, Métricas.
2. Elija la métrica personalizada que quiera eliminar. Elimine la métrica personalizada de cualquier perfil de seguridad que aparezca en la sección Perfiles de seguridad de la página de detalles de la métrica personalizada.
3. En la consola deAWS IoT, en el panel de navegación, amplíe Defend y, a continuación, seleccione Detect, Métricas.
4. Seleccione el botón de opción situado junto a la métrica personalizada que quiera eliminar. En Acciones, seleccione Eliminar.
5. En el mensaje ¿Seguro que quiere eliminar la métrica personalizada?, seleccione Eliminar métrica personalizada.

> **Warning**
>
> Después de eliminar una métrica personalizada, se pierden todos los datos asociados a la métrica. Esta acción no se puede deshacer.

Cómo usar métricas personalizadas desde la CLI

Tutoriales

- AWS IoT Device Defender Agent SDK (Python)
- Crear una métrica personalizada y agregarla a un perfil de seguridad

- Ver los detalles de las métricas personalizadas
- Actualizar de una métrica personalizada
- Eliminar una métrica personalizada

AWS IoT Device Defender Agent SDK (Python)

Para empezar, descargue el agente de ejemplo AWS IoT Device Defender Agent SDK (Python). El agente recopila las métricas y publica los informes. Una vez publicadas las métricas del dispositivo, podrá ver las métricas que se están recopilando y determinar los umbrales para configurar las alarmas. Las instrucciones para configurar el agente del dispositivo están disponibles en el archivo Readme de AWS IoT Device Defender Agent SDK (Python). Para obtener más información, consulte AWS IoT Device Defender Agent SDK (Python).

Crear una métrica personalizada y agregarla a un perfil de seguridad

El siguiente procedimiento muestra cómo crear una métrica personalizada y agregarla a un perfil de seguridad desde la CLI.

1. Utilice el comando de `create-custom-metric` para crear su métrica personalizada. En el siguiente ejemplo se crea una métrica personalizada que mide el porcentaje de batería.

   ```
   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" \
   ```

   Salida:

   ```
   {
       "metricName": "batteryPercentage",
       "metricArn": "arn:aws:iot:us-
   east-1:1234564789012:custommetric/batteryPercentage"
   }
   ```

2. Una vez creada la métrica personalizada, puede agregarla a un perfil existente utilizando `update-security-profile` o crear un nuevo perfil de seguridad para agregar la métrica personalizada utilizando `create-security-profile`. Aquí, creamos un nuevo perfil de

seguridad llamado *batteryUsage* al que agregar nuestra nueva métrica personalizada *batteryPercentage*. También agregamos una métrica de Rules Detect llamada *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
```

Salida:

```
{
    "securityProfileArn": "arn:aws:iot:us-east-1:1234564789012:securityprofile/
batteryUsage",
    "securityProfileName": "batteryUsage"
}
```

> **Note**
>
> Las estadísticas de percentiles no están disponibles para las métricas cuando alguno de los valores de métricas es un número negativo.

Ver los detalles de las métricas personalizadas

El siguiente procedimiento le muestra cómo ver los detalles de una métrica personalizada desde la CLI.

- Utilice el comando de `list-custom-metrics` para ver todas las métricas personalizadas.

```
aws iot list-custom-metrics \
    --region us-east-1
```

El resultado de este comando tendrá un aspecto similar al siguiente.

```
{
    "metricNames": [
        "batteryPercentage"
    ]
}
```

Actualizar de una métrica personalizada

El siguiente procedimiento le muestra cómo actualizar una métrica personalizada desde la CLI.

- Utilice el comando de `update-custom-metric` para actualizar una métrica personalizada. El siguiente ejemplo actualiza la `display-name`.

```
aws iot update-custom-metric \
    --metric-name batteryPercentage \
    --display-name 'remaining battery percentage on device' \
    --region us-east-1
```

El resultado de este comando tendrá un aspecto similar al siguiente.

```
{
    "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"
}
```

Eliminar una métrica personalizada

El siguiente procedimiento le muestra cómo eliminar una métrica personalizada desde la CLI.

1. Para eliminar una métrica personalizada, elimínela primero de los perfiles de seguridad a los que esté asociada. Utilice el comando `list-security-profiles` para ver los perfiles de seguridad con una determinada métrica personalizada.
2. Para eliminar una métrica personalizada de un perfil de seguridad, utilice el comando `update-security-profiles`. Introduzca toda la información que desee conservar, pero excluya la métrica personalizada.

```
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}}]"
```

El resultado de este comando tendrá un aspecto similar al siguiente.

```
{
  "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. Una vez desasociada la métrica personalizada, utilice el comando `delete-custom-metric` para eliminarla.

```
aws iot delete-custom-metric  \
  --metric-name batteryPercentage \
  --region us-east-1
```

El resultado de este comando tendrá un aspecto similar al siguiente.

```
HTTP 200
```

Comandos de la CLI para métricas personalizadas

Puede utilizar los siguientes comandos de la CLI para crear y administrar métricas personalizadas.

- create-custom-metric
- describe-custom-metric
- list-custom-metrics
- update-custom-metric
- delete-custom-metric
- list-security-profiles

API de métricas personalizadas

Las siguientes API pueden utilizarse para crear y administrar métricas personalizadas.

- CreateCustomMetric
- DescribeCustomMetric
- ListCustomMetrics
- UpdateCustomMetric
- DeleteCustomMetric
- ListSecurityProfiles

Métricas del lado del dispositivo

Al crear un perfil de seguridad, puede especificar el comportamiento esperado de su dispositivo IoT configurando comportamientos y umbrales para las métricas generadas por los dispositivos IoT. Las siguientes son métricas del dispositivo, que son métricas de los agentes que se instalan en los dispositivos.

Bytes salientes (**`aws:all-bytes-out`**)

El número de bytes salientes de un dispositivo durante un período de tiempo determinado.

Utilice esta métrica para especificar la cantidad máxima o mínima de tráfico saliente que un dispositivo debe enviar, medido en bytes, en un período de tiempo determinado.

Compatible con: Rules Detect | ML Detect

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Unidades: bytes

Duración: un entero no negativo. Los valores válidos son 300, 600, 900, 1800 o 3600 segundos.

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 Ejemplo en el que se utiliza **`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 Ejemplo de uso de ML Detect

```
{
  "name": "Outbound traffic ML behavior",
  "metric": "aws:all-bytes-out",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Bytes entrantes (`aws:all-bytes-in`)

El número de bytes entrantes en un dispositivo durante un período de tiempo determinado.

Utilice esta métrica para especificar la cantidad máxima o mínima de tráfico entrante que un dispositivo debe recibir, medido en bytes, en un período de tiempo determinado.

Compatible con: Rules Detect | ML Detect

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Unidades: bytes

Duración: un entero no negativo. Los valores válidos son 300, 600, 900, 1800 o 3600 segundos.

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 Ejemplo en el que se utiliza **`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 Ejemplo de uso de ML Detect

```
{
  "name": "Inbound traffic ML behavior",
  "metric": "aws:all-bytes-in",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Recuento de puertos TCP de escucha (**`aws:num-listening-tcp-ports`**)

El número de puertos TCP en los que escucha el dispositivo.

Utilice esta métrica para especificar el número máximo de puertos TCP que cada dispositivo debe monitorizar.

Compatible con: Rules Detect | ML Detect

Unidad: errores

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Unidades: errores

Duración: un entero no negativo. Los valores válidos son 300, 600, 900, 1800 o 3600 segundos.

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 Ejemplo en el que se utiliza **`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 Ejemplo de uso de ML Detect

```
{
  "name": "Max TCP Port ML behavior",
  "metric": "aws:num-listening-tcp-ports",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Recuento de puertos UDP de escucha (**`aws:num-listening-udp-ports`**)

El número de puertos UDP en los que escucha el dispositivo.

Utilice esta métrica para especificar el número máximo de puertos UDP que cada dispositivo debe monitorizar.

Compatible con: Rules Detect | ML Detect

Unidad: errores

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Unidades: errores

Duración: un entero no negativo. Los valores válidos son 300, 600, 900, 1800 o 3600 segundos.

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 Ejemplo en el que se utiliza **`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 Ejemplo de uso de ML Detect

```
{
  "name": "Max UPD Port ML behavior",
  "metric": "aws:num-listening-tcp-ports",
  "criteria": {
  "consecutiveDatapointsToAlarm": 1,
  "consecutiveDatapointsToClear": 1,
  "mlDetectionConfig": {
    "confidenceLevel": "HIGH"
   }
 },
```

```
  "suppressAlerts": true
}
```

Paquetes salientes (**`aws:all-packets-out`**)

El número de paquetes salientes de un dispositivo durante un período de tiempo determinado.

Utilice esta métrica para especificar la cantidad máxima o mínima de tráfico saliente total que un dispositivo debe enviar en un período de tiempo determinado.

Compatible con: Rules Detect | ML Detect

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Unidades: paquetes

Duración: un entero no negativo. Los valores válidos son 300, 600, 900, 1800 o 3600 segundos.

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 Ejemplo en el que se utiliza **`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 Ejemplo de uso de ML Detect

```
{
  "name": "Outbound sent ML behavior",
  "metric": "aws:all-packets-out",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Paquetes entrantes (`aws:all-packets-in`)

El número de paquetes entrantes en un dispositivo durante un período de tiempo determinado.

Utilice esta métrica para especificar la cantidad máxima o mínima de tráfico entrante total que un dispositivo debe recibir en un período de tiempo determinado.

Compatible con: Rules Detect | ML Detect

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Unidades: paquetes

Duración: un entero no negativo. Los valores válidos son 300, 600, 900, 1800 o 3600 segundos.

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

Ejemplo en el que se utiliza `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 Ejemplo de uso de ML Detect

```
{
  "name": "Inbound sent ML behavior",
  "metric": "aws:all-packets-in",
  "criteria": {
```

```
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

IP de destino (`aws:destination-ip-addresses`)

Un conjunto de destinos de IP.

Utilice esta métrica para especificar un conjunto de enrutamientos entre dominios sin clases (CIDR) permitidos (previamente denominado lista blanca) y denegados (previamente denominado lista negra) desde los que cada dispositivo debe o no conectarse a AWS IoT.

Compatible con: Rules Detect

Operadores: in-cidr-set | not-in-cidr-set

Valores: una lista de CIDR

Unidades: n/a

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
}
```

Puertos TCP de escucha (`aws:listening-tcp-ports`)

Los puertos TCP en los que escucha el dispositivo.

Utilice esta métrica para especificar un conjunto de puertos TCP permitidos (previamente denominado lista blanca) y denegados (previamente denominado lista negra) en los que cada dispositivo debe o no escuchar.

Compatible con: Rules Detect

Operadores: in-port-set | not-in-port-set

Valores: una lista de puertos

Unidades: n/a

Example

```
{
  "name": "Listening TCP Ports",
  "metric": "aws:listening-tcp-ports",
  "criteria": {
    "comparisonOperator": "in-port-set",
    "value": {
      "ports": [ 443, 80 ]
    }
  },
  "suppressAlerts": true
}
```

Puertos UDP de escucha (`aws:listening-udp-ports`)

Los puertos UDP en los que escucha el dispositivo.

Utilice esta métrica para especificar un conjunto de puertos UDP permitidos (previamente denominado lista blanca) y denegados (previamente denominado lista negra) en los que cada dispositivo debe o no escuchar.

Compatible con: Rules Detect

Operadores: in-port-set | not-in-port-set

Valores: una lista de puertos

Unidades: n/a

Example

```
{
  "name": "Listening UDP Ports",
  "metric": "aws:listening-udp-ports",
  "criteria": {
    "comparisonOperator": "in-port-set",
    "value": {
      "ports": [ 1025, 2000 ]
    }
  }
}
```

Recuento de conexiones TCP establecidas (`aws:num-established-tcp-connections`)

El número de conexiones TCP para un dispositivo.

Utilice esta métrica para especificar el número máximo o mínimo de conexiones TCP activas que cada dispositivo debe tener (todos los estados de TCP).

Compatible con: Rules Detect | ML Detect

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Unidades: conexiones

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 Ejemplo en el que se utiliza **`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 Ejemplo de uso de ML Detect

```
{
  "name": "Connection count ML behavior",
  "metric": "aws:num-established-tcp-connections",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Especificación de documentos de métricas de dispositivos

Estructura general

Nombre largo	Nombre corto	Obligatoria	Tipo	Restricciones	Notas
header	hed	Y	Objeto		Bloque completo

Nombre largo	Nombre corto	Obligatoria	Tipo	Restricciones	Notas
					obligatorio para componer un informe correcto.
métricas	met	Y	Objeto		Un informe puede tener ambos o al menos un parámetro `metrics` o un bloque `custom_metrics` .
custom_metrics	cmet	Y	Objeto		Un informe puede tener ambos o al menos un parámetro `metrics` o un bloque `custom_metrics` .

Bloque de encabezado

Nombre largo	Nombre corto	Obligatoria	Tipo	Restricciones	Notas
report_id	rid	Y	Entero		Valor monotónico en aumento. Se recomienda una marca

Nombre largo	Nombre corto	Obligatoria	Tipo	Restricciones	Notas
					temporal Epoch.
versión	v	Y	Cadena	Major.Minor	Incrementos de versiones secundarias con suma de campo. Incrementos de versiones principales si se eliminan las métricas.

Bloque de métricas:

Conexiones de TCP

Nombre largo	Nombre corto	Elemento principal	Obligatoria	Tipo	Restricciones	Notas
tcp_connections	tc	métricas	N	Objeto		
established_connections	ec	tcp_connections	N	Objeto		Estado de TCP establecido
connections	cs	established_connections	N	Lista<Objeto>		
remote_addr	rad	connections	Y	Número	ip:port	La IP puede ser IPv6 o IPv4

Nombre largo	Nombre corto	Elemento principal	Obligatoria	Tipo	Restricciones	Notas
local_port	lp	connections	N	Número	>= 0	
local_interface	li	connections	N	Cadena		Nombre de la interfaz
total	t	established_connections	N	Número	>= 0	Número de conexiones establecidas

Puertos TCP de escucha

Nombre largo	Nombre corto	Elemento principal	Obligatoria	Tipo	Restricciones	Notas
listening_tcp_ports	tp	métricas	N	Objeto		
ports	pts	listening_tcp_ports	N	Lista<Objeto>	> 0	
port	pt	ports	N	Número	> 0	Los puertos deben ser números mayores que 0
interface	if	ports	N	Cadena		Nombre de la interfaz
total	t	listening_tcp_ports	N	Número	>= 0	

Puertos UDP de escucha

Nombre largo	Nombre corto	Elemento principal	Obligatoria	Tipo	Restricciones	Notas
listening_udp_ports	up	métricas	N	Objeto		
ports	pts	listening_udp_ports	N	Lista<Puerto>	> 0	
port	pt	ports	N	Número	> 0	Los puertos deben ser números mayores que 0
interface	if	ports	N	Cadena		Nombre de la interfaz
total	t	listening_udp_ports	N	Número	>= 0	

Estadísticas de la red

Nombre largo	Nombre corto	Elemento principal	Obligatoria	Tipo	Restricciones	Notas
network_stats	ns	métricas	N	Objeto		
bytes_in	bi	network_stats	N	Número	Delta Metric, >= 0	
bytes_out	bo	network_stats	N	Número	Delta Metric, >= 0	

Nombre largo	Nombre corto	Elemento principal	Obligatoria	Tipo	Restricciones	Notas
packets_in	pi	network_stats	N	Número	Delta Metric, >= 0	
packets_out	po	network_stats	N	Número	Delta Metric, >= 0	

Example

La siguiente estructura JSON utiliza nombres largos.

```
{
  "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 Ejemplo de una estructura JSON con nombres cortos

```
{
  "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"
        ]
      }
    ]
  }
}
```

Envío de métricas desde dispositivos

AWS IoT Device Defender Detect puede recopilar, agregar y monitorizar los datos de métricas generados por los dispositivos de AWS IoT para identificar aquellos dispositivos que muestran un comportamiento anómalo. En esta sección, se explica cómo enviar métricas desde un dispositivo a AWS IoT Device Defender.

Debe implementar de forma segura la versión 2 del SDK de AWS IoT en sus dispositivos conectados o puertas de enlace de dispositivo de AWS IoT para recopilar métricas del lado del dispositivo. Consulte la lista completa de SDK aquí.

Puede usar AWS IoT Device Client para publicar métricas, ya que proporciona un agente único que cubre las funciones presentes tanto en AWS IoT Device Defender como en Device Management AWS IoT. Estas funciones incluyen trabajos, tunelización segura, publicación de métricas de AWS IoT Device Defender y mucho más.

Las métricas del dispositivo se publican en el tema reservado para recopilarlas y AWS IoT evaluarlasAWS IoT Device Defender.

Uso de AWS IoT Device Client para publicar métricas

Para instalar AWS IoT Device Client, puede descargarlo de Github. Una vez que haya instalado AWS IoT Device Client en el dispositivo para el que quiera recopilar datos del lado del dispositivo, debe configurarlo para que envíe las métricas del lado del dispositivo a AWS IoT Device Defender. Compruebe que el archivo de configuración de AWS IoT Device Client tenga los siguientes parámetros establecidos en la sección `device-defender`.

```
"device-defender":    {
      "enabled":    true,
      "interval-in-seconds": 300
  }
```

> **Warning**
>
> Debe establecer el intervalo de tiempo en un mínimo de 300 segundos. Si establece el intervalo de tiempo en un valor inferior a 300 segundos, es posible que los datos de su métrica estén restringidos.

Tras actualizar la configuración, puede crear perfiles y comportamientos de seguridad en la consola de AWS IoT Device Defender para monitorizar las métricas que sus dispositivos publican en la nube. Para buscar las métricas publicadas en la consola de AWS IoT Core, seleccione Defender, Detectar y, a continuación, Métricas.

Métricas del lado de la nube

Al crear un perfil de seguridad, puede especificar el comportamiento esperado de su dispositivo IoT configurando comportamientos y umbrales para las métricas generadas por los dispositivos IoT. Las siguientes son métricas del lado de la nube, que son métricas de AWS IoT.

Tamaño del mensaje (aws:message-byte-size)

El número de bytes de un mensaje. Utilice esta métrica para especificar el tamaño máximo o mínimo (en bytes) de cada mensaje transmitido desde un dispositivo a AWS IoT.

Compatible con: Rules Detect | ML Detect

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Unidades: bytes

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 Ejemplo en el que se utiliza **`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 Ejemplo de uso de ML Detect

```
{
  "name": "Message size ML behavior",
  "metric": "aws:message-byte-size",
  "criteria": {
  "consecutiveDatapointsToAlarm": 1,
  "consecutiveDatapointsToClear": 1,
  "mlDetectionConfig": {
    "confidenceLevel": "HIGH"
   }
 },
  "suppressAlerts": true
}
```

Se genera una alarma para un dispositivo si, durante tres períodos consecutivos de cinco minutos, transmite mensajes cuyo tamaño acumulado es mayor que el medido para el 90 por ciento de todos los demás dispositivos que informan sobre este comportamiento de perfil de seguridad.

Mensajes enviados (aws:num-messages-sent)

El número de mensajes enviados por un dispositivo durante un período de tiempo determinado.

Utilice esta métrica para especificar el número máximo o mínimo de mensajes que pueden enviarse entre AWS IoT y cada dispositivo en un período de tiempo determinado.

Compatible con: Rules Detect | ML Detect

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Unidades: mensajes

Duración: un entero no negativo. Los valores válidos son 300, 600, 900, 1800 o 3600 segundos.

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 Ejemplo en el que se utiliza **`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 Ejemplo de uso de ML Detect

```
{
  "name": "Messages sent ML behavior",
  "metric": "aws:num-messages-sent",
```

```
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Mensajes recibidos (aws:num-messages-received)

El número de mensajes recibidos por un dispositivo durante un período de tiempo determinado.

Utilice esta métrica para especificar el número máximo o mínimo de mensajes que pueden recibirse entre AWS IoT y cada dispositivo en un período de tiempo determinado.

Compatible con: Rules Detect | ML Detect

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Unidades: mensajes

Duración: un entero no negativo. Los valores válidos son 300, 600, 900, 1800 o 3600 segundos.

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 Ejemplo en el que se utiliza **`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 Ejemplo de uso de ML Detect

```
{
  "name": "Messages received ML behavior",
  "metric": "aws:num-messages-received",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

Fallos de autorización (aws:num-authorization-failures)

Utilice esta métrica para especificar la cantidad máxima de errores de autorización permitidos para cada dispositivo en un período de tiempo determinado. Se produce un error de autorización cuando se deniega una solicitud desde un dispositivo a AWS IoT (por ejemplo, si un dispositivo intenta publicar en un tema para el que no tiene suficientes permisos).

Compatible con: Rules Detect | ML Detect

Unidad: errores

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Duración: un entero no negativo. Los valores válidos son 300, 600, 900, 1800 o 3600 segundos.

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 Ejemplo en el que se utiliza **`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 Ejemplo de uso de ML Detect

```
{
```

```
  "name": "Authorization failures ML behavior",
  "metric": "aws:num-authorization-failures",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": true
}
```

IP de origen (aws:source-ip-address)

La dirección IP desde la que se ha conectado un dispositivo a AWS IoT.

Utilice esta métrica para especificar un conjunto de enrutamientos entre dominios sin clases (CIDR) permitidos (previamente denominado lista blanca) y denegados (previamente denominado lista negra) desde los que cada dispositivo debe o no conectarse a AWS IoT.

Compatible con: Rules Detect

Operadores: in-cidr-set | not-in-cidr-set

Valores: una lista de CIDR

Unidades: n/a

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
}
```

Intentos de conexión (aws:num-connection-attempts)

Número de veces que un dispositivo intenta realizar una conexión durante un periodo determinado.

Utilice esta métrica para especificar el número máximo o mínimo de intentos de conexión para cada dispositivo. Se cuentan los intentos correctos y los no correctos.

Compatible con: Rules Detect | ML Detect

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Unidades: intentos de conexión

Duración: un entero no negativo. Los valores válidos son 300, 600, 900, 1800 o 3600 segundos.

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 Ejemplo en el que se utiliza **`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 Ejemplo de uso de ML Detect

```
{
  "name": "Connection attempts ML behavior",
  "metric": "aws:num-connection-attempts",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
  "suppressAlerts": false
}
```

Desconexiones (aws:num-disconnects)

Número de veces que un dispositivo se desconecta de AWS IoT durante un periodo de tiempo determinado.

Utilice esta métrica para especificar el número máximo o mínimo de veces que un dispositivo se ha desconectado de AWS IoT durante un periodo de tiempo determinado.

Compatible con: Rules Detect | ML Detect

Operadores: less-than | less-than-equals | greater-than | greater-than-equals

Valor: un entero no negativo

Unidades: desconexiones

Duración: un entero no negativo. Los valores válidos son 300, 600, 900, 1800 o 3600 segundos.

Example

```
{
```

```
  "name": "Disconnections",
  "metric": "aws:num-disconnects",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "value": {
      "count": 5
    },
    "durationSeconds": 600,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Ejemplo en el que se utiliza **`statisticalThreshold`**:

```
{
  "name": "Disconnections",
  "metric": "aws:num-disconnects",
  "criteria": {
    "comparisonOperator": "less-than-equals",
    "statisticalThreshold": {
      "statistic": "p10"
    },
    "durationSeconds": 300,
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1
  },
  "suppressAlerts": true
}
```

Example Ejemplo de uso de ML Detect

```
{
  "name": "Disconnects ML behavior",
  "metric": "aws:num-disconnects",
  "criteria": {
    "consecutiveDatapointsToAlarm": 1,
    "consecutiveDatapointsToClear": 1,
    "mlDetectionConfig": {
      "confidenceLevel": "HIGH"
    }
  },
```

```
  "suppressAlerts": true
}
```

Duración de la desconexión (aws:disconnect-duration)

El tiempo durante el que un dispositivo permanece desconectado de AWS IoT.

Usa esta métrica para especificar el tiempo máximo durante el que un dispositivo permanece desconectado de AWS IoT.

Compatible con: Rules Detect

Operadores: menores que | menores que iguales

Valor: un entero no negativo (en minutos)

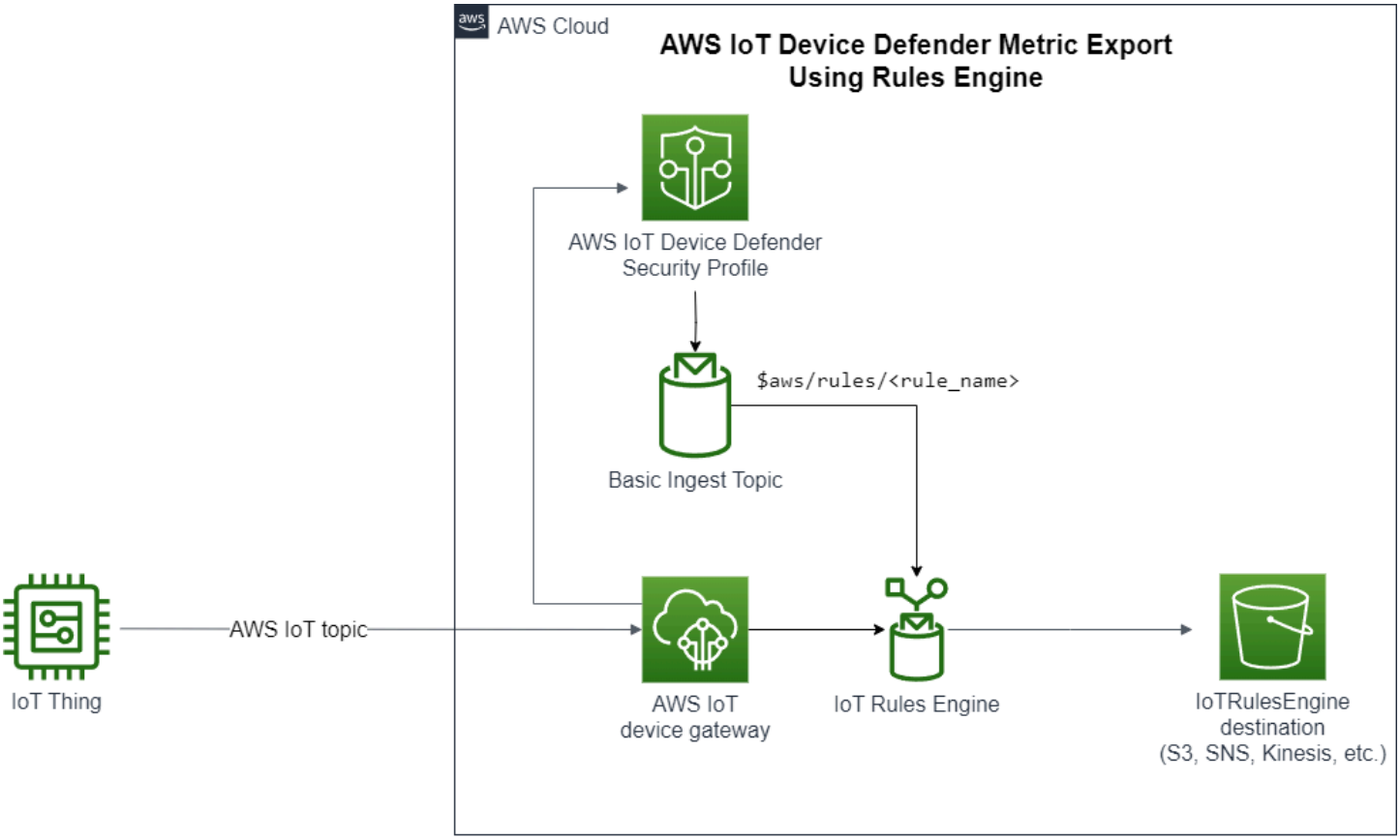
Example

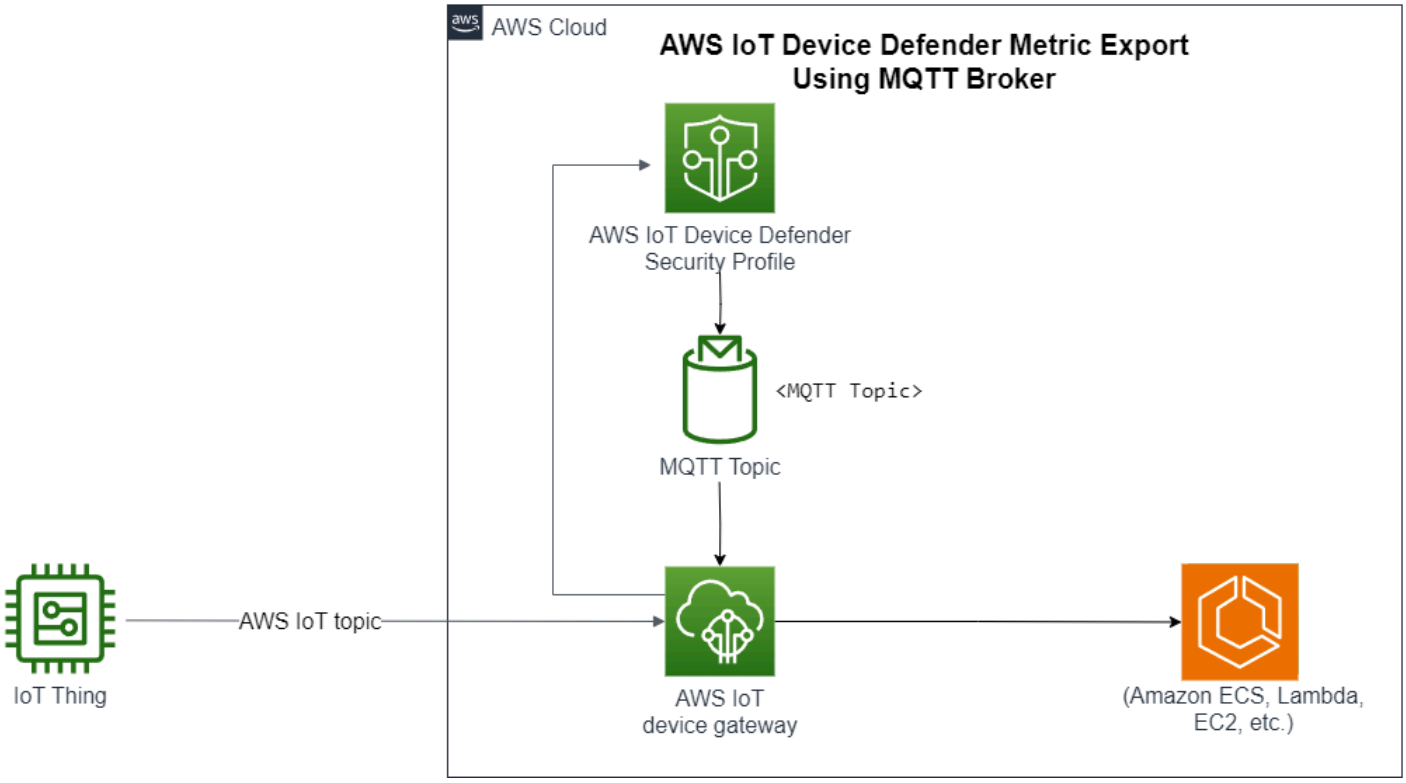
```
{
"name": "DisconnectDuration",
  "metric": "aws:disconnect-duration",
  "criteria": {
"comparisonOperator": "less-than-equals",
    "value": {
"count": 5
    }
  },
  "suppressAlerts": true
}
```

Exportación de métricas de Detect

Con la exportación de métricas, puede exportar métricas de la nube, del dispositivo o personalizadas desde AWS IoT Device Defender y publicarlas un tema de MQTT que configure. Esta característica admite la exportación masiva de métricas de Detect, lo que no solo permite generar informes y análisis de datos más eficientes, sino que también ayuda a controlar los costes. Puede elegir su tema de MQTT como un tema de AWS IoT Rules Basic Ingest o crear su propio tema de MQTT y suscribirse a él. Configure la exportación de métricas mediante la API, la CLI o la consola de AWS IoT Device Defender. Esta característica está disponible en todas las regiones de AWS en las que AWS IoT Device Defender está disponible.

La siguiente imagen muestra cómo puede configurarse AWS IoT Device Defender para exportar métricas. En el primer diagrama, se muestra cómo configurar las métricas de exportación en un tema de Basic Ingest. A continuación, puede enrutar las métricas exportadas a varios destinos compatibles con AWS IoT Rules. El segundo diagrama muestra cómo configurar AWS IoT Device Defender a fin de publicar datos en un tema de MQTT. Luego, el cliente MQTT se suscribe a ese tema. Puede ejecutar un cliente MQTT en un contenedor de Amazon Elastic Container Service, Lambda o una instancia de Amazon EC2 que esté suscrita al mismo tema de MQTT. Siempre que AWS IoT Device Defender publique los datos, el cliente MQTT los recibirá y los procesará. Para obtener más información, consulte Temas de 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.)

Cómo funciona la exportación de métricas de Detect

Al configurar un perfil de seguridad, se eligen las métricas que se van a exportar y se especifica el tema de MQTT. También puede configurar un rol de IAM que le conceda a AWS IoT Device Defender Detect los permisos necesarios para publicar mensajes en el tema de MQTT configurado. Puede configurar un tema de MQTT de AWS IoT Rules Basic Ingest y enviar las métricas exportadas a los destinos compatibles con AWS IoT Rules. Si desea obtener instrucciones sobre la configuración de AWS IoT Rules, consulte Rules for AWS IoT, en la Guía para desarrolladores de AWS IoT.

AWS IoT Device Defender Detect agrupa en un lote los valores de las métricas de cada métrica configurada y los publica en el tema de MQTT configurado a intervalos regulares. Con la excepción del tamaño de bytes del mensaje y del tamaño total de bytes, las métricas de la nube se agregan sumando los valores de las métricas de la duración del lote. Las métricas personalizadas y las del dispositivo no se agregan. En cuanto al tamaño de bytes del mensaje, los valores de exportación son el tamaño de byte mínimo, máximo y total durante la duración del lote. Para la duración de la desconexión, el valor de exportación es la duración de la desconexión (en segundos) de todos los dispositivos rastreados. Esto ocurre en cada intervalo de una hora y cuando hay eventos de conexión o desconexión. Para los dispositivos conectados o los eventos de conexión, el valor será cero. Para obtener más información sobre las métricas de la nube, las métricas del dispositivo y las métricas personalizadas, consulte los siguientes temas en la Guía para desarrolladores de AWS IoT Device Defender

- Métricas personalizadas
- Métricas del lado de la nube
- Métricas del lado del dispositivo

Puede exportar métricas por lotes a diferentes destinos con AWS IoT Rules. Para obtener una lista de los destinos compatibles, consulte AWS IoT rule actions. A fin de enviar métricas individuales de un mensaje de exportación por lotes a un destino compatible, puede usar la opción batchMode para las acciones de las reglas de AWS IoT. Si su destino de AWS IoT Rules preferido no es compatible con `batchMode`, puede enviar métricas individuales dentro de un mensaje por lotes mediante acciones intermedias, como Lambda o Kinesis Data Streams.

Esquema de exportación de métricas

Consulte el siguiente esquema para ver los datos de exportación de métricas por lotes.

```
{
 "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}"
 }
 }
 ]
}
```

Precios de exportación de métricas de Detect

Al publicar métricas de la nube, del dispositivo o personalizadas en un tema de MQTT que usted configure, no se le cobrará por este paso del proceso de exportación. Sin embargo, en los pasos siguientes, cuando transfiera las métricas publicadas al destino que elija (mediante el motor de reglas o Messaging), se le cobrará en función del método de transferencia que elija. AWS IoT Device Defender publica las métricas por lotes en los temas de MQTT como un mensaje único que contiene datos de métricas de varios dispositivos, lo que ayuda a controlar los costes. Para obtener más información sobre los precios, consulte la calculadora de precios de AWS.

Permisos

Esta sección contiene información sobre cómo configurar los roles y las políticas de IAM necesarios para administrar la exportación de métricas en AWS IoT Device Defender Detect. Para obtener más información, consulte la Guía del usuario de IAM.

Otorgar permiso a AWS IoT Device Defender Detect para publicar mensajes en un tema de SNS

Si utiliza la exportación de métricas en CreateSecurityProfile, debe especificar un rol de IAM con dos políticas: una política de permisos y otra de confianza. La política de permisos le otorga a AWS IoT Device Defender el permiso para publicar mensajes que incluyan métricas en un tema de MQTT. La política de confianza otorga permiso a AWS IoT Device Defender para asumir el rol requerido.

Política de permisos

```
{
  "Version":"2012-10-17",
  "Statement":[
      {
        "Effect":"Allow",
        "Action":[
          "iot:Publish"
        ],
        "Resource":[
          "arn:aws:iot:region:account-id:topic/your-topic-name"
        ]
    }
  ]
}
```

Política de confianza

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "iot.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Política para pasar roles

También necesita una política de permisos de IAM asociada al usuario de IAM que permita al usuario pasar roles. Consulte Concesión de permisos a un usuario para transferir un rol a un servicio de AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": [
          "iam:GetRole",
          "iam:PassRole"
      ],
      "Resource": "arn:aws:iam::account-id:role/Role_To_Pass"
    }
  ]
}
```

Configuración de la exportación de métricas de Detect en la consola de AWS IoT

Cree, vea y edite un nuevo perfil de seguridad que incluya la exportación de métricas en la consola.

Requisitos previos

Antes de configurar la exportación de métricas de Detect, asegúrese de cumplir los siguientes requisitos previos:

- Un rol de IAM. Para obtener información sobre la creación de un rol de IAM, consulte Creación de roles de IAM en la Guía del usuario de IAM.
- Una cuenta de AWS en la que puede iniciar sesión como usuario de AWS Identity and Access Management (IAM) con los permisos adecuados. Para obtener más información sobre los permisos de AWS IoT Device Defender Detect, consulte Permisos en la Guía para desarrolladores de AWS IoT Core.

Creación de un nuevo perfil de seguridad con exportación de métricas (consola)

Para poder exportar los datos de comportamiento de las métricas, primero debe configurar un perfil de seguridad que incluya la exportación de métricas. El siguiente procedimiento detalla cómo configurar un perfil de seguridad basado en reglas que incluya la exportación de métricas de Detect.

Para crear un nuevo perfil de seguridad con exportación de métricas

1. Abra la consola de AWS IoT. En la barra de navegación, amplíe Seguridad, Detect y Perfiles de seguridad.
2. En Crear perfil de seguridad, seleccione Crear perfil de detección de anomalías basado en reglas.
3. Para especificar las propiedades de su perfil de seguridad, introduzca el nombre de su perfil de seguridad y, en Destino, elija un grupo de dispositivos a los que dirigir las anomalías. (Opcional) Incluya una descripción y etiquetas para etiquetar los recursos de AWS. Seleccione Siguiente.
4. En Métrica, elija las métricas para definir el comportamiento del dispositivo. Puede definir el umbral de comportamiento para recibir alertas cuando su dispositivo no cumpla las expectativas de comportamiento.
5. Para recibir alertas sobre anomalías de comportamiento, elija Enviar una alerta (definir el comportamiento de la métrica) y especifique el Nombre del comportamiento y las condiciones. Para retener las métricas sin alertas, seleccione No enviar una alerta (retener la métrica). Elija Siguiente.
6. Para configurar las exportaciones de métricas, elija Activar las métricas de exportación.

7. Introduzca el nombre de un tema de MQTT para publicar los datos de las métricas en AWS IoT Core. Elija un rol de IAM para conceder a AWS IoT el permiso “AWS IoT:Publish” para publicar mensajes en el tema configurado. Seleccione la métrica que desea exportar y, a continuación, Siguiente.

> **Note**
>
> Utilice la barra diagonal para representar información jerárquica al introducir el nombre del tema de MQTT. Por ejemplo, `$AWS/rules/rule-name/`.

8. A fin de enviar alertas a su consola de AWS cuando un dispositivo infrinja un comportamiento establecido, elija o cree un tema de Amazon SNS y un rol de IAM. Seleccione Siguiente.
9. Revise sus configuraciones y elija Siguiente.

Visualización y edición de los detalles del perfil de seguridad (consola)

Para ver y editar los detalles del perfil de seguridad

1. Abra la consola de AWS IoT. En la barra de navegación, amplíe Seguridad, Detect y Perfiles de seguridad.
2. Seleccione el perfil de seguridad que creó para incluir la exportación de métricas y elija Editar en Acciones.
3. En Destino, seleccione los grupos de dispositivos de destino que desee editar y seleccione Siguiente.
4. Para editar las configuraciones del comportamiento de las métricas, elija Recibir alertas (definir el comportamiento de la métrica) y defina las condiciones en las que se cumplen los comportamientos de las métricas. Seleccione Siguiente.
5. Para desactivar las configuraciones de exportación de métricas, elija Desactivar las métricas de exportación. Seleccione Siguiente.
6. A fin de configurar Amazon SNS de modo que envíe alertas a su consola de AWS IoT cuando un dispositivo infrinja un comportamiento establecido, elija o cree un tema de Amazon SNS y un rol de IAM. Seleccione Siguiente.
7. Revise sus configuraciones y elija Siguiente.

Crear un perfil de seguridad y habilitar la exportación de métricas

Utilice el comando `create-security-profile` para crear su perfil de seguridad y habilitar la exportación de métricas.

Para crear un perfil de seguridad con exportación de métricas

1. Para habilitar la exportación de métricas e indicar si Detect necesita exportar las métricas correspondientes, defina el valor `exportMetric` como verdadero en `Behavior` y `AdditionalMetricsToRetainV2`.
2. Incluya el valor para `MetricsExportConfig`. Esto especifica el tema de MQTT y el Nombre de recurso de Amazon (ARN) de rol necesarios para la exportación de métricas.

> **Note**
>
> Incluya `mqttTopic` para que AWS IoT Device Defender Detect pueda publicar mensajes. El ARN de rol tiene permiso para publicar mensajes de MQTT, tras lo cual, AWS IoT Device Defender Detect puede asumir el rol y publicar mensajes en su nombre.

```
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
```

Salida:

```
{
    "securityProfileName": "CreateSecurityProfileWithMetricsExport",
    "securityProfileArn": "arn:aws:iot:us-east-1:123456789012:securityprofile/
CreateSecurityProfileWithMetricsExport"
}
```

Actualización de un perfil de seguridad para habilitar la exportación de métricas (CLI)

Utilice el comando de `update-security-profile` para actualizar un perfil de seguridad existente y activar la exportación de métricas.

Para actualizar un perfil de seguridad a fin de activar la exportación de métricas

1. Para habilitar la exportación de métricas e indicar si Detect necesita exportar las métricas correspondientes, defina el valor `exportMetric` como verdadero en `Behavior` y `AdditionalMetricsToRetainV2`.
2. Incluya el valor para `MetricsExportConfig`. Esto especifica el tema de MQTT y el Nombre de recurso de Amazon (ARN) de rol necesarios para la exportación de métricas.

> **Note**
>
> Incluya `mqttTopic` para que AWS IoT Device Defender Detect pueda publicar mensajes. El ARN de rol tiene permiso para publicar mensajes de MQTT, tras lo cual, AWS IoT Device Defender Detect puede asumir el rol y publicar mensajes en su nombre.

```
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
```

Salida:

```
{
    "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"
    }
}
```

Actualización de un perfil de seguridad para deshabilitar la exportación de métricas (CLI)

Utilice el comando de `update-security-profile` para actualizar un perfil de seguridad existente y desactivar la exportación de métricas.

Para actualizar un perfil de seguridad a fin de desactivar la exportación de métricas

- Para actualizar su perfil de seguridad y eliminar la configuración de exportación de métricas, utilice el 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
```

Salida:

```
{
    "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"
}
```

Para obtener más información, consulte comandos Detect en la Guía para desarrolladores de AWS IoT.

Comandos de la CLI para exportación de métricas

Puede utilizar los siguientes comandos de la CLI para crear y administrar la exportación de métricas de Detect.

- CreateSecurityProfile
- UpdateSecurityProfile
- DescribeSecurityProfile

Operaciones de la API de exportación de métricas

Puede utilizar las siguientes operaciones de API para crear y administrar la exportación de métricas de Detect.

- CreateSecurityProfile
- UpdateSecurityProfile
- DescribeSecurityProfile

Establecer el ámbito de las métricas en los perfiles de seguridad utilizando dimensiones

Las dimensiones son atributos que se pueden definir para obtener datos más precisos sobre las métricas y los comportamientos del perfil de seguridad. El ámbito se define proporcionando un valor o patrón que se utiliza como filtro. Por ejemplo, puede definir una dimensión de filtrado de temas que aplique una métrica solo a los temas de MQTT que coincidan con un determinado valor; por ejemplo "data/bulb/+/activity". Para obtener más información acerca de cómo definir una dimensión que pueda utilizar en el perfil de seguridad, consulte CreateDimension.

Se pueden utilizar comodines de MQTT en los valores de las dimensiones. Los comodines de MQTT le permiten suscribirse a varios temas simultáneamente. Hay dos tipos diferentes de comodines: de un nivel (+) y de varios niveles (`#`). Por ejemplo, el valor de dimensión `Data/bulb/+/activity` crea una suscripción que busca correspondencias en todos los temas que existen en el mismo nivel que +. Los valores de dimensión también admiten la variable de sustitución del ID de cliente de MQTT ${iot:ClientId}.

Las dimensiones de tipo TOPIC_FILTER son compatibles con el siguiente conjunto de métricas del lado de la nube:

- Número de errores de autorización
- Tamaño de bytes del mensaje
- Número de mensajes recibidos
- Número de mensajes enviados
- Dirección IP de origen (solo disponible para Rules Detect)

Cómo utilizar las dimensiones en la consola

Para crear una dimensión y aplicarla a un comportamiento del perfil de seguridad

1. Abra la consola de AWS IoT. En el panel de navegación, amplíe Seguridad, Detect y, a continuación, elija Perfiles de seguridad.
2. Seleccione Perfiles de seguridad, Crear perfil de seguridad y, a continuación, Crear perfil de detección de anomalías basado en reglas. O bien, para aplicar una dimensión a un perfil de seguridad basado en reglas existente, seleccione el perfil de seguridad y elija Editar.
3. En la página Especificar las propiedades del perfil de seguridad, introduzca un nombre para el perfil de seguridad.
4. Elija el grupo de dispositivos al que desee dirigirse para detectar anomalías.
5. Seleccione Siguiente.
6. En la página Configurar los comportamientos de las métricas, elija una de las dimensiones métricas del lado de la nube en Tipo de métrica.
7. En Comportamientos de la métrica, seleccione Enviar una alerta (definir el comportamiento de la métrica) para definir el comportamiento esperado de la métricas.
8. Elija cuándo quiere que se le notifique el comportamiento inusual del dispositivo.
9. Seleccione Siguiente.
10. Revise la configuración del perfil de seguridad y seleccione Crear.

Para ver sus alarmas

1. Abra la consola de AWS IoT. En el panel de navegación, amplíe Seguridad, Detect y, a continuación, elija Alarmas.

2. En la columna Nombre de la cosa, seleccione el objeto para ver información sobre la causa de la alarma.

Para ver y actualizar las dimensiones

1. Abra la consola de AWS IoT. En el panel de navegación, amplíe Seguridad, Detect y, a continuación, elija Dimensiones.
2. Seleccione la dimensión y, a continuación, elija Editar.
3. Edite la dimensión y, a continuación, elija Actualizar.

Para eliminar una dimensión

1. Abra la consola de AWS IoT. En el panel de navegación, amplíe Seguridad, Detect y, a continuación, elija Dimensiones.
2. Antes de eliminar una dimensión, debe eliminar el comportamiento métrico que hace referencia a la dimensión. Para confirmar que la dimensión no está asociada a ningún perfil de seguridad, consulte la columna Perfiles de seguridad. Si la dimensión está asociada a un perfil de seguridad, abra la página Security profiles (Perfiles de seguridad) de la izquierda y edite el perfil de seguridad al que está asociada la dimensión. Continúe después con la eliminación del comportamiento. Si desea eliminar otra dimensión, siga los pasos de esta sección.
3. Seleccione la dimensión y elija Eliminar.
4. Escriba el nombre de la dimensión para confirmarlo y luego elija Eliminar.

Cómo utilizar las dimensiones en la AWS CLI

Para crear una dimensión y aplicarla a un comportamiento del perfil de seguridad

1. Primero cree la dimensión antes de asociarla a un perfil de seguridad. Utilice el comando CreateDimension para crear una dimensión.

```
aws iot create-dimension \
  --name TopicFilterForAuthMessages \
  --type TOPIC_FILTER \
  --string-values device/+/auth
```

   El resultado de este comando tendrá un aspecto similar al siguiente.

```
{
    "arn": "arn:aws:iot:us-west-2:123456789012:dimension/
TopicFilterForAuthMessages",
    "name": "TopicFilterForAuthMessages"
}
```

2. Agregue la dimensión a un perfil de seguridad existente mediante UpdateSecurityProfile, o agregue la dimensión a un nuevo perfil de seguridad mediante CreateSecurityProfile. En el siguiente ejemplo, creamos un nuevo perfil de seguridad que comprueba si los mensajes a `TopicFilterForAuthMessages` tienen menos de 128 bytes y conserva el número de mensajes enviados a temas que no son de autenticación.

```
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\"}}]"
```

El resultado de este comando tendrá un aspecto similar al siguiente.

```
{
    "securityProfileArn": "arn:aws:iot:us-west-2:1234564789012:securityprofile/
ProfileForConnectedDevice",
    "securityProfileName": "ProfileForConnectedDevice"
}
```

Para ahorrar tiempo, también puede cargar un parámetro desde un archivo en lugar de escribirlo como un valor de parámetro de línea de comandos. Para obtener más información, consulte Carga de parámetros de AWS CLI desde un archivo. A continuación se muestra el parámetro `behavior` en formato JSON expandido:

```
[
  {
    "criteria": {
      "comparisonOperator": "less-than",
      "consecutiveDatapointsToAlarm": 1,
      "consecutiveDatapointsToClear": 1,
      "value": {
        "count": 128
      }
    },
    "metric": "aws:message-byte-size",
    "metricDimension": {
      "dimensionName:": "TopicFilterForAuthMessages"
    },
    "name": "CellularBandwidth"
  }
]
```

O utilice CreateSecurityProfile con la dimensión con machine learning, como en el siguiente ejemplo:

```
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
```

Para ver perfiles de seguridad con una dimensión

- Utilice el comando ListSecurityProfiles para ver perfiles de seguridad con una dimensión determinada:

```
aws iot list-security-profiles \
  --dimension-name TopicFilterForAuthMessages
```

El resultado de este comando tendrá un aspecto similar al siguiente.

```
{
    "securityProfileIdentifiers": [
        {
            "name": "ProfileForConnectedDevice",
            "arn": "arn:aws:iot:us-west-2:1234564789012:securityprofile/
ProfileForConnectedDevice"
        }
    ]
}
```

Para actualizar la dimensión

- Utilice el comando UpdateDimension para actualizar una dimensión:

```
aws iot update-dimension \
  --name TopicFilterForAuthMessages \
  --string-values device/${iot:ClientId}/auth
```

El resultado de este comando tendrá un aspecto similar al siguiente.

```
{
    "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"
}
```

Para eliminar una dimensión

1. Para eliminar una dimensión, primero desconéctela de los perfiles de seguridad a los que esté asociada. Utilice el comando ListSecurityProfiles para ver perfiles de seguridad con una dimensión determinada.

2. Para quitar una dimensión de un perfil de seguridad, utilice el comando UpdateSecurityProfile. Introduzca toda la información que desee conservar, pero excluya la dimensión:

```
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}}]"
```

El resultado de este comando tendrá un aspecto similar al siguiente.

```
{
  "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. Una vez desconectada la dimensión, utilice el comando DeleteDimension para eliminar la dimensión:

```
aws iot delete-dimension \
  --name TopicFilterForAuthMessages
```

Permisos

Esta sección contiene información sobre cómo configurar los roles y políticas de IAM necesarios para administrar AWS IoT Device Defender Detect. Para obtener más información, consulte la Guía del usuario de IAM.

Otorgar permiso a AWS IoT Device Defender Detect para publicar alarmas en un tema de SNS

Si utiliza el parámetro `alertTargets` en CreateSecurityProfile, debe especificar un rol de IAM con dos políticas: una política de permisos y una política de confianza. La política de permisos concede permiso a AWS IoT Device Defender para publicar notificaciones en su tema de SNS. La política de confianza otorga permiso a AWS IoT Device Defender para asumir el rol requerido.

Política de permisos

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

```
        "Action":[
          "sns:Publish"
        ],
        "Resource":[
          "arn:aws:sns:region:account-id:your-topic-name"
        ]
    }
  ]
}
```

Política de confianza

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "iot.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Política para pasar roles

También necesita una política de permisos de IAM asociada al usuario de IAM que permita al usuario pasar roles. Consulte Concesión de permisos a un usuario para transferir un rol a un servicio de AWS.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Action": [
          "iam:GetRole",
          "iam:PassRole"
      ],
```

```
      "Resource": "arn:aws:iam::account-id:role/Role_To_Pass"
    }
  ]
}
```

Comandos de detección

Puede usar los comandos Detect de esta sección para configurar los perfiles de seguridad ML Detect o Rules Detect, con el fin de identificar y monitorizar comportamientos inusuales que puedan indicar un dispositivo comprometido.

Comandos de las acciones de mitigación de Detect

Iniciar y administrar la ejecución de Detect
CancelDetectMitigationActionsTask
DescribeDetectMitigationActionsTask
ListDetectMitigationActionsTasks
StartDetectMitigationActionsTask
ListDetectMitigationActionsExecutions

Comandos de las acciones de dimensiones

Iniciar y administrar la ejecución de dimensiones
CreateDimension
DescribeDimension
ListDimensions
DeleteDimension
UpdateDimension

Comandos de las acciones de métricas personalizadas

Iniciar y administrar la ejecución de métricas personalizadas
CreateCustomMetric
UpdateCustomMetric
DescribeCustomMetric
ListCustomMetrics
DeleteCustomMetric

Comandos de las acciones de perfil de seguridad

Iniciar y administrar la ejecución del perfil de seguridad
CreateSecurityProfile
AttachSecurityProfile
DetachSecurityProfile
DeleteSecurityProfile
DescribeSecurityProfile
ListTargetsForSecurityProfile
UpdateSecurityProfile
ValidateSecurityProfileBehaviors
ListSecurityProfilesForTarget

Comandos de las acciones de alarmas

Administrar las alarmas y los destinos
ListActiveViolations

Administrar las alarmas y los destinos
ListViolationEvents
PutVerificationStateOnViolation

Comandos de las acciones de ML Detect

Enumerar los datos de entrenamiento del modelo ML
GetBehaviorModelTrainingSummaries

Cómo utilizar AWS IoT Device Defender Detect

1. Puede usar AWS IoT Device Defender Detect solo con las métricas del lado de la nube, pero si pretende usar métricas notificadas por el dispositivo, primero debe implementar el SDK de AWS IoT en sus dispositivos conectados a AWS IoT o en las gateways de dispositivos. Para obtener más información, consulte Envío de métricas desde dispositivos.
2. Considere la posibilidad de ver las métricas que sus dispositivos generan antes de definir comportamientos y crear alarmas. AWS IoT puede recopilar métricas de sus dispositivos, por lo que puede identificar en primer lugar un comportamiento habitual o inusual de un grupo de dispositivos o de todos los dispositivos de su cuenta. Use CreateSecurityProfile, pero especifique solo aquellos `additionalMetricsToRetain` que le interesen. No especifique `behaviors` en este punto.

   Utilice la consola de AWS IoT para analizar sus métricas de dispositivos y determinar qué constituye un comportamiento típico para sus dispositivos.
3. Cree un conjunto de comportamientos para el perfil de seguridad. Los comportamientos contienen métricas que especifican el comportamiento normal de un grupo de dispositivos o de todos los dispositivos de su cuenta. Para obtener más información y ejemplos, consulte Métricas del lado de la nube y Métricas del lado del dispositivo. Después de crear un conjunto de comportamientos, puede validarlos con ValidateSecurityProfileBehaviors.
4. Utilice la acción CreateSecurityProfile para crear un perfil de seguridad que incluya los comportamientos. Puede utilizar el parámetro `alertTargets` para enviar alarmas a un destino (un tema de SNS) cuando un dispositivo vulnere un comportamiento. (Si envía alarmas usando SNS, tenga en cuenta que estas se tendrán en cuenta para calcular la cuota de temas de SNS

de su Cuenta de AWS. Si se produce una gran oleada de infracciones, podría superarse la cuota de temas de SNS. También puede utilizar las métricas de CloudWatch para comprobar las vulneraciones. Para obtener más información, consulte Monitor AWS IoT alarms and metrics using Amazon CloudWatch, en la Guía para desarrolladores de AWS IoT Core.

5. Utilice la acción AttachSecurityProfile para asociar el perfil de seguridad a un grupo de dispositivos (un grupo de objetos), a todos los objetos registrados en la cuenta, a todos los objetos no registrados o a todos los dispositivos AWS IoT Device Defender. Detect comienza comprobando si hay un comportamiento anómalo, y si se detectan vulneraciones del comportamiento, envía alarmas. Es posible que desee asociar un perfil de seguridad a todos los objetos no registrados si, por ejemplo, tiene previsto interactuar con dispositivos móviles que no están en el registro de objetos de su cuenta. Puede definir diferentes conjuntos de comportamientos para diferentes grupos de dispositivos para satisfacer sus necesidades.

   Para asociar un perfil de seguridad a un grupo de dispositivos, debe especificar el ARN del grupo de objetos que los contiene. El ARN de un grupo de objetos tiene el siguiente formato:

   ```
   arn:aws:iot:region:account-id:thinggroup/thing-group-name
   ```

   Para asociar un perfil de seguridad a todos los objetos registrados en una Cuenta de AWS (y omitir los objetos no registrados), debe especificar un ARN con el siguiente formato.

   ```
   arn:aws:iot:region:account-id:all/registered-things
   ```

   Para asociar un perfil de seguridad a todos los objetos no registrados, debe especificar un ARN con el siguiente formato:

   ```
   arn:aws:iot:region:account-id:all/unregistered-things
   ```

   Para asociar un perfil de seguridad a todos los dispositivos, debe especificar un ARN con el siguiente formato:

   ```
   arn:aws:iot:region:account-id:all/things
   ```

6. También puede realizar un seguimiento de las infracciones con la acción ListActiveViolations , que le permite ver qué infracciones se han detectado en un perfil de seguridad o dispositivo de destino determinado.

Utilice la acción ListViolationEvents para ver qué infracciones se detectaron durante un período de tiempo especificado. Puede filtrar estos resultados por perfil de seguridad, dispositivo o estado de verificación de alarma.

7. Puede verificar, organizar y administrar sus alarmas marcando su estado de verificación y proporcionando una descripción de ese estado de verificación mediante la acción PutVerificationStateOnViolation.
8. Si sus dispositivos infringen los comportamientos definidos con demasiada frecuencia o no lo suficiente, debe ajustar el comportamiento.
9. Para revisar los perfiles de seguridad que ha configurado y los dispositivos que se están monitorizando, utilice las acciones ListSecurityProfiles, ListSecurityProfilesForTarget y ListTargetsForSecurityProfile.

   Utilice la acción DescribeSecurityProfile para obtener más detalles sobre un perfil de seguridad.
10. Para actualizar un perfil de seguridad, utilice la acción UpdateSecurityProfile. Utilice la acción DetachSecurityProfile para desconectar un perfil de seguridad de destino de una cuenta o grupo de objetos. Utilice la acción DeleteSecurityProfile para eliminar completamente un perfil de seguridad.

Acciones de mitigación

Se puede utilizar AWS IoT Device Defender para tomar medidas con el fin de mitigar los problemas que se detectaron en un resultado de auditoría o en una alarma de Detect.

> **Note**
>
> No se llevarán a cabo acciones de mitigación cuando se supriman los resultados de una auditoría. Para obtener más información acerca de las supresiones de resultados de la auditoría, consulte Supresiones de resultados de auditoría.

Acciones de mitigación de auditoría

AWS IoT Device Defender proporciona acciones predefinidas para las diferentes comprobaciones de auditoría. Puede configurar esas acciones para su Cuenta de AWS y, a continuación, aplicarlas a un conjunto de resultados. Estos resultados pueden ser:

- Todos los resultados de una auditoría. Esta opción está disponible en la consola de AWS IoT y a través de la AWS CLI.
- Una lista de resultados individuales. Esta opción solo está disponible a través de la AWS CLI
- Un conjunto filtrado de los resultados de una auditoría.

En la siguiente tabla se muestran los tipos de las comprobaciones de auditoría y las acciones de mitigación compatibles para cada una de ellas:

Comprobación de auditoría y acción de mitigación

Comprobación de auditoría	Acciones de mitigación admitidas
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

Comprobación de auditoría	Acciones de mitigación admitidas
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

Comprobación de auditoría	Acciones de mitigación admitidas
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

Todas las comprobaciones de auditoría admiten la publicación de los resultados de la auditoría en Amazon SNS para que pueda tomar acciones personalizadas en respuesta a la notificación. Cada tipo de comprobación de auditoría puede admitir acciones de mitigación adicionales:

REVOKED_CA_CERT_CHECK

- Cambiar el estado del certificado para marcarlo como inactivo en AWS IoT.

DEVICE_CERTIFICATE_SHARED_CHECK

- Cambiar el estado del certificado del dispositivo para marcarlo como inactivo en AWS IoT.
- Agregar dispositivos que utilizan dicho certificado a un grupo de objetos.

UNAUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK

- No se admiten otras acciones.

AUTHENTICATED_COGNITO_ROLE_OVERLY_PERMISSIVE_CHECK

- No se admiten otras acciones.

IOT_POLICY_OVERLY_PERMISSIVE_CHECK

- Agregar una versión de política de AWS IoT en blanco para restringir los permisos.

IOT_POLICY_POTENTIAL_MISCONFIGURATION_CHECK

- Identificar posibles errores de configuración en las políticas de AWS IoT.

CA_CERT_APPROACHING_EXPIRATION_CHECK

- Cambiar el estado del certificado para marcarlo como inactivo en AWS IoT.

CONFLICTING_CLIENT_IDS_CHECK

- No se admiten otras acciones.

DEVICE_CERT_APPROACHING_EXPIRATION_CHECK

- Cambiar el estado del certificado del dispositivo para marcarlo como inactivo en AWS IoT.
- Agregar dispositivos que utilizan dicho certificado a un grupo de objetos.

DEVICE_CERTIFICATE_KEY_QUALITY_CHECK

- Cambiar el estado del certificado del dispositivo para marcarlo como inactivo en AWS IoT.
- Agregar dispositivos que utilizan dicho certificado a un grupo de objetos.

CA_CERTIFICATE_KEY_QUALITY_CHECK

- Cambiar el estado del certificado para marcarlo como inactivo en AWS IoT.

REVOKED_DEVICE_CERT_CHECK

- Cambiar el estado del certificado del dispositivo para marcarlo como inactivo en AWS IoT.
- Agregar dispositivos que utilizan dicho certificado a un grupo de objetos.

LOGGING_DISABLED_CHECK

- Habilitar el registro.

AWS IoT Device Defender admite los siguientes tipos de acciones de mitigación en los resultados de auditoría:

Tipo de acción	Notas
ADD_THINGS_TO_THING_GROUP	Debe especificar el grupo a la que desea agregar los dispositivos. También debe especificar si la suscripción a uno o varios grupos dinámicos debe anularse si se supera el número máximo de grupos a los que el objeto puede pertenecer.
ENABLE_IOT_LOGGING	Debe especificar el nivel de registro y el rol con permisos para el registro. No puede especificar un nivel de registro `DISABLED`.
PUBLISH_FINDING_TO_SNS	Debe especificar el tema en el que se debe publicar la búsqueda.
REPLACE_DEFAULT_POLICY_VERSION	Debe especificar el nombre de la plantilla. Sustituye la versión de la política predeterm

Tipo de acción	Notas
	inada con una política en blanco. En este momento solo es compatible un valor de `BLANK_POLICY` .
UPDATE_CA_CERTIFICATE	Debe especificar el nuevo estado para el certificado de entidad de certificación. En este momento solo es compatible un valor de `DEACTIVATE` .
UPDATE_DEVICE_CERTIFICATE	Debe especificar el nuevo estado para el certificado del dispositivo. En este momento solo es compatible un valor de `DEACTIVATE` .

Al configurar acciones estándar para los problemas encontrados durante una auditoría, puede responder a estos problemas de forma coherente. Utilizar estas acciones de mitigación definidas también le ayuda a resolver los problemas con mayor rapidez y con menos posibilidad de que se produzcan errores.

> **Important**
>
> La aplicación de acciones de mitigación que cambian los certificados, agregan objetos a un nuevo grupo de objetos o sustituyen la política puede tener un impacto en sus dispositivos y aplicaciones. Por ejemplo, es posible que los dispositivos no puedan conectarse. Tenga en cuenta las implicaciones de las acciones de mitigación antes de aplicarlas. Es posible que tenga que adoptar otras medidas para corregir problemas antes de que los dispositivos y las aplicaciones puedan funcionar con normalidad. Por ejemplo, es posible que tenga que proporcionar certificados de dispositivo actualizados. Las acciones de mitigación pueden ayudarle a limitar rápidamente los riesgos pero, aún así, tiene que tomar medidas correctoras para resolver los problemas.

Algunas acciones, como, por ejemplo, reactivar un certificado de dispositivo, solo se pueden realizar manualmente. AWS IoT Device Defender no proporciona un mecanismo para revertir automáticamente las acciones de mitigación que se han aplicado.

Acciones de mitigación de Detect

AWS IoT Device Defender admite los siguientes tipos de acciones de mitigación en alarmas de Detect:

Tipo de acción	Notas
ADD_THINGS_TO_THING_GROUP	Debe especificar el grupo a la que desea agregar los dispositivos. También debe especificar si la suscripción a uno o varios grupos dinámicos debe anularse si se supera el número máximo de grupos a los que el objeto puede pertenecer.

Cómo definir y administrar las acciones de mitigación

Puede utilizar la consola de AWS IoT o la AWS CLI para definir y administrar acciones de mitigación para su Cuenta de AWS.

Creación de acciones de mitigación

Cada acción de mitigación que defina es una combinación de un tipo de acción predefinida y los parámetros específicos de su cuenta.

Para utilizar la consola de AWS IoT para crear acciones de mitigación

1. Abra la página Acciones de mitigación en la consola de AWS IoT.
2. En la página Acciones de mitigación, elija Crear.
3. En la página Crear una nueva acción de mitigación, en Nombre de la acción, escriba un nombre único para la acción de mitigación.
4. En Action type (Tipo de acción), especifique el tipo de acción que desea definir.
5. En Permisos, elija el rol de IAM bajo cuyos permisos se aplica la acción.
6. Cada tipo de acción solicita un conjunto diferente de parámetros. Escriba los parámetros de la acción. Por ejemplo, si elige el tipo de acción Agregar objetos al grupo de objetos, debe elegir el grupo de destino y seleccionar o quitar la marca de verificación de Override dynamic groups (Anular grupos dinámicos).

7. Elija Guardar para guardar la acción de mitigación en su cuenta de AWS.

Para utilizar la AWS CLI para crear acciones de mitigación

- Utilice el comando CreateMitigationAction para crear la acción de mitigación. El nombre único que dé a la acción se utiliza cuando se aplica dicha acción a los resultados de la auditoría. Elija un nombre significativo.

Para utilizar la consola de AWS IoT para ver y modificar las acciones de mitigación

1. Abra la página Acciones de mitigación en la consola de AWS IoT.

   La página Acciones de mitigación muestra una lista de todas las acciones de mitigación definidas para su Cuenta de AWS.
2. Elija el enlace del nombre de acción de la acción de mitigación que desea cambiar.
3. Seleccione Editar y realice sus cambios en la acción de mitigación. No puede cambiar el nombre porque el nombre de la acción de mitigación se utiliza para identificarla.
4. Elija Actualizar para guardar los cambios de la acción de mitigación en su Cuenta de AWS.

Para utilizar la AWS CLI para obtener una lista de acciones de mitigación

- Utilice el comando ListMitigationAction para mostrar las acciones de mitigación. Si desea cambiar o eliminar una acción de mitigación, anote del nombre.

Para utilizar la AWS CLI para actualizar una acción de mitigación

- Utilice el comando UpdateMitigationAction para cambiar la acción de mitigación.

Para utilizar la consola de AWS IoT para eliminar una acción de mitigación

1. Abra la página Acciones de mitigación en la consola de AWS IoT.

   La página Acciones de mitigación muestra todas las acciones de mitigación definidas para su Cuenta de AWS.
2. Elija la acción de mitigación que quiera eliminar y, a continuación, seleccione Eliminar.
3. En la ventana de confirmación de la eliminación, seleccione Eliminar.

Para utilizar la AWS CLI para eliminar acciones de mitigación

- Utilice el comando UpdateMitigationAction para cambiar la acción de mitigación.

Para utilizar la consola de AWS IoT para ver los detalles de una acción de mitigación

1. Abra la página Acciones de mitigación en la consola de AWS IoT.

   La página Acciones de mitigación muestra todas las acciones de mitigación definidas para su Cuenta de AWS.

2. Elija el enlace del nombre de acción de la acción de mitigación que quiera ver.

Para utilizar la AWS CLI para ver los detalles de una acción de mitigación

- Utilice el comando DescribeMitigationAction para ver los detalles de su acción de mitigación.

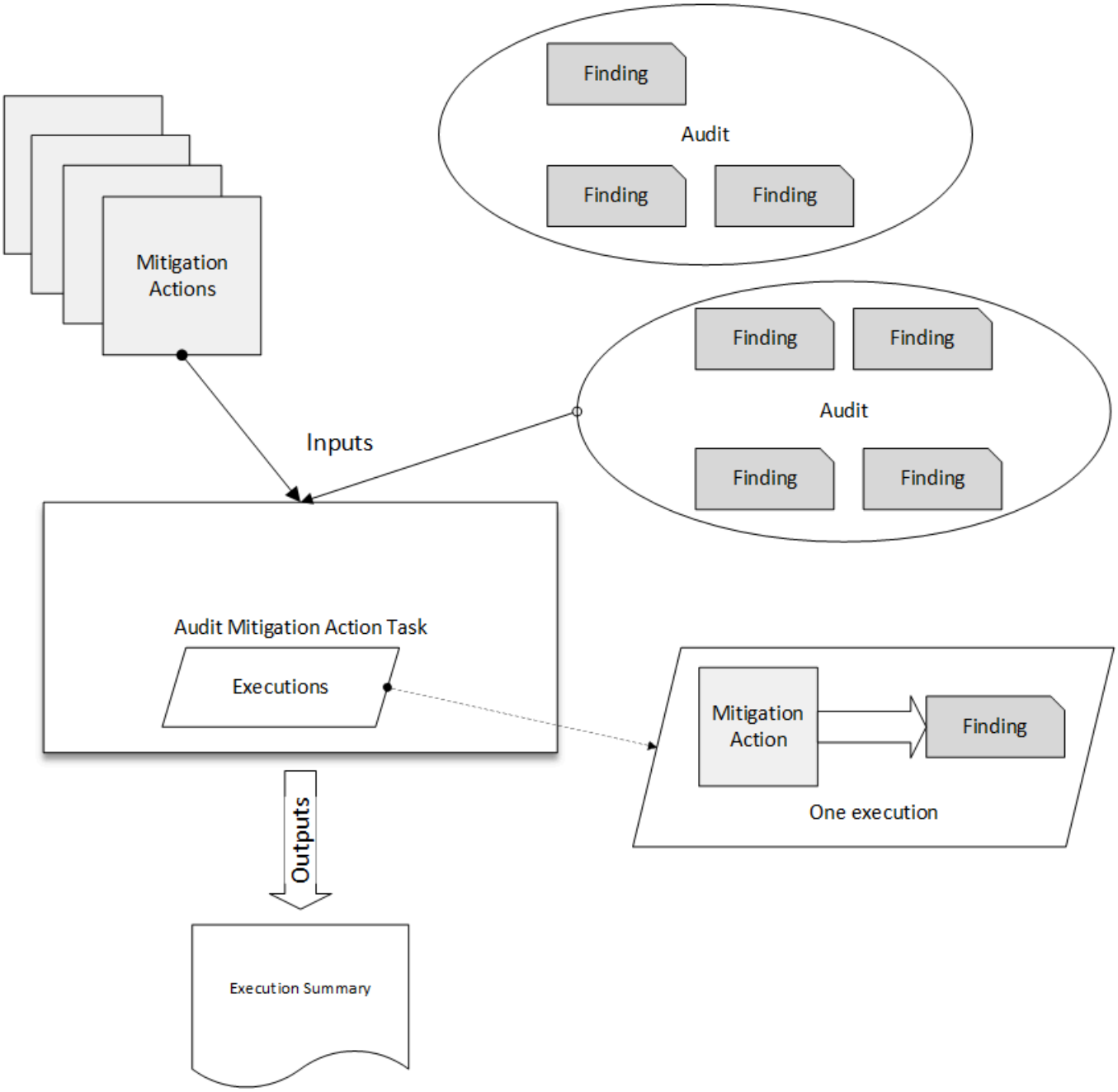
Aplicación de acciones de mitigación

Después de haber definido un conjunto de acciones de mitigación, puede aplicar esas acciones a los resultados de una auditoría. Cuando se aplican acciones, empieza una tarea de acciones de mitigación de auditoría. Esta tarea podría tardar un tiempo en completarse, en función del conjunto de resultados y las acciones que se aplican a ellos. Por ejemplo, si tiene un gran grupo de dispositivos cuyos certificados han caducado, puede tardar algún tiempo en desactivar todos estos certificados o en mover esos dispositivos a un grupo de cuarentena. Otras acciones, como la habilitación del registro, se pueden realizar con rapidez.

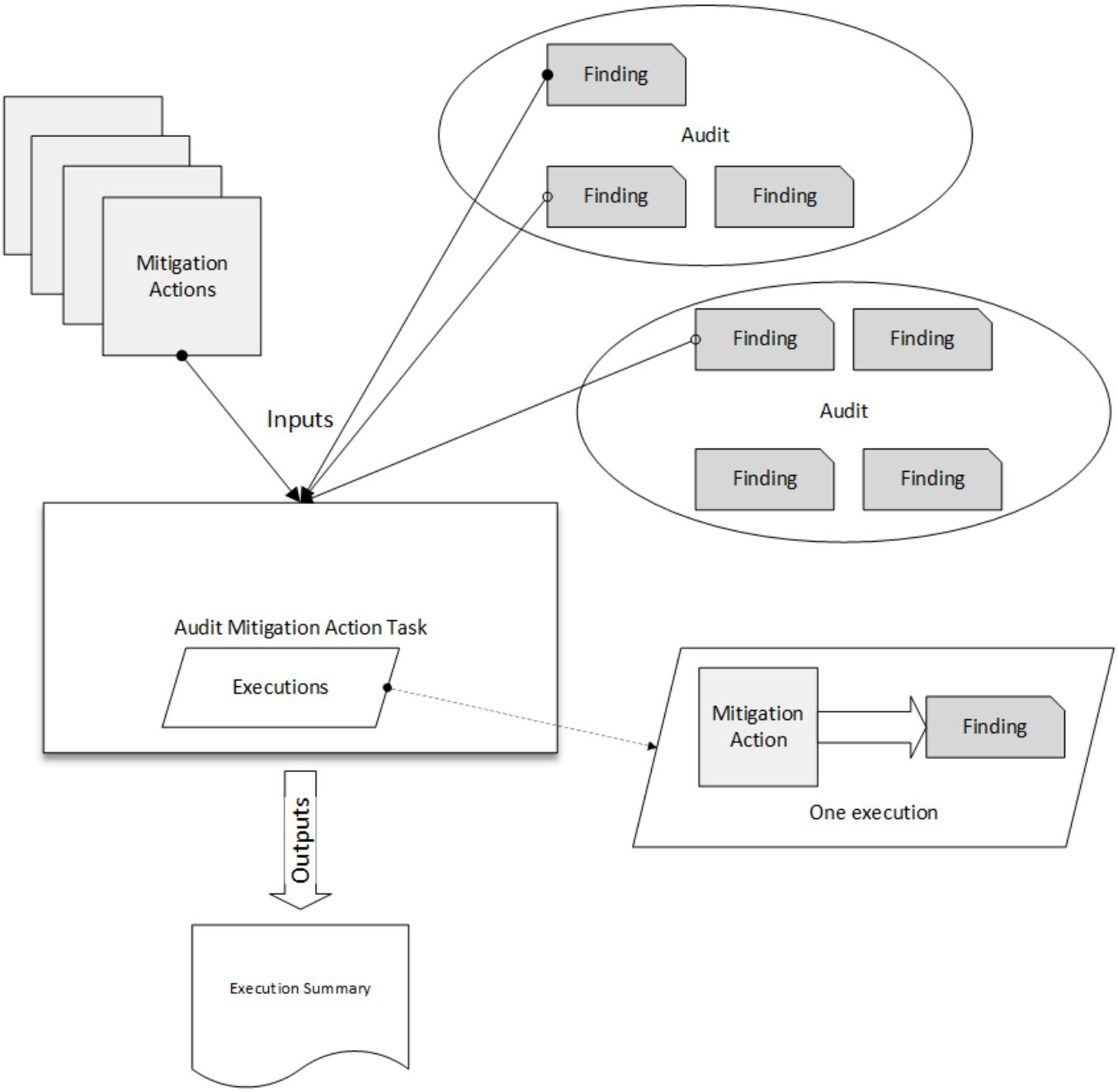
Puede ver la lista de ejecuciones de acciones y cancelar una ejecución que aún no se ha completado. Las acciones ya realizadas como parte de la ejecución de la acción cancelada no se revierten. Si está aplicando varias acciones a un conjunto de resultados y una de esas acciones produce un error, se omiten la acciones posteriores para ese resultado (pero se siguen aplicado a otros resultados). El estado de la tarea para el resultado es FAILED. El `taskStatus` se establece como error (Failed) si una o varias de las acciones fracasan cuando se aplican a los resultados. Las acciones se aplican en el orden en que estén especificadas.

Cada ejecución de acción aplica a un conjunto de acciones a un destino. Ese destino puede ser una lista de resultados o puede ser todos los resultados de una auditoría.

En el siguiente diagrama se muestra cómo puede definir una tarea de mitigación de auditoría para que tome todos los resultados de una auditoría y les aplique un conjunto de acciones. Una única ejecución aplica una acción a un resultado. La tarea de acciones de mitigación de auditoría genera un resumen de ejecución.



En el siguiente diagrama se muestra cómo puede definir una tarea de mitigación de auditoría para que tome una lista de resultados individuales de una o varias auditorías y les aplique un conjunto de acciones. Una única ejecución aplica una acción a un resultado. La tarea de acciones de mitigación de auditoría genera un resumen de ejecución.



Puede utilizar la AWS CLI o la consola de AWS IoT para aplicar acciones de mitigación.

Para usar la consola AWS IoT para aplicar acciones de mitigación iniciando la ejecución de una acción

1. Abra la página de resultados de la auditoría en la consola de AWS IoT.
2. Elija el nombre de la auditoría a la que desea aplicar acciones.

3. Seleccione Iniciar las acciones de mitigación. Este botón no está disponible si todos las comprobaciones son correctas.
4. En Iniciar una acción de mitigación nueva, el nombre de la tarea viene predeterminado por el ID de auditoría, pero puede cambiarlo por algo más significativo.
5. Para cada tipo de comprobación que tenga uno o varios resultados no conformes en la auditoría, puede elegir una o más acciones para aplicar. Solo se muestran las acciones que son válidas para el tipo de comprobación.

   > **Note**
   >
   > Si no ha configurado las acciones para su Cuenta de AWS, la lista de acciones está vacía. Puede elegir el enlace Crear acción de mitigación para crear una o más acciones de mitigación.

6. Cuando haya especificado todas las acciones que se van a aplicar, seleccione Confirmar.

Para usar la AWS CLI para aplicar acciones de mitigación iniciando la ejecución de una acción de mitigación de auditoría

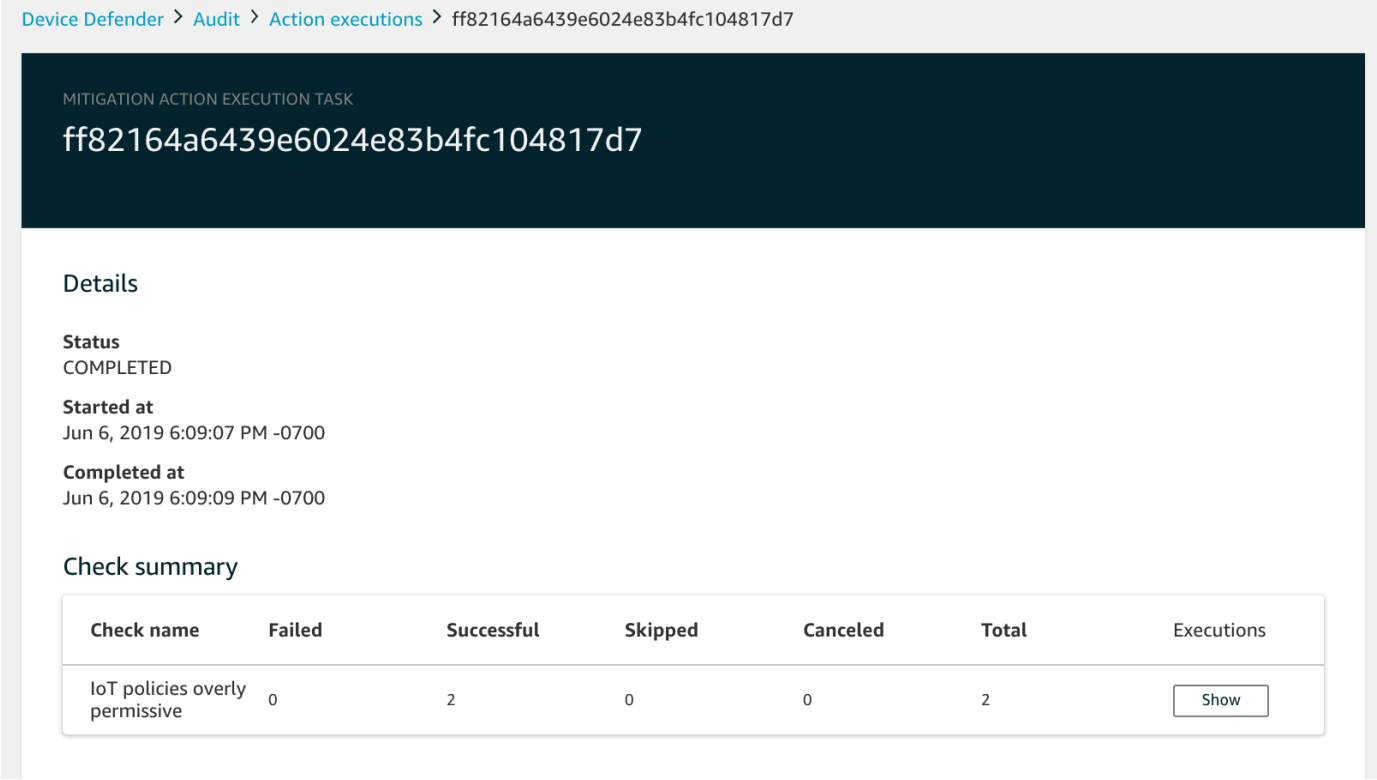
1. Si desea aplicar acciones a todos los resultados de la auditoría, utilice el comando ListAuditTasks para encontrar el ID de la tarea.
2. Si desea aplicar acciones solo a resultados seleccionados, utilice el comando ListAuditFindings para obtener los ID de los resultados.
3. Utilice el comando ListMitigationActions y anote los nombres de las acciones de mitigación que se van a aplicar.
4. Utilice el comando StartAuditMitigationActionsTask para aplicar acciones al destino. Anote el ID de la tarea. Puede utilizar el ID para comprobar el estado de la ejecución de la acción, revisar los detalles o cancelarla.

Para utilizar la consola de AWS IoT para ver sus ejecuciones de acciones

1. Abra la página de tareas de acción en la consola de AWS IoT.

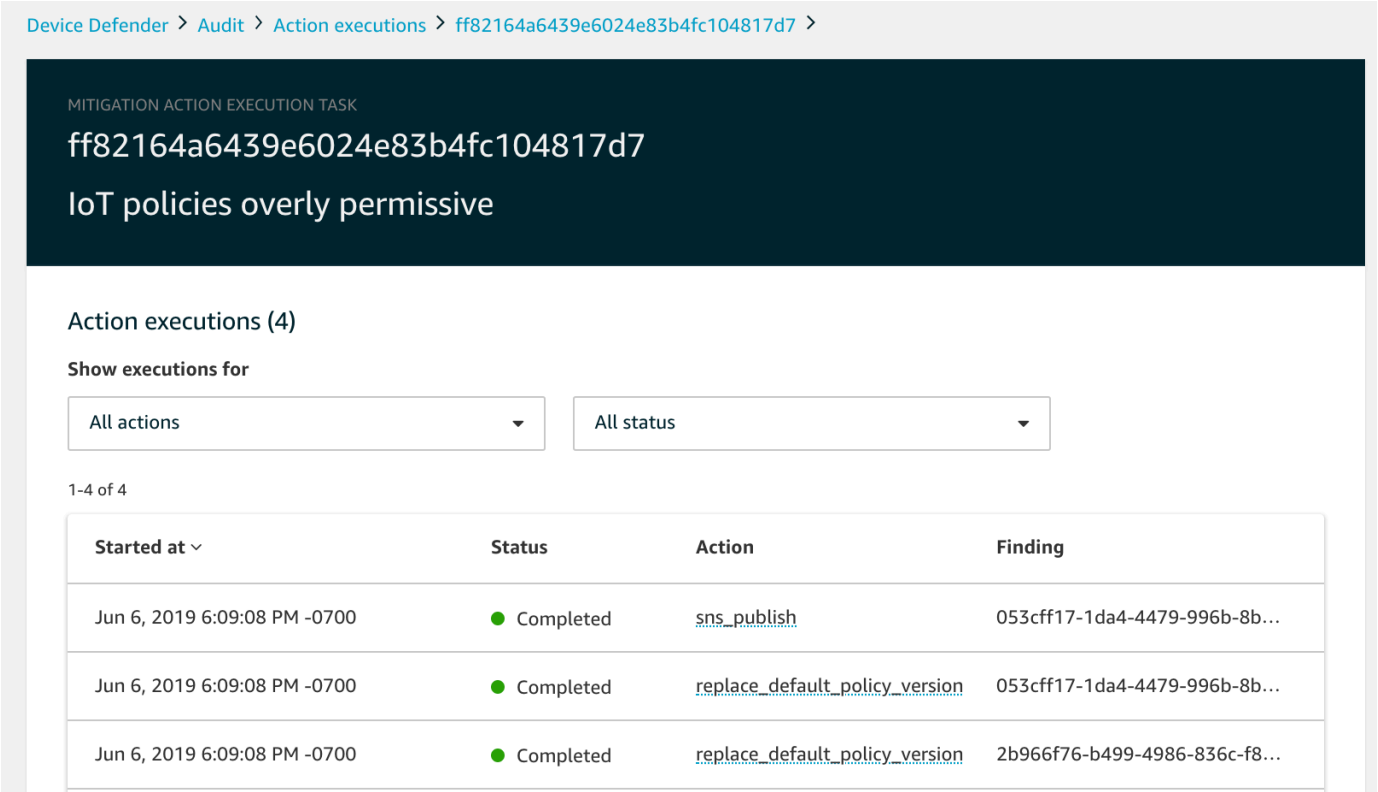
   Una lista de tareas de acción muestra cuando cada se inició cada una y su estado actual.

2. Elija el enlace Name (Nombre) para ver los detalles de la tarea. Los detalles incluyen todas las acciones que aplica la tarea, su destino y su estado.



Puede utilizar los filtros Show executions for (Mostrar ejecuciones para) en tipo de acciones o estados de acción.

3. Para ver los detalles de la tarea, en Executions (Ejecuciones), elija Show (Mostrar).



Para utilizar la AWS CLI para mostrar una lista de tareas iniciadas

1. Utilice ListAuditMitigationActionsTasks para ver tus tareas de acciones de mitigación de auditoría. Puede proporcionar filtros para limitar los resultados. Si desea ver los detalles de la tarea, anote el ID de la tarea.
2. Utilice ListAuditMitigationActionsExecutions para ver los detalles de ejecución de una tarea de acciones de mitigación de auditoría en particular.
3. Use DescribeAuditMitigationActionsTask para ver los detalles de la tarea, como los parámetros especificados cuando se inició la tarea.

Para utilizar la AWS CLI para cancelar una tarea de acciones de mitigación de auditoría en ejecución

1. Utilice el comando ListAuditMitigationActionsTasks para encontrar el ID de la tarea cuya ejecución desea cancelar. Puede proporcionar filtros para limitar los resultados.
2. Utilice el comando ListDetectMitigationActionsExecutions, utilizando el ID de la tarea, para cancelar una tarea de acciones de mitigación. No es posible cancelar tareas que se han completado. Cuando se cancela una tarea, las acciones restantes no se aplican, pero las acciones de mitigación que ya se han aplicado no se revierten.

Permisos

Para cada acción de mitigación que defina, debe proporcionar el rol utilizado para aplicar dicha acción.

Permisos para acciones de mitigación

Tipo de acción	Plantilla de política de permisos
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 de acción	Plantilla de política de permisos	

	``
	"iot:UpdateCACertificate"
	],
	"Resource":[
	"*"
	]
	}
	]
	}
	``	

ADD_THINGS_TO_THING_GROUP	```
	{
	"Version":"2012-10-17",
	"Statement":[
	{
	"Effect":"Allow",
	"Action":[
	"iot:ListPrincipalThings",
	"iot:AddThingToThingGroup"
	],
	"Resource":[
	"*"
	]
	}
	]
	}
	``	

Tipo de acción	Plantilla de política de permisos	
REPLACE_DEFAULT_POLICY_VERSION	`{ "Version":"2012-10-17", "Statement":[ { "Effect": "Allow", "Action":[ "iot:CreatePolicyVersion" ], "Resource": [ "*" ] } ] }`	

Tipo de acción	Plantilla de política de permisos	
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 de acción	Plantilla de política de permisos	
PUBLISH_FINDING_TO_SNS	`{ "Version":"2012-10-17", "Statement":[ { "Effect": "Allow", "Action":[ "sns:Publish" ], "Resource": [ "<The SNS topic to which the finding is published> " ] } ] }`	

Para todos los tipos de acciones de mitigación, utilice la siguiente plantilla de política de confianza:

```
{
  "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:"
        }
      }
    }
  ]
}
```

Comandos de las acciones de mitigación

Puede utilizar estos comandos de acciones de mitigación para definir un conjunto de acciones para su Cuenta de AWS que más tarde se pueden aplicar a uno o más conjuntos de resultados de auditoría. Hay tres categorías de comandos:

- Los que se usan para definir y administrar acciones.
- Los que se usan para iniciar y administrar la aplicación de esas acciones a los resultados de Audit.
- Los que se usan para iniciar y administrar la aplicación de esas acciones a las alarmas de Detect.

Comandos de las acciones de mitigación

Definir y administrar acciones	Iniciar y administrar la ejecución de Audit	Iniciar y administrar la ejecución de Detect
CreateMitigationAction	CancelAuditMitigationActionsTask	CancelDetectMitigationActionsTask
DeleteMitigationAction	DescribeAuditMitigationActionsTask	DescribeDetectMitigationActionsTask
DescribeMitigationAction	ListAuditMitigationActionsTasks	ListDetectMitigationActionsTasks
ListMitigationActions	StartAuditMitigationActionsTask	StartDetectMitigationActionsTask
UpdateMitigationAction	ListAuditMitigationActionsExecutions	ListDetectMitigationActionsExecutions

Uso de AWS IoT Device Defender con otros servicios de AWS.

Uso de AWS IoT Device Defender con dispositivos que ejecutan AWS IoT Greengrass

AWS IoT Greengrass proporciona una integración prediseñada con AWS IoT Device Defender para monitorizar los comportamientos de los dispositivos de forma continua.

- Integración de Device Defender con AWS IoT Greengrass V1
- Integración de Device Defender con AWS IoT Greengrass V2

Uso de AWS IoT Device Defender con FreeRTOS y dispositivos integrados

Para utilizar AWS IoT Device Defender en un dispositivo FreeRTOS, su dispositivo debe tener instalado SDK de FreeRTOS Embedded C o la biblioteca de AWS IoT Device Defender. El SDK de FreeRTOS Embedded C incluye la biblioteca de AWS IoT Device Defender. Para obtener información acerca de cómo integrar AWS IoT Device Defender con sus dispositivos FreeRTOS, consulte las siguientes demostraciones:

- AWS IoT Device Defender para demostraciones de métricas estándar y métricas personalizadas de FreeRTOS
- Utilizar el agente de MQTT para enviar métricas a AWS IoT Device Defender
- Utilizar la biblioteca principal de MQTT para enviar métricas a AWS IoT Device Defender

Para utilizar AWS IoT Device Defender en un dispositivo integrado sin FreeRTOS, su dispositivo debe tener el SDK AWS IoT Embedded C o la biblioteca de AWS IoT Device Defender. El SDK de AWS IoT Embedded C incluye la biblioteca de AWS IoT Device Defender. Para obtener información sobre cómo realizar la integración de AWS IoT Device Defender con sus dispositivos integrados, consulte siguientes demostraciones de métricas estándar y personalizadas del SDK de AWS IoT Device Defender para AWS IoT Embedded.

Uso de AWS IoT Device Defender con AWS IoT Device Management

Puede utilizar la indexación de flotas de AWS IoT Device Management para indexar, buscar y agregar las infracciones de AWS IoT Device Defender Detect. Una vez que los datos sobre infracciones de Device Defender estén indexados en la indexación de flotas, podrá acceder a los datos de infracciones de Device Defender desde las aplicaciones de Fleet Hub y consultarlos, crear alarmas de flota a partir de los datos de infracciones para monitorizar las anomalías en toda su flota de dispositivos y ver las alarmas de la flota en los paneles de Fleet Hub.

> **Note**
>
> La función de indexación de flotas para admitir la indexación de datos sobre infracciones de AWS IoT Device Defender está en versión preliminar para AWS IoT Device Management y está sujeta a cambios.

- Administración de la indexación de flotas
- Sintaxis de la consulta
- Administración de la indexación de flotas para las aplicaciones de Fleet Hub
- Introducción

Integración con AWS Security Hub

AWS Security Hub le proporciona una visión completa de su estado de seguridad en AWS y le ayuda a comprobar su entorno con los estándares y las prácticas recomendadas del sector de la seguridad. Security Hub recopila datos de seguridad de Cuentas de AWS, los servicios y los productos de terceros compatibles. Puede utilizar Security Hub con el fin de analizar sus tendencias de seguridad e identificar los problemas de seguridad más prioritarios.

Con la integración de AWS IoT Device Defender con Security Hub, puede enviar los resultados de AWS IoT Device Defender a Security Hub. Security Hub incluye esos resultados en su análisis de la posición de seguridad.

Contenido

- Habilitación y configuración de la integración

- Cómo AWS IoT Device Defender envía los resultados a Security Hub
  - Tipos de resultados que envía AWS IoT Device Defender
  - Latencia para el envío de resultados
  - Reintento cuando Security Hub no está disponible
  - Actualización de los resultados existentes en Security Hub
- Resultado típico de AWS IoT Device Defender
- Impedir que AWS IoT Device Defender envíe resultados a Security Hub

Habilitación y configuración de la integración

Antes de realizar la integración de AWS IoT Device Defender con Security Hub, debe activar Security Hub. Para obtener información acerca de cómo habilitar Security Hub, consulte la Configuración de Security Hub en la Guía del usuario de AWS Security Hub.

Tras activar tanto AWS IoT Device Defender como Security Hub, abra la página Integraciones en la consola de Security Hub y, a continuación, seleccione Aceptar resultados para Audit, Detect o ambas opciones. AWS IoT Device Defender comienza a enviar los resultados a Security Hub.

Cómo AWS IoT Device Defender envía los resultados a Security Hub

En Security Hub, los problemas de seguridad se rastrean como resultados. Algunos resultados provienen de problemas detectados por otros servicios de AWS o productos de terceros.

Security Hub proporciona herramientas para administrar los resultados de todas estas fuentes. Puede ver y filtrar listas de resultados y ver los detalles de una búsqueda. Para obtener más información, consulte Visualización de resultados en la Guía del usuario de AWS Security Hub. También puede realizar un seguimiento del estado de una investigación de un resultado. Para obtener más información, consulte Adopción de medidas en función de los resultados en la Guía del usuario de AWS Security Hub.

Todos los resultados en Security Hub usan un formato JSON estándar denominado AWS Security Finding Format (ASFF). El ASFF incluye detalles sobre el origen del problema, los recursos afectados y el estado actual del resultado. Para obtener más información acerca de ASFF, consulte AWS Security Finding Format (ASFF) en la Guía del usuario de AWS Security Hub.

AWS IoT Device Defender es uno de los servicios de AWS que envía los resultados a Security Hub.

Tipos de resultados que envía AWS IoT Device Defender

Tras habilitar la integración del Security Hub, AWS IoT Device Defender Audit envía las conclusiones que genera (denominadas resúmenes de comprobación) a Security Hub. Los resúmenes de comprobación son información general para un tipo de comprobación de auditoría y una tarea de auditoría específicas. Para obtener más información, consulte Comprobaciones de auditoría.

AWS IoT Device Defender Audit envía las actualizaciones de búsqueda a Security Hub tanto para los resúmenes de comprobación de auditoría como para las conclusiones de las auditorías de cada tarea de auditoría. Si todos los recursos que se encuentran en las comprobaciones de auditoría son conformes o se cancela una tarea de auditoría, Audit actualiza los resúmenes de comprobación de Security Hub a un estado de registro ARCHIVED. Si un recurso se notificó como no conforme en una comprobación de auditoría, pero se notificó que era conforme en la última tarea de auditoría, Audit lo cambia a conforme y también actualiza el resultado en Security Hub a un estado de registro ARCHIVED.

AWS IoT Device Defender Detect envía los resultados de infracciones a Security Hub. Estos resultados de infracciones incluyen el machine learning (ML) y los comportamientos estadísticos y estáticos.

Para enviar los resultados a Security Hub, AWS IoT Device Defender utiliza AWS Security Finding Format (ASFF). En ASFF, el campo `Types` proporciona el tipo de resultado. Los resultados de AWS IoT Device Defender pueden tener los siguientes valores para `Types`.

Comportamientos inusuales

El tipo de resultado para los ID de cliente de MQTT y las comprobaciones compartidas de certificados de dispositivo contradictorios, y el tipo de resultado para Detect.

Comprobaciones de software y configuración/Vulnerabilidades

El tipo de resultado para todas las demás comprobaciones de auditoría.

Latencia para el envío de resultados

Cuando AWS IoT Device Defender Audit crea un nuevo resultado, se envía inmediatamente a Security Hub una vez finalizada la tarea de auditoría. La latencia depende del volumen de los resultados generados en la tarea de auditoría. Por lo general, Security Hub recibe los resultados en una hora.

AWS IoT Device Defender Detect envía los resultados de infracciones casi en tiempo real. Cuando una infracción entra o sale de alarma (lo que significa que la alarma se crea o se elimina), el resultado correspondiente de Security Hub se crea o archiva inmediatamente.

Reintento cuando Security Hub no está disponible

Si Security Hub no está disponible, Audit AWS IoT Device Defender y Detect AWS IoT Device Defender vuelven a intentar enviar los resultados hasta que los reciben.

Actualización de los resultados existentes en Security Hub

Después de enviar un resultado de AWS IoT Device Defender Audit a Security Hub, puede identificarlo comprobando el identificador del recurso y el tipo de comprobación de auditoría. Si se genera un nuevo resultado de auditoría con una tarea de auditoría posterior para el mismo recurso y verificación de AWS IoT Device Defender Audit, Audit envía actualizaciones para reflejar observaciones adicionales de la actividad de resultados a Security Hub. Si no se genera ningún resultado de auditoría adicional con una tarea de auditoría posterior para el mismo recurso y la misma comprobación de auditoría, el recurso cambia para cumplir la comprobación de auditoría. AWS IoT Device Defender A continuación, Audit archiva los resultados en Security Hub.

AWS IoT Device Defender Audit también actualiza los resúmenes de comprobación en Security Hub. Si se encuentran recursos no conformes en una comprobación de auditoría o la comprobación falla, el estado del resultado de Security Hub pasa a estar activo. En caso contrario, AWS IoT Device Defender Audit archiva el resultado en Security Hub.

AWS IoT Device Defender Detect crea un resultado de Security Hub cuando se produce una infracción (por ejemplo, en caso de alarma). Ese resultado se actualiza solo si se cumple uno de los siguientes criterios:

- El resultado caducará pronto en Security Hub, por lo que AWS IoT Device Defender envía una actualización para mantenerlo actualizado. Los resultados se eliminan al cabo 90 días de la última actualización o 90 días después de que se crearan si no hay actualizaciones. Para obtener más información, consulte Cuotas de Security Hub en la Guía del usuario de AWS Security Hub.
- La infracción correspondiente sale de alarma, por lo que AWS IoT Device Defender actualiza el estado de su resultado a ARCHIVED.

Resultado típico de AWS IoT Device Defender

AWS IoT Device Defender utiliza AWS Security Finding Format (ASFF) para enviar los resultados a Security Hub.

El siguiente ejemplo muestra un resultado típico de Security Hub para un resultado de auditoría. El `ReportType` en `ProductFields` es `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"
    ]
  }
}
```

El siguiente ejemplo muestra un resultado de Security Hub para un resumen de comprobación de auditoría. El `ReportType` en `ProductFields` es `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"
    ]
  }
}
```

El siguiente ejemplo muestra un resultado típico de Security Hub para una infracción de 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"
    ]
  }
}
```

Impedir que AWS IoT Device Defender envíe resultados a Security Hub

Para dejar de enviar resultados a Security Hub, puede utilizar la consola de Security Hub o la API.

Para obtener más información, consulte Desactivar y habilitar el flujo de resultados desde una integración (consola) o Desactivar el flujo de resultados desde una integración (Security Hub API, AWS CLI) en la Guía del usuario de AWS Security Hub.

Prevención de la sustitución confusa entre servicios

El problema de la sustitución confusa es un problema de seguridad en el que una entidad que no tiene permiso para realizar una acción puede obligar a una entidad con más privilegios a realizar la acción. En AWS, la suplantación entre servicios puede dar lugar al problema de la sustitución confusa. La suplantación entre servicios puedes producirse cuando un servicio (el servicio que lleva a cabo las llamadas) llama a otro servicio (el servicio al que se llama). El servicio que lleva a cabo las llamadas se puede manipular para utilizar sus permisos a fin de actuar en función de los recursos de otro cliente a través del servicio al que se llama de una manera en la que no debe tener permiso para acceder. Para evitarlo, AWS proporciona herramientas que le ayudan a proteger sus datos para todos los servicios con entidades principales de servicio a las que se les ha dado acceso a los recursos de su cuenta.

Hay tres recursos de AWS IoT Device Defender a los que puede afectar el problema de seguridad de la sustitución confusa, ejecutar auditorías, enviar notificaciones SNS por infracciones del perfil

de seguridad y ejecutar acciones de mitigación. Para cada una de estas acciones, los valores de `aws:SourceArn` deben ser los siguientes:

- En el caso de los recursos transferidos a la API UpdateAccountAuditConfiguration (atributos RoleArn y notificationTarget RoleArn), debe delimitar la política de recursos utilizando `aws:SourceArn` como `arn:arnPartition:iot:region:accountId:`.
- En el caso de los recursos transferidos a la API CreateMitigationAction (el atributo RoleArn), debe limitar la política de recursos utilizando `aws:SourceArn` como `arn:arnPartition:iot:region:accountId:mitigationaction/mitigationActionName`.
- En el caso de los recursos transferidos a la API CreateSecurityProfile (el atributo alertTargets), debe limitar la política de recursos utilizando `aws:SourceArn` como `arn:arnPartition:iot:region:accountId:securityprofile/securityprofileName`.

La forma más eficaz de protegerse contra el problema de la sustitución confusa es utilizar la clave de contexto de condición global de `aws:SourceArn` con el ARN completo del recurso. Si no conoce el ARN completo del recurso o si especifica varios recursos, utiliza la clave de condición de contexto global `aws:SourceArn` con comodines (`*`) para las partes desconocidas del ARN. Por ejemplo, `arn:aws:servicename:*:123456789012:*`.

El siguiente ejemplo muestra cómo se pueden utilizar las claves contextuales de condición global `aws:SourceArn` y `aws:SourceAccount` en AWS IoT Device Defender para evitar el problema del suplente confundido.

```
 {
"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:"
```

```
      }
    }
  }
}
```

Prácticas recomendadas de seguridad para agentes de dispositivos

Privilegio mínimo

Al proceso del agente se debe otorgar solo los permisos mínimos necesarios para realizar sus tareas.

Mecanismos básicos

- El agente debe ejecutarse como un usuario no raíz.
- El agente se debe ejecutar como un usuario dedicado, en su propio grupo.
- Al usuario/grupo se le deben otorgar permisos de solo lectura sobre los recursos necesarios para recopilar y transmitir métricas.
- Ejemplo: solo lectura en /proc /sys para el agente de muestra.
- Para obtener un ejemplo de cómo configurar un proceso para que se ejecute con permisos reducidos, consulte las instrucciones de configuración que se incluyen con el agente de muestra de Python.

Hay una serie de mecanismos Linux conocidos que pueden ayudarle a restringir o aislar aún más el proceso de su agente:

Mecanismos avanzados

- CGroups
- SELinux
- Chroot
- Espacios de nombres Linux

Resiliencia operativa

Un proceso de agente debe ser resiliente a errores y excepciones operativas inesperados y no debe bloquearse ni salir de forma permanente. El código debe manejar con soltura excepciones

y, como precaución, debe configurarse para reiniciarse automáticamente en caso de terminación inesperada (por ejemplo, debido a reinicios del sistema o excepciones no detectadas).

Dependencias mínimas

Un agente debe usar el menor número posible de dependencias (es decir, bibliotecas de terceros) en su implementación. Si el uso de una biblioteca se justifica debido a la complejidad de una tarea (por ejemplo, Transport Layer Security), use solo dependencias bien mantenidas y establezca un mecanismo para mantenerlas actualizadas. Si las dependencias agregadas contienen funcionalidades que el agente no usa y que están activas de manera predeterminada (por ejemplo, abrir puertos, sockets de dominio), desactívelas en su código o por medio de los archivos de configuración de la biblioteca.

Aislamiento de procesos

Un proceso de agente solo debe contener la funcionalidad requerida para realizar la recopilación y la transmisión de métricas del dispositivo. No debe aprovecharse de otros procesos del sistema como un contenedor ni implementar funcionalidad para otros casos de uso fuera de su ámbito. Además, el proceso del agente debe abstenerse de crear canales de comunicación de entrada como puertos de socket de dominio y de servicio de red que permitirían que procesos locales o remotos interfiriesen en su funcionamiento e influyesen en su integridad y aislamiento.

Sigilo

El nombre de un proceso de agente no debe contener palabras clave como seguridad, monitorización o auditoría que indiquen su finalidad y valor de seguridad. Se debe optar por nombres genéricos de códigos y nombres de procesos aleatorios y únicos en cada dispositivo. Se debe seguir el mismo principio al asignar nombre al directorio en el que residen los binarios del agente y los nombres y valores de los argumentos del proceso.

Información mínima compartida

Ningún artefacto de agente implementado en los dispositivos debe contener información confidencial como credenciales con privilegios, depuración ni código muerto, o comentarios insertados o archivos de documentación que revelen detalles sobre el procesamiento del lado del servidor de métricas recopiladas por el agente u otros detalles sobre sistemas backend.

Transport Layer Security

Para establecer canales seguros de TLS para la transmisión de datos, un agente debe hacer cumplir todas las validaciones del lado del cliente, como la validación de certificados y nombres de dominio en el nivel de la aplicación, si no están habilitadas de manera predeterminada.

Además, un agente debe usar un almacén de certificados raíz que contenga entidades de confianza y no contenga certificados que pertenezcan a emisores de certificados atacados.

Implementación segura

Cualquier mecanismo de implementación del agente, como inserción o sincronización de código y repositorios que contengan sus binarios, código fuente y cualquier archivo de configuración (incluidos certificados raíz de confianza), debe controlarse para evitar la inserción o alteración no autorizada del código. Si el mecanismo de implementación se basa en la comunicación de red, se deben usar métodos criptográficos para proteger la integridad de los artefactos de implementación en tránsito.

Documentación adicional

- Seguridad en AWS IoT Device Defender
- Descripción del modelo de seguridad de AWS IoT
- Redhat: A Bite of Python
- 10 common security gotchas in Python and how to avoid them
- What Is Least Privilege & Why Do You Need It?
- OWASP Embedded Security Top 10
- OWASP IoT Project

Guía para solucionar problemas de AWS IoT Device Defender

Ayúdenos a mejorar este tema

Explíquenos cómo mejorarlo

General

P: ¿Hay algún requisito previo para usar AWS IoT Device Defender?

R: Si desea utilizar métricas registradas por el dispositivo, primero debe implementar un agente en sus dispositivos AWS IoT conectados o en las gateways de dispositivos. Los dispositivos deben proporcionar un identificador de cliente o nombre de objeto coherentes.

Auditoría

P: Permití una comprobación y mi auditoría ha estado mostrando "En curso" durante mucho tiempo. ¿Hay algún problema? ¿Cuándo recibiré los resultados?

R: Cuando se habilita una comprobación, la recopilación de datos comienza inmediatamente. Sin embargo, si la cuenta tiene una gran cantidad de datos por recopilar (certificados, objetos, políticas, etc.), es posible que los resultados de la comprobación tarden algo de tiempo en estar disponibles después de la habilitación.

Detect

P: ¿Cómo puedo conocer los umbrales que se establecen en un comportamiento del perfil de seguridad de AWS IoT Device Defender?

R: Comience por crear un comportamiento del perfil de seguridad con umbrales bajos y asócielo a un grupo de objetos que conste de un conjunto representativo de dispositivos. Puede utilizar AWS IoT Device Defender para ver las métricas actuales y después ajustar el comportamiento de los umbrales para que coincidan con su caso de uso.

P: He creado un comportamiento, pero no activa una vulneración cuando la espero. ¿Cómo debo solucionarlo?

R: Cuando define un comportamiento, especifica la forma en que espera que el dispositivo se comporte con normalidad. Por ejemplo, si tiene una cámara de seguridad que se conecta exclusivamente a un servidor central en el puerto TCP 8888, no espere que se realicen otras conexiones. Para recibir una alerta si la cámara hace una conexión en otro puerto, puede definir un comportamiento como este:

```
{
  "name": "Listening TCP Ports",
  "metric": "aws:listening-tcp-ports",
  "criteria": {
    "comparisonOperator": "in-port-set",
    "value": {
      "ports": [ 8888 ]
    }
  }
}
```

Si la cámara realiza una conexión TCP en el puerto TCP 443, el comportamiento del dispositivo se infringiría y se activaría una alerta.

P: Se están vulnerando uno o más de mis comportamientos. ¿Cómo elimino la vulneración?

R: Las alarmas se desactivan después de que el dispositivo retoma un comportamiento esperado, tal y como se define en los perfiles de comportamiento. Los perfiles de comportamiento se evalúan al recibir los datos de las métricas de su dispositivo. Si el dispositivo no publica ninguna métrica durante más de dos días, el evento de vulneración se establece en `alarm-invalidated` automáticamente.

P: Eliminé un comportamiento que generaba una vulneración; ¿cómo puedo detener las alertas?

R: Al eliminar un comportamiento se detienen todas las vulneraciones y alertas futuras de dicho comportamiento. Las alertas anteriores deben eliminarse del mecanismo de notificación. Cuando se elimina un comportamiento, el registro de vulneraciones de ese comportamiento se conserva durante el mismo período de tiempo que todas las demás vulneraciones en su cuenta.

Métricas de dispositivo

P: Estoy enviando informes de métricas que sé que vulneran mis comportamientos, pero no se activa ninguna vulneración. ¿Por qué?

R: Verifique que sus informes de métricas se estén aceptando suscribiéndose a los siguientes temas de MQTT:

```
$aws/things/THING_NAME/defender/metrics/FORMAT/rejected
$aws/things/THING_NAME/defender/metrics/FORMAT/accepted
```

`THING_NAME` es el nombre del objeto que informa de la métrica y `FORMAT` es “JSON” o “CBOR”, según el formato del informe de métricas que envía el objeto.

Una vez que se haya suscrito, debe recibir mensajes sobre estos temas para cada informe de métrica enviado. Un mensaje `rejected` indica que hubo un problema al analizar el informe de métrica. Se incluye un mensaje de error en la carga del mensaje para ayudarle a corregir cualquier error en su informe de métrica. Un mensaje `accepted` indica que se ha analizado correctamente el informe de métrica.

P: ¿Qué sucede si envío una métrica vacía en mi informe de métrica?

R: Una lista vacía de puertos o direcciones IP se considera siempre que está en conformidad con el comportamiento correspondiente. Si el comportamiento correspondiente supusiera una vulneración, la vulneración se eliminaría.

P: ¿Por qué los informes de métricas de mi dispositivo contienen mensajes para dispositivos que no están en el registro de AWS IoT?

Si tiene uno o varios perfiles de seguridad asociados a todos los objetos o a todos los objetos no registrados, AWS IoT Device Defender incluye métricas de los objetos no registrados. Si desea excluir las métricas de objetos no registrados, puede asociar los perfiles a todos los dispositivos registrados en lugar de a todos los dispositivos.

P: No veo los mensajes de uno o varios dispositivos no registrados a pesar de que puedo aplicar un perfil de seguridad a todos los dispositivos no registrados o a todos los dispositivos. ¿Cómo puedo solucionarlo?

Compruebe que está enviando un informe de métricas con el formato adecuado, en uno de los formatos compatibles. Para obtener más información, consulte Especificación de documentos de métricas de dispositivos. Compruebe que los dispositivos no registrados utilizan un identificador

de cliente o nombre de objeto coherentes. Si el nombre del objeto contiene caracteres de control o tiene más de 128 bytes de caracteres con codificación UTF-8, los mensajes notificados por los dispositivos se rechazarán.

P: ¿Qué sucede si un dispositivo no registrado se añade al registro o si un dispositivo registrado deja de estarlo?

R: Si un dispositivo se añade o se elimina del registro:

- Verá dos vulneraciones independientes para el dispositivo (una en su nombre de objeto registrado y otra en su identidad no registrada) si se siguen publicando métricas para las vulneraciones. Las vulneraciones activas de la identidad antigua dejan de aparecer al cabo de dos días, pero están disponibles en el historial de vulneraciones durante un máximo de 14 días.

P: ¿Qué valor debo proporcionar en el campo de ID del informe de métricas de mi dispositivo?

R: Utilice un valor único para cada informe de métrica, expresado como un número entero positivo. Una práctica común es utilizar una marca de tiempo Epoch de Unix.

P: ¿Debo crear una conexión con MQTT dedicada para las métricas de AWS IoT Device Defender?

R: No se requiere una conexión con MQTT independiente.

P: ¿Qué ID de cliente debería usar al conectarme para publicar métricas de dispositivos?

Para dispositivos (objetos) que estén el registro de AWS IoT registro, utilice el nombre del objeto registrado. Para los productos que no estén en el registro de AWS IoT, utilice un identificador coherente al conectarse a AWS IoT. Esta práctica le permite crear una correspondencia entre las vulneraciones y el nombre de objeto.

P: ¿Puedo publicar métricas para un dispositivo con un ID de cliente diferente?

Es posible publicar métricas en nombre de otro objeto. Para ello, publique las métricas en el tema de AWS IoT Device Defender reservado para dicho dispositivo. Por ejemplo, `Thing-1` desea publicar métricas de sí mismo y también en nombre de `Thing-2`. `Thing-1` recopila sus propias métricas y las publica en el tema de MQTT:

```
$aws/things/Thing-1/defender/metrics/json
```

`Thing-1` obtiene las métricas de `Thing-2` y publica dichas métricas en el tema de MQTT:

```
$aws/things/Thing-2/defender/metrics/json
```

P: ¿Cuántos comportamientos y perfiles de seguridad puedo tener en mi cuenta?

R: Consulte AWS IoT Device Defender Endpoints and Quotas.

P: ¿Qué aspecto tiene un rol de destino prototípico para un destino de alerta?

R: Un rol que permite a AWS IoT Device Defender publicar alertas en un destino de alerta (tema de SNS) requiere dos cosas:

- Una relación de confianza que especifique iot.amazonaws.com como la entidad de confianza y
- Una política asociada que conceda a AWS IoT permiso para publicar en un tema de SNS especificado. Por ejemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": "sns:Publish",
            "Resource": "<sns-topic-arn>"
        }
    ]
}
```

- Si el tema SNS utilizado para publicar las alertas es un tema cifrado, es necesario otorgarle a AWS IoT dos permisos más, además del permiso para publicar un tema SNS. Por ejemplo:

```
{
    "Version": "2012-10-17",
    "Statement": [
       {
           "Effect": "Allow",
           "Action": [
               "sns:Publish",
               "kms:Decrypt",
               "kms:GenerateDataKey"
           ],
           "Resource": "<sns-topic-arn>"
       }
    ]
}
```

P: El envío del informe de métricas con un tipo de métrica `number` personalizado da el mensaje de error `Malformed metrics report`. ¿Por qué?

R: El tipo `number` solo toma un valor único de métrica como entrada, pero, cuando envía el valor de métrica en el informe DeviceMetrics, debe pasarlo como una matriz con un solo valor. Envíe el valor de la métrica como una matriz.

Carga útil del error:

```
{"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}}}
```

Mensaje de error:

```
{"thingName":"myThing","status":"REJECTED","statusDetails":
{"ErrorCode":"InvalidPayload","ErrorMessage":"Malformed metrics
 report"},"timestamp":1635802047699}
```

Carga sin errores:

```
{"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}]}}
```

Respuesta:

```
{"thingName":"myThing","12334567":1635800375,"status":"ACCEPTED","timestamp":1635801636023}
```

Seguridad en AWS IoT Device Defender

En AWS, la seguridad en la nube es la máxima prioridad. Como cliente de AWS, se beneficiará de una arquitectura de red y de centros de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y usted. El modelo de responsabilidad compartida la describe como seguridad de la nube y seguridad en la nube:

- Seguridad de la nube: AWS es responsable de proteger la infraestructura que ejecuta servicios de AWS en la Nube de AWS. AWS también le proporciona servicios que puede utilizar de forma segura. Los auditores externos prueban y verifican periódicamente la eficacia de nuestra seguridad como parte de los Programas de conformidad de AWS . Para obtener información sobre los programas de conformidad que se aplican a AWS IoT Device Defender, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida a la hora de utilizar AWS IoT Device Defender. Los siguientes temas le mostrarán cómo configurar AWS IoT Device Defender para satisfacer sus objetivos de seguridad y de conformidad. También puede aprender a utilizar otros servicios de AWS que lo ayuden a monitorizar y proteger los recursos de AWS IoT Device Defender. Para obtener más información sobre la seguridad en AWS IoT Core, consulte el capítulo de seguridad de la Guía para desarrolladores de AWS IoT Core

Temas

- Protección de datos en AWS IoT Device Defender
- Administración de identidades y accesos en AWS IoT Device Defender
- Validación de conformidad para AWS IoT Device Defender
- Resiliencia en AWS IoT Device Defender

Protección de datos en AWS IoT Device Defender

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos en AWS IoT Device Defender. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta toda la Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog sobre el Modelo de responsabilidad compartida de AWS y GDPR en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se otorgan a cada usuario los permisos necesarios para cumplir sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice la autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. Se recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure los registros de API y de actividad de los usuarios con AWS CloudTrail. Para obtener información sobre cómo utilizar registros de seguimiento de CloudTrail para capturar actividades de AWS, consulte Working with CloudTrail trails en la Guía del usuario de AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los servicios de Servicios de AWS.
- Utilice servicios de seguridad administrados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-3 al acceder a AWS a través de una interfaz de línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-3.

Se recomienda encarecidamente no introducir nunca información confidencial o sensible, como, por ejemplo, direcciones de correo electrónico de clientes, en etiquetas o campos de formato libre, tales como el campo Nombre. Esto incluye los casos en los que debe trabajar con AWS IoT Device

Defender u otros Servicios de AWS a través de la consola, la API, la AWS CLI o los SDK de AWS. Cualquier dato que ingrese en etiquetas o campos de formato libre utilizados para nombres se puede emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Administración de identidades y accesos en AWS IoT Device Defender

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los gestionadores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién está autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar los recursos de AWS IoT Device Defender. IAM es un servicio de Servicio de AWS que se puedes utilizar sin cargo adicional.

Temas

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo AWS IoT Device Defender funciona con IAM
- Ejemplos de políticas basadas en identidades de AWS IoT Device Defender
- Solución de problemas de identidades de AWS IoT Device Defender y accesos

Público

La forma en que utilice AWS Identity and Access Management (IAM) difiere en función del trabajo que realice en AWS IoT Device Defender.

Usuario de servicio: si utiliza el servicio de AWS IoT Device Defender para realizar su trabajo, su administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de AWS IoT Device Defender para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarlo a solicitar los permisos correctos al gestionador. Si no puede acceder a una característica en AWS IoT Device Defender, consulte Solución de problemas de identidades de AWS IoT Device Defender y accesos.

Administrador de servicio: si está a cargo de los recursos de AWS IoT Device Defender en su empresa, es probable que tenga acceso completo a AWS IoT Device Defender. Su trabajo consiste en determinar a qué características y recursos de AWS IoT Device Defender deben acceder los usuarios del servicio. Luego, debe enviar solicitudes a su gestionador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con AWS IoT Device Defender, consulte Cómo AWS IoT Device Defender funciona con IAM.

Administrador de IAM: si es un administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a AWS IoT Device Defender. Para consultar ejemplos de políticas basadas en la identidad de AWS IoT Device Defender que puede utilizar en IAM, consulte Ejemplos de políticas basadas en identidades de AWS IoT Device Defender.

Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puedes iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (del Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su gestionador habrá configurado previamente la federación de identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puedes iniciar sesión en AWS Management Console o en el portal de acceso AWS. Para obtener más información sobre el inicio de sesión en AWS, consulta Cómo iniciar sesión en su Cuenta de AWS en la Guía del usuario de AWS Sign-In.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no usa las herramientas de AWS, debe firmar las solicitudes. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes por su cuenta, consulte AWS Signature Version 4 para solicitudes de API en la Guía del usuario de IAM.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación

multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la AWS IAM Identity CenterGuía del usuario y AWS Autenticación multifactor en IAM en la Guía del usuario de IAM.

Usuario raíz de Cuenta de AWS

Cuando se crea una Cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los recursos y Servicios de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con el email y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utiliza el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulta Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

Identidad federada

Como práctica recomendada, solicite que los usuarios humanos, incluidos los que requieren acceso de gestionador, utilicen la federación con un proveedor de identidades para acceder a los Servicios de AWS utilizando credenciales temporales.

Una identidad federada es un usuario del directorio de usuarios de su empresa, un proveedor de identidades web, el AWS Directory Service, el directorio del Identity Center, o cualquier usuario que acceda a Servicios de AWS utilizando credenciales proporcionadas a través de una fuente de identidad. Cuando identidades federadas acceden a Cuentas de AWS, asumen roles y los roles proporcionan credenciales temporales.

Para una administración de acceso centralizada, le recomendamos que utiliza AWS IAM Identity Center. Puedes crear usuarios y grupos en el IAM Identity Center o puedes conectarse y sincronizar con un conjunto de usuarios y grupos de su propia fuente de identidad para usarlos en todas sus aplicaciones y Cuentas de AWS. Para obtener más información, consulta ¿Qué es el Centro de identidades de IAM? en la Guía del usuario de AWS IAM Identity Center.

Usuarios y grupos de IAM

Un usuario de IAM es una identidad de la Cuenta de AWSque dispone de permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran

credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulta Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No puedes iniciar sesión como grupo. Puedes usar los grupos para especificar permisos para varios usuarios a la vez. Los grupos facilitan la administración de los permisos de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales de larga duración permanentes; no obstante, los roles proporcionan credenciales temporales. Para obtener más información, consulte Casos de uso para usuarios de IAM en la Guía del usuario de IAM.

Roles de IAM

Un rol de IAM es una identidad de la Cuenta de AWSque dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Para asumir temporalmente un rol de IAM en la AWS Management Console, puede cambiar de un rol de usuario a un rol de IAM (consola). Puedes asumir un rol llamando a una operación de la AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulta Métodos para asumir un rol en la Guía del usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puedes crear un rol y definir sus permisos. Cuando se autentica una identidad federada, se asocia la identidad al rol y se le conceden los permisos define el rol. Para obtener información acerca de roles para federación, consulte Crear un rol para un proveedor de identidades de terceros (federación) en la Guía del usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué puedes acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center.
- Permisos de usuario de IAM temporales: un usuario de IAM puedes asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.

- Acceso entre cuentas: puedes utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puedes adjuntar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para obtener información acerca de la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Acceso a recursos entre cuentas en IAM en la Guía del usuario de IAM.
- Acceso entre servicios: algunos Servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a servicios.
  - Reenviar sesiones de acceso (FAS): cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un gestionador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Rol vinculado a los servicios: un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un gestionador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puedes utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia de EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia adjuntado a

la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia de EC2 obtener credenciales temporales. Para más información, consulte Usar un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias Amazon EC2 en la Guía del usuario de IAM.

Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulta Información general de políticas JSON en la Guía del usuario de IAM.

Los gestionadores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Un gestionador de IAM puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el gestionador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utiliza para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puedes obtener información del usuario de la AWS Management Console, la AWS CLI o la API de AWS.

Políticas basadas en identidades

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puedes asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones puedes realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener información sobre cómo crear una política basada en identidades, consulte Definición de permisos de IAM personalizados con políticas gestionadas por el cliente en la Guía del usuario de IAM.

Las políticas basadas en identidades pueden clasificarse además como políticas insertadas o políticas gestionadas. Las políticas insertadas se integran directamente en un único usuario, grupo

o rol. Las políticas gestionadas son políticas independientes que puede adjuntar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas gestionadas incluyen las políticas gestionadas de AWS y las políticas gestionadas por el cliente. Para obtener información sobre cómo elegir entre una política gestionada o una política insertada, consulte Elección entre políticas gestionadas y políticas insertadas en la Guía del usuario de IAM.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los gestionadores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Las entidades principales puedes incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Las políticas basadas en recursos son políticas insertadas que se encuentran en ese servicio. No se puede utilizar políticas de IAM gestionadas de AWS en una política basada en recursos.

Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulta Información general de Lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas puedes establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política basada en identidad puedes conceder a una entidad de IAM (usuario o rol de IAM). Puedes establecer un límite de permisos para una entidad. Los permisos resultantes son la intersección de las políticas basadas en la identidad de la entidad

y los límites de permisos. Las políticas basadas en recursos que especifiquen el usuario o rol en el campo `Principal` no estarán restringidas por el límite de permisos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para obtener más información sobre los límites de los permisos, consulta Límites de permisos para las entidades de IAM en la Guía del usuario de IAM.

- Políticas de control de servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias Cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada Usuario raíz de la cuenta de AWS. Para obtener más información acerca de SCP y Organizations, consulta Políticas de control de servicios en la Guía del usuario de AWS Organizations.
- Políticas de control de recursos (RCP): las RCP son políticas JSON que permiten establecer los permisos máximos disponibles para los recursos de las cuentas sin actualizar las políticas de IAM asociadas a cada recurso que posea. La RCP limita los permisos de los recursos en las cuentas de miembros y puede afectar a los permisos efectivos de las identidades, incluidos los Usuario raíz de la cuenta de AWS, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations y RCP, incluida una lista de los Servicios de AWS que admiten RCP, consulte Políticas de control de recursos (RCP) en la Guía del usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidades del rol y las políticas de la sesión. Los permisos también puedes proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulta Políticas de sesión en la Guía del usuario de IAM.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información acerca de cómo AWS decide si permitir o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

Cómo AWS IoT Device Defender funciona con IAM

Antes de utilizar IAM para administrar el acceso a AWS IoT Device Defender, descubra qué características de IAM se pueden utilizar con AWS IoT Device Defender.

Características de IAM que puede utilizar con AWS IoT Device Defender

Característica de IAM	Compatibilidad con AWS IoT Device Defender
Políticas basadas en identidad	Sí
Políticas basadas en recursos	No
Acciones de políticas	Sí
Recursos de políticas	Sí
Claves de condición de política	Sí
ACL	No
ABAC (etiquetas en políticas)	Parcial
Credenciales temporales	Sí
Permisos de entidades principales	Sí
Roles de servicio	Sí
Roles vinculados al servicio	No

Para obtener una perspectiva general sobre cómo funcionan AWS IoT Device Defender y otros servicios de AWS con las características de IAM, consulte Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Políticas de AWS IoT Device Defender basadas en identidades

Compatibilidad con las políticas basadas en identidad: sí

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puedes asociar a una identidad, como un usuario de IAM, un grupo de usuarios o un rol. Estas políticas controlan qué acciones puedes realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información acerca de cómo crear una política basada en identidad, consulte Definición de permisos de IAM personalizados con políticas gestionadas por el cliente en la Guía del usuario de IAM.

Con las políticas basadas en identidades de IAM, puedes especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. No es posible especificar la entidad principal en una política basada en identidad porque se aplica al usuario o rol al que está adjunto. Para más información sobre los elementos que puedes utilizar en una política de JSON, consulta Referencia de los elementos de las políticas de JSON de IAM en la Guía del usuario de IAM.

Ejemplos de políticas basadas en identidades de AWS IoT Device Defender

Para ver ejemplos de políticas basadas en identidad de AWS IoT Device Defender, consulte Ejemplos de políticas basadas en identidades de AWS IoT Device Defender.

Políticas basadas en recursos de AWS IoT Device Defender

Admite políticas basadas en recursos: no

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los gestionadores de servicios pueden utilizarlos para controlar el acceso a un recurso específico. Para el recurso al que se asocia la política, la política define qué acciones puedes realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Las entidades principales puedes incluir cuentas, usuarios, roles, usuarios federados o Servicios de AWS.

Para habilitar el acceso entre cuentas, puedes especificar toda una cuenta o entidades de IAM de otra cuenta como la entidad principal de una política en función de recursos. Añadir a una política en función de recursos una entidad principal entre cuentas es solo una parte del establecimiento de una relación de confianza. Cuando la entidad principal y el recurso se encuentran en Cuentas de AWS diferentes, un gestionador de IAM de la cuenta de confianza también debe conceder a la entidad principal (usuario o rol) permiso para acceder al recurso. Para conceder el permiso, adjunte la entidad a una política basada en identidad. Sin embargo, si la política en función de recursos

concede el acceso a una entidad principal de la misma cuenta, no es necesaria una política basada en identidad adicional. Para más información, consulta Cross account resource access in IAM en la Guía del usuario de IAM.

Acciones de política para AWS IoT Device Defender

Compatibilidad con las acciones de política: sí

Los gestionadores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puedes utilizar para conceder o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

Para ver una lista de las acciones de AWS IoT Device Defender, consulte la Referencia de autorizaciones de servicio.

Las acciones de políticas de AWS IoT Device Defender utilizan el siguiente prefijo antes de la acción:

Para especificar varias acciones en una única instrucción, sepárelas con comas.

```
"Action": [
      ":action1",
      ":action2"
         ]
```

Para ver ejemplos de políticas basadas en identidad de AWS IoT Device Defender, consulte Ejemplos de políticas basadas en identidades de AWS IoT Device Defender.

Recursos de políticas para AWS IoT Device Defender

Compatibilidad con los recursos de políticas: sí

Los gestionadores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puedes hacerlo para acciones que admitan un tipo de recurso específico, conocido como permisos de nivel de recurso.

Para las acciones que no admiten permisos de nivel de recurso, como las operaciones de descripción, utiliza un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para ver una lista de tipos de recursos de AWS IoT Device Defender y sus ARN, consulte la Referencia de autorizaciones de servicio. Para obtener información acerca de con qué acciones puede especificar los ARN de cada recurso, consulte .

Para ver ejemplos de políticas basadas en identidad de AWS IoT Device Defender, consulte Ejemplos de políticas basadas en identidades de AWS IoT Device Defender.

Claves de condición de políticas para AWS IoT Device Defender

Compatibilidad con claves de condición de políticas específicas del servicio: sí

Los gestionadores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El elemento `Condition` (o bloque de `Condition`) permite especificar condiciones en las que entra en vigor una instrucción. El elemento `Condition` es opcional. Puedes crear expresiones condicionales que utilizan operadores de condición, tales como igual o menor que, para que la condición de la política coincida con los valores de la solicitud.

Si especifica varios elementos de `Condition` en una instrucción o varias claves en un único elemento de `Condition`, AWS las evalúa mediante una operación `AND` lógica. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación lógica `OR`. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puedes utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puedes conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulta Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulta Claves de contexto de condición globales de AWSen la Guía del usuario de IAM.

Para ver una lista de claves de condición de AWS IoT Device Defender, consulte la Referencia de autorizaciones de servicio. Para obtener más información acerca de las acciones y los recursos con los que puede utilizar una clave de condición, consulte .

Para ver ejemplos de políticas basadas en identidad de AWS IoT Device Defender, consulte Ejemplos de políticas basadas en identidades de AWS IoT Device Defender.

ACL en AWS IoT Device Defender

Compatibilidad con ACL: no

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de políticas JSON.

ABAC con AWS IoT Device Defender

Compatibilidad con ABAC (etiquetas en las políticas): parcial

El control de acceso basado en atributos (ABAC) es una estrategia de autorización que define permisos en función de atributos. En AWS, estos atributos se denominan etiquetas. Puedes adjuntar etiquetas a entidades de IAM (usuarios o roles) y a muchos recursos de AWS. El etiquetado de entidades y recursos es el primer paso de ABAC. A continuación, designa las políticas de ABAC para permitir operaciones cuando la etiqueta de la entidad principal coincida con la etiqueta del recurso al que se intenta acceder.

ABAC es útil en entornos que crecen con rapidez y ayuda en situaciones en las que la administración de las políticas resulta engorrosa.

Para controlar el acceso en función de etiquetas, debe proporcionar información de las etiquetas en el elemento de condición de una política utilizando las claves de condición `aws:ResourceTag/key-name`, `aws:RequestTag/key-name` o `aws:TagKeys`.

Si un servicio admite las tres claves de condición para cada tipo de recurso, el valor es Sí para el servicio. Si un servicio admite las tres claves de condición solo para algunos tipos de recursos, el valor es Parcial.

Para obtener más información sobre ABAC, consulte Definir permisos con la autorización de ABAC en la Guía del usuario de IAM. Para ver un tutorial con los pasos para configurar ABAC, consulta Uso del control de acceso basado en atributos (ABAC) en la Guía del usuario de IAM.

Uso de credenciales temporales con AWS IoT Device Defender

Compatibilidad con credenciales temporales: sí

Algunos Servicios de AWS no funcionan cuando inicia sesión con credenciales temporales. Para obtener información adicional, incluida la información sobre qué Servicios de AWS funcionan con credenciales temporales, consulta Servicios de AWS que funcionan con IAM en la Guía del usuario de IAM.

Utiliza credenciales temporales si inicia sesión en la AWS Management Console con cualquier método, excepto un nombre de usuario y una contraseña. Por ejemplo, cuando accede a AWS utilizando el enlace de inicio de sesión único (SSO) de la empresa, ese proceso crea automáticamente credenciales temporales. También crea automáticamente credenciales temporales cuando inicia sesión en la consola como usuario y luego cambia de rol. Para más información sobre el cambio de roles, consulte Cambiar de usuario a un rol de IAM (consola) en la Guía del usuario de IAM.

Puede crear credenciales temporales de forma manual mediante la AWS CLI o la API de AWS. A continuación, puedes usar esas credenciales temporales para acceder a AWS. AWS recomienda generar credenciales temporales de forma dinámica en lugar de usar claves de acceso a largo plazo. Para más información, consulta Credenciales de seguridad temporales en IAM.

Permisos de entidades principales entre servicios de AWS IoT Device Defender

Admite sesiones de acceso directo (FAS): sí

Cuando utiliza un usuario o un rol de IAM para llevar a cabo acciones en AWS, se lo considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe

una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulta Reenviar sesiones de acceso.

Roles de servicio para AWS IoT Device Defender

Compatibilidad con roles de servicio: sí

Un rol de servicio es un rol de IAM que asume un servicio para realizar acciones en su nombre. Un gestionador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.

> **Warning**
>
> Cambiar los permisos de un rol de servicio podría interrumpir la funcionalidad de AWS IoT Device Defender. Edite los roles de servicio sólo cuando AWS IoT Device Defender proporcione orientación para hacerlo.

Roles vinculados a servicios de AWS IoT Device Defender

Compatibilidad con roles vinculados al servicio: no

Un rol vinculado al servicio es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puedes asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en la Cuenta de AWS y son propiedad del servicio. Un gestionador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

Para más información sobre cómo crear o administrar roles vinculados a servicios, consulta Servicios de AWS que funcionan con IAM. Busque un servicio en la tabla que incluya `Yes` en la columna Rol vinculado a un servicio. Seleccione el vínculo Sí para ver la documentación acerca del rol vinculado a servicios para ese servicio.

Ejemplos de políticas basadas en identidades de AWS IoT Device Defender

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar los recursos de AWS IoT Device Defender. Tampoco puedes realizar tareas mediante la AWS Management Console, la AWS Command Line Interface (AWS CLI) o la API de AWS. Un gestionador de IAM

puede crear políticas de IAM para conceder permisos a los usuarios para realizar acciones en los recursos que necesitan. A continuación, el gestionador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Para obtener información acerca de cómo crear una política basada en identidades de IAM mediante el uso de estos documentos de políticas JSON de ejemplo, consulte Creación de políticas de IAM (consola) en la Guía del usuario de IAM.

A fin de obtener más información sobre las acciones y los tipos de recursos definidos por AWS IoT Device Defender, incluido el formato de los ARN para cada tipo de recurso, consulte Acciones, recursos y claves de condición para AWS IoT Device Defender en la Referencia de autorizaciones de servicio.

Temas

- Prácticas recomendadas sobre las políticas
- Mediante la consola de AWS IoT Device Defender
- Cómo permitir a los usuarios consultar sus propios permisos

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear o eliminar los recursos de AWS IoT Device Defender en la cuenta o acceder a estos. Estas acciones pueden generar costos adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas gestionadas por AWSy continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas gestionadas por AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas gestionadas por el cliente de AWS específicas para sus casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas gestionadas por AWS o las políticas gestionadas por AWS para funciones de trabajo en la Guía de usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se puedes llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulta Políticas y permisos en IAM en la Guía del usuario de IAM.

- Utiliza condiciones en las políticas de IAM para restringir aún más el acceso: puedes agregar una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puedes escribir una condición de políticas para especificar que todas las solicitudes deben enviarse utilizando SSL. También puedes usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado como, por ejemplo, AWS CloudFormation. Para obtener más información, consulta Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utiliza el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulta Validación de políticas mediante el Analizador de acceso de IAM en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus políticas. Para más información, consulte Acceso seguro a la API con MFA en la Guía de usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulta las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

Mediante la consola de AWS IoT Device Defender

Para acceder a la consola de AWS IoT Device Defender, debe tener un conjunto mínimo de permisos. Estos permisos deben permitirle registrar y consultar los detalles acerca de los recursos de AWS IoT Device Defender en su Cuenta de AWS. Si crea una política basada en identidades que sea más restrictiva que el mínimo de permisos necesarios, la consola no funcionará del modo esperado para las entidades (usuarios o roles) que tengan esa política.

No es necesario que conceda permisos mínimos para la consola a los usuarios que solo realizan llamadas a la AWS CLI o a la API de AWS. En su lugar, permite acceso únicamente a las acciones que coincidan con la operación de API que intentan realizar.

Para asegurarse de que los usuarios y los roles puedan seguir utilizando la consola de AWS IoT Device Defender, asocie también a las entidades la política administrada por AWS IoT Device

Defender `ConsoleAccess` o `ReadOnly` AWS. Para más información, consulte Adición de permisos a un usuario en la Guía del usuario de IAM:

Cómo permitir a los usuarios consultar sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas gestionadas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para llevar a cabo esta acción en la consola o mediante programación con la AWS CLI o la API de 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": "*"
        }
    ]
}
```

Solución de problemas de identidades de AWS IoT Device Defender y accesos

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con IAM y AWS IoT Device Defender.

Temas

- No tengo autorización para realizar una acción en AWS IoT Device Defender
- No tengo autorización para realizar la operación iam:PassRole
- Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de AWS

No tengo autorización para realizar una acción en AWS IoT Device Defender

Si recibe un error que indica que no tiene autorización para realizar una acción, las políticas se deben actualizar para permitirle realizar la acción.

En el siguiente ejemplo, el error se produce cuando el usuario de IAM `mateojackson` intenta utilizar la consola para consultar los detalles acerca de un recurso ficticio *`my-example-widget`*, pero no tiene los permisos ficticios `:`*`GetWidget`*.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: :GetWidget on resource: my-example-widget
```

En este caso, la política del usuario `mateojackson` debe actualizarse para permitir el acceso al recurso *`my-example-widget`* mediante la acción `:`*`GetWidget`*.

Si necesita ayuda, póngase en contacto con su gestionador de AWS. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

No tengo autorización para realizar la operación iam:PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas para permitirle pasar un rol a AWS IoT Device Defender.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado al servicio. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en AWS IoT Device Defender. Sin embargo, la acción requiere que el servicio cuente con permisos que otorguen un rol de servicio. Mary no tiene permisos para transferir el rol al servicio.

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

En este caso, las políticas de Mary se deben actualizar para permitirle realizar la acción `iam:PassRole`.

Si necesita ayuda, póngase en contacto con su gestionador de AWS. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir a personas externas a mi Cuenta de AWS el acceso a mis recursos de AWS

Puedes crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puedes especificar una persona de confianza para que asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puedes utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para más información, consulta lo siguiente:

- Para obtener información acerca de si AWS IoT Device Defender admite estas características, consulte Cómo AWS IoT Device Defender funciona con IAM.
- Para obtener información acerca de cómo proporcionar acceso a los recursos de las Cuenta de AWS de su propiedad, consulta Proporcionar acceso a un usuario de IAM a otra Cuentas de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información acerca de cómo proporcionar acceso a tus recursos a Cuentas de AWS de terceros, consulta Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante una federación de identidades, consulta Proporcionar acceso a usuarios autenticados externamente (identidad federada) en la Guía del usuario de IAM.
- Para conocer sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulta Cross account resource access in IAM en la Guía del usuario de IAM.

Validación de conformidad para AWS IoT Device Defender

Para saber si un Servicio de AWS está incluido en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad y elija el programa de conformidad que le interese. Para obtener información general, consulta Programas de conformidad de AWS.

Puedes descargar los informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulta Descarga de informes en AWS Artifact.

Su responsabilidad de conformidad al utilizar Servicios de AWS se determina en función de la sensibilidad de los datos, los objetivos de cumplimiento de su empresa y la legislación y los reglamentos correspondientes. AWS proporciona los siguientes recursos para ayudar con la conformidad:

- Cumplimiento de seguridad y gobernanza: en estas guías se explican las consideraciones de arquitectura y se proporcionan pasos para implementar las características de seguridad y cumplimiento.
- Referencia de servicios válidos de HIPAA: muestra una lista con los servicios válidos de HIPAA. No todos los Servicios de AWS son aptos para HIPAA.
- Recursos de conformidad de AWS: este conjunto de manuales y guías podría aplicarse a su sector y ubicación.
- Guías de cumplimiento para clientes de AWS: comprenda el modelo de responsabilidad compartida desde el punto de vista del cumplimiento. Las guías resumen las mejores prácticas para garantizar la seguridad de los Servicios de AWS y orientan los controles de seguridad en varios marcos (incluidos el Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés), el Consejo de Estándares de Seguridad de la Industria de Tarjetas de Pago (PCI, por sus siglas en inglés) y la Organización Internacional de Normalización (ISO, por sus siglas en inglés)).
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este Servicio de AWS proporciona una visión completa de su estado de seguridad en AWS. Security Hub utiliza controles de seguridad para evaluar sus recursos de AWS y comprobar su cumplimiento con los estándares y las prácticas recomendadas del sector de la seguridad. Para obtener una lista de los servicios y controles compatibles, consulta la Referencia de controles de Security Hub.

- Amazon GuardDuty: este Servicio de AWS detecta posibles amenazas para sus Cuentas de AWS, cargas de tarea, contenedores y datos mediante la supervisión de su entorno para detectar actividades sospechosas y maliciosas. GuardDuty puedes ayudarlo a satisfacer varios requisitos de conformidad, como PCI DSS, cumpliendo los requisitos de detección de intrusos que exigen determinados marcos de conformidad.
- AWS Audit Manager: este Servicio de AWS le ayuda a auditar continuamente el uso de AWS con el fin de simplificar la forma en que administra el riesgo y la conformidad con las normativas y los estándares del sector.

Resiliencia en AWS IoT Device Defender

La infraestructura global de AWS se divide en Regiones de AWS y zonas de disponibilidad. Las Regiones de AWS proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que conmutan automáticamente entre zonas sin interrupción. Las zonas de disponibilidad tienen una mayor disponibilidad, tolerancia a errores y escalabilidad que las infraestructuras tradicionales de uno o varios centros de datos.

Para obtener más información sobre las Regiones de AWS y las zonas de disponibilidad, consulte la Infraestructura global de AWS.

Además de la infraestructura global de AWS, AWS IoT Device Defender ofrece varias características para ayudarle con sus necesidades de resiliencia y copia de seguridad de los datos.

Historial de documentos para la guía del usuario de AWS IoT Device Defender

En la siguiente tabla se describen las versiones de la documentación de la AWS IoT Device Defender.

Cambio	Descripción	Fecha
Disponibilidad general	Esta es la versión pública inicial de AWS IoT Device Defender.	2 de agosto de 2023
Ahora, AWS IoT Device Defender permite supervisar la duración de la desconexión de los dispositivos	AWS IoT Device Defender Rules Detect incluye ahora una nueva métrica de duración de desconexión con el fin de supervisar la duración de la desconexión de cada dispositivo. Con esta métrica adicional, puede hacer un seguimiento del tiempo que ha estado desconectado un dispositivo, y saber así si funciona según lo esperado. También puede configurar las alarmas en niveles de umbral predefinidos y recibir alertas en caso de problemas persistentes de conectividad del dispositivo. Para obtener documentación relacionada, consulte Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender.	20 de julio de 2023

La característica AWS IoT Device Defender Audit identifica posibles errores de configuración en las políticas de IoT	Identifique los defectos, solucione los problemas y tome las medidas correctivas necesarias mediante la característica Audit Esta nueva característica también le ayuda a identificar las políticas de IoT con declaraciones de permiso poco restrictivas, lo que podría generar que los dispositivos obtuviesen acceso a recursos imprevistos. También comprueba el uso de comodines MQTT en las declaraciones de denegación, algo que los dispositivos podrían eludir al sustituir los comodines por cadenas específicas. Para obtener más información, consulte Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender	6 de diciembre de 2022

Compatibilidad con dimensiones y métricas personalizadas en AWS IoT Device Defender ML Detect	AWS IoT Device Defender admite ahora una nueva comprobación de auditoría para la entidad de certificación (CA) intermedia revocada. Si una CA revoca una CA intermedia porque podría estar comprometida, todos los certificados emitidos por esa CA intermedia también podrían estar comprometidos y no serán válidos. Esta nueva comprobación de auditoría identifica los certificados de dispositivos activos emitidos por una CA intermedia revocada, y ayuda a los clientes a revisar y reemplazar esos certificados de dispositivos activos. Para obtener más información, consulte Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender	10 de noviembre de 2022

Compatibilidad con dimensiones y métricas personalizadas en AWS IoT Device Defender ML Detect	ML Detect permite ahora la supervisión de métricas personalizadas, de modo que pueda evaluar los parámetros de estado operativo que sean exclusivos de su flota. Además de configurar las alarmas estáticas manualmente con Rules Detect, ahora puede utilizar el machine learning para conocer automátic amente el comportamiento esperado de su flota a partir de métricas personalizadas. Además, con la nueva compatibilidad con los filtros de dimensiones para ML Detect, podrá definir atributos para evaluar métricas más precisas en su perfil de seguridad de ML. Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender	14 de septiembre de 2022

AWS IoT Device Management y AWS IoT Device Defender permiten ahora la supervisión de métricas de dispositivos mediante la API ListMetricValues	Acceda a métricas históricas y personalizadas del dispositivo y de la nube desde dispositivos conectados que pertenezcan a un perfil de seguridad con la API ListMetricValues. Además de ver los datos en la consola de administración de AWS IoT, ahora podrá supervisar y crear su propia visualización mediante programación. Para obtener documentación relacionada, consulte Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender.	5 de abril de 2022
AWS IoT Device Defender es ahora compatible con los estados de verificación de alarmas de Detect	Verifique una alarma basándose en lo que estas muestren sobre las anomalías de comportamiento detectadas. Pueden verificar una alarma como Verdadero positivo, Benigno positivo, Falso positivo o Desconocido, así como ofrecer una descripción de su verificación. Para obtener documentación relacionada, consulte Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender.	24 de septiembre de 2021

Versión AWS IoT Device Defender Audit One-Click	Con Audit One-Click, los clientes de AWS IoT Core pueden mejorar su referenci a de seguridad, ya que les permite empezar a auditar sus cuentas y dispositivos de IoT para compararlos con los procedimientos recomenda dos de seguridad con un solo clic. Con Audit One-Click, los clientes pueden activar una auditoría AWS IoT Device Defender con configura ciones prestablecidas, lo que incluye la habilitación de todas las comprobaciones de auditoría disponibles y un programa de auditoría diario. También proporciona explicaci ones contextuales sobre las ventajas de las auditorías de seguridad periódicas. Audit One-Click solo está disponible desde la consola de AWS IoT. Para obtener documentación relacionada, consulte Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender.	22 de septiembre de 2021

Compatibilidad con AWS IoT Device Defender CloudFormation	AWS IoT Device Defender Rules Detect dispone ahora de una nueva métrica de duración de desconexión para supervisar la duración de dAWS IoT Device Defender es ahora compatible con AWS CloudFormation para la creación y configuración de los recursos de AWS IoT Device Defender, como las auditorías programadas y los perfiles de seguridad, de una forma segura, eficiente y repetible. Para obtener más información sobre los tipos de recursos de AWS CloudFormation compatibles con AWS IoT Device Defender, visite la Referencia de tipo de recurso de IoT.	5 de marzo de 2021
AWS IoT Device Defender agrega la compatibilidad con métricas personalizadas	Utilice AWS IoT Device Defender para supervisar las métricas de estado operativo que sean exclusivas de su flota o caso de uso. Las alertas se pueden ver en la consola de Device Defender o se pueden compartir a través de AWS Simple Notification Service (SNS). Para obtener documentación relacionada, consulte Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender.	15 de diciembre de 2020

AWS IoT Device Defender presenta Audit Finding Suppression	La característica Audit Finding Suppression le permite elegir los resultados de la auditoría que desea ver, y desactiva r los que no cumplan con los requisitos, para recursos específicos. Además, puede configurar las supresiones de los resultados de auditoría durante un periodo de tiempo determinado o de forma indefinida. Para obtener documentación relacionada, consulte Audit en la Guía para desarrolladores de AWS IoT Device Defender.	12 de agosto de 2020
AWS IoT Device Defender es ahora compatible con Dimensions para la supervisión de métricas por temas	La característica Dimension s permite a los clientes filtrar las métricas que Device Defender Detect evalúa por tema de MQTT. Dimension s es compatible con las siguientes métricas en la nube: número de mensajes recibidos, tamaño en bytes de los mensajes, número de mensajes enviados, IP de origen y número de errores de autorización. Para obtener documentación relacionada, consulte Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender.	2 de abril de 2020

Disponibilidad general de AWS IoT Device Defender ML Detect	La característica ML Detect de AWS IoT Device Defender detecta automáticamente las anomalías operativas y de seguridad en el nivel del dispositivo de toda la flota, usando para ello los datos históricos. Para obtener documentación relacionada, consulte Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender.	24 de marzo de 2020

AWS IoT Device Defender agrega cuatro nuevas comprobaciones a su capacidad de auditoría	Utilice AWS IoT Device Defender Audit para comprobar si hay dispositi vos en su flota que tengan permisos muy poco restricti vos, que tengan acceso a servicios que no se hayan utilizado en más de 365 días, que usen versiones de OpenSSL en sistemas operativos basados en Debian identificados por tener claves criptográficas predecibles (lo que hace que sean susceptib les a ataques de fuerza bruta) o que utilicen versiones de la biblioteca RSA de Infineon identificadas por una mala gestión de la generación de claves RSA (lo que hace que sean susceptibles a sufrir ataques informáticos). Para obtener documentación relacionada, consulte Audit en la Guía para desarrolladores de AWS IoT Device Defender.	25 de noviembre de 2019
AWS IoT Device Defender es compatible con las acciones de mitigación para los resultados de auditoría	AWS IoT Device Defender es compatible con la capacidad de los clientes de aplicar medidas de mitigación a los resultados de las auditorías. Para obtener documentación relacionada, consulte Audit en la Guía para desarrolladores de AWS IoT Device Defender.	6 de agosto de 2019

AWS IoT Device Defender es compatible con la monitorización del comportamiento de dispositivos no registrados	Identifique el comportamiento inusual de los dispositivos que no están registrados en AWS IoT Core. Para obtener documentación relacionada, consulte Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender.	15 de mayo de 2019
Ahora, AWS IoT Device Defender ofrece detección estadística de anomalías y visualización de datos	Utilice la detección estadística de anomalías y reciba alertas cuando un dispositivo no esté dentro del umbral basado en percentiles. Para obtener documentación relacionada, consulte Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender.	19 de febrero de 2019
Ahora, AWS IoT Device Defender permite supervisar la duración de la desconexión de los dispositivos	Ahora, AWS IoT Device Defender incluye dos métricas adicionales en la nube: el número de intentos de conexión y el número de desconexiones. Para obtener documentación relacionada, consulte Cloud-side metrics en la Guía para desarrolladores de AWS IoT Device Defender.	19 de diciembre de 2018