Guía del usuario

Amazon Detective

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

Amazon Detective: Guía del usuario

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

Las marcas comerciales y la imagen comercial de Amazon no se pueden utilizar en relación con 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 son propiedad de sus respectivos propietarios, que pueden o no estar afiliados, conectados o patrocinados por Amazon.

Table of Contents

¿Qué es Detective? ... 1
Características de Amazon Detective ... 1
Acceso a Amazon Detective ... 3
Precios de Amazon Detective ... 5
¿Cómo funciona Detective? ... 5
¿Quiénes usan Detective? ... 6
Servicios relacionados ... 7
Conceptos y terminología ... 9
Introducción ... 14
Configuración ... 14
Inscríbase en una Cuenta de AWS ... 15
Creación de un usuario con acceso administrativo ... 15
Requisitos previos ... 16
Concesión de los permisos requeridos de Detective ... 17
AWS Command Line Interface Versión compatible ... 17
Recomendaciones ... 17
Alineación recomendada con GuardDuty y AWS Security Hub ... 17
Actualización recomendada de la frecuencia de notificaciones GuardDuty CloudWatch ... 18
Habilitación de Detective ... 19
Comprobar que el Detective está ingiriendo datos ... 21
Datos de un gráfico de comportamiento ... 22
Cómo rellena el Detective un gráfico de comportamiento ... 23
Cómo procesa Detective los datos de origen ... 23
Extracción de Detective ... 23
Análisis de Detective ... 24
Periodo de aprendizaje de nuevos gráficos de comportamiento ... 24
Descripción general de la estructura de datos del gráfico de comportamiento ... 25
Tipos de elementos de la estructura de datos del gráfico de comportamiento ... 25
Tipos de entidades de la estructura de datos del gráfico de comportamiento ... 26
Datos de origen usados en un gráfico de comportamiento ... 32
Tipos de orígenes de datos principales en Detective ... 32
Tipos de orígenes de datos opcionales en Detective ... 33
Registros EKS de auditoría de Amazon ... 34
AWS hallazgos de seguridad ... 35

Cómo Detective ingiere y almacena datos de origen ... 36
Cómo aplica Detective la cuota de volumen de datos a los gráficos de comportamiento ... 37
Panel Resumen ... 39
Investigaciones ... 39
Geolocalizaciones recién observadas ... 40
Grupos de resultados activos en los últimos 7 días ... 41
Funciones y usuarios con mayor volumen de API llamadas ... 41
EC2instancias con el mayor volumen de tráfico ... 42
Clústeres de contenedor con mayor número de pods de Kubernetes ... 42
Notificación de valor aproximado ... 43
Cómo usar Detective con fines de investigación ... 44
Fases de una investigación ... 44
Puntos de partida para una investigación de Detectives ... 45
Los hallazgos detectados por GuardDuty ... 45
AWS hallazgos de seguridad agregados por Security Hub ... 45
Entidades extraídas de los datos de origen de Detective ... 46
Flujo de investigación de Detectives ... 46
Investigación de Detectives ... 48
Llevar a cabo una investigación de Detectives ... 48
Revisión de los informes de Investigaciones de Detectives ... 51
Comprensión de un informe de Investigaciones de Detectives ... 52
Resumen del informe de Investigaciones de Detectives ... 54
Descarga de un informe de Investigaciones de Detectives ... 54
Archivar un informe de Investigaciones de Detectives ... 55
Análisis de resultados ... 57
Descripción general del resultado ... 58
Rango temporal utilizado para la descripción general del resultado ... 58
Detalles del resultado ... 58
Entidades relacionadas ... 58
Solución de problemas de 'Página no encontrada' ... 58
Búsqueda de grupos ... 59
Explicación de la página de grupos de resultados ... 61
Resultados informativos en grupos de resultados ... 63
Perfiles de grupos de resultados ... 64
Visualización de grupos de resultados ... 65
Resumen de grupo de resultados ... 68

Revisión de resumen del grupo de resultados ... 69
Deshabilitación del resumen de grupo de resultados ... 70
Deshabilitación del resumen de grupo de resultados ... 71
Regiones admitidas ... 71
Archivar un hallazgo GuardDuty ... 71
Analizando entidades ... 73
Uso de perfiles de entidades ... 73
Rango temporal de un perfil de entidad ... 74
Identificador y tipo de entidad ... 74
Resultados implicados ... 74
Grupos de resultados que impliquen a esta entidad ... 74
Paneles de perfil que contienen detalles de entidad y resultados de análisis ... 75
Navegar por el perfil de una entidad ... 75
Paneles de perfiles ... 76
Tipos de información de un panel de perfil ... 76
Tipos de visualizaciones de un panel de perfil ... 80
Preferencias de los paneles de perfil ... 85
Navegar a un perfil de entidad ... 86
Pasar desde otra consola ... 87
Desplazarse mediante una URL ... 89
Añadir URL de resultados de Detective a Splunk ... 93
Pasar a otra consola ... 93
Pasar a otro perfil de entidad ... 93
Explorar detalles de actividad ... 94
Volumen total de API llamadas ... 95
Geolocalización ... 102
Volumen VPC de flujo total ... 106
Volumen total de llamadas de Kubernetes API ... 111
Administración del rango temporal ... 115
Establecer fechas y horas de inicio y de finalización específicas ... 116
Edición de la duración del rango temporal ... 116
Establecer el rango temporal en una franja horaria de resultados. ... 117
Establecer el rango temporal en la página de resumen ... 117
Ver los resultados de una entidad ... 118
Entidades de gran volumen ... 119
¿Qué es una entidad de gran volumen? ... 119

Ver la notificación de entidad de gran volumen en un perfil 120
Ver la lista de entidades de gran volumen para el rango temporal actual 120
Búsqueda de resultados o entidades 122
Completar la búsqueda 122
Uso de los resultados de búsqueda 124
Solución de problemas de búsqueda 125
Administración de cuentas 126
Restricciones y recomendaciones 127
Número máximo de cuentas miembro 127
Cuentas y regiones 127
Alineación de las cuentas de administrador con Security Hub y GuardDuty 128
Concesión de los permisos necesarios para cuentas de administrador 128
Reflejo de las actualizaciones en una organización en Detective 128
Uso de Organizations para gestionar cuentas con gráficos de comportamiento 128
Designación de una cuenta de administrador de Detective para la organización 129
Habilitación de cuentas de la organización como cuentas de miembros 130
Designación de la cuenta de administrador de Detective 131
Designación de un administrador de Detectives 132
Eliminación de la cuenta de administrador de Detective 135
Acciones disponibles para las cuentas 138
Visualización de la lista de cuentas 140
Listado de cuentas (consola) 141
Listar sus cuentas de miembros (DetectiveAPI, AWS CLI) 143
Administrar las cuentas de miembros de la organización 144
Habilitar nuevas cuentas de organización 145
Habilitar las cuentas de la organización como cuentas de miembros de Detectives 147
Desasociación de cuentas de la organización 149
Administración de cuentas de miembros invitadas 150
Cómo invitar a las cuentas individuales a un gráfico de comportamiento 152
Incluir una lista de las cuentas de los miembros en un gráfico de comportamiento 154
Habilitación de una cuenta de miembro con el estado No habilitado 156
Eliminar cuentas de miembro 157
Para cuentas de miembros: administración de invitaciones y suscripciones 159
IAMpolítica para una cuenta de miembro 159
Visualización de invitaciones a gráficos de comportamiento 161
Respuesta a una invitación de un gráfico de comportamiento 162

Eliminación de la cuenta de un gráfico de comportamiento 164
Efecto de las acciones de la cuenta 165
Deshabilitación de Detective 165
Eliminación de una cuenta de miembro del gráfico de comportamiento 165
Abandono de la organización por parte de una cuenta de miembro 165
AWS cuenta suspendida 166
AWS cuenta cerrada 166
Secuencias de comandos Python de Amazon Detective 167
Descripción general del script `enableDetective.py` 167
Descripción general del script `disableDetective.py` 168
Permisos necesarios para los scripts 168
Configuración del entorno de ejecución para scripts de Python 170
Creación de una lista en formato `.csv` con las cuentas de miembros para agregar o eliminar 172
Ejecución de `enableDetective.py` 172
Ejecución de `disableDetective.py` 174
Integración de Detectives con Security Lake 176
Habilitación de la integración 176
Antes de empezar 178
Paso 1: Crear un suscriptor de Security Lake en Detective 178
Paso 2: Añadir los permisos de IAM necesarios 179
Paso 3: Aceptar la invitación del ARN de Resource Share 182
Cambiar la configuración de integración de Detective 189
AWS Regiones compatibles 190
Consulta de registros sin procesar en Detective 191
Consultando registros sin procesar para un rol AWS 195
Consulta de registros sin procesar para un clúster de Amazon EKS 195
Consulta de registros sin procesar para una instancia de Amazon EC2 196
Deshabilitación de la integración 196
Eliminar una CloudFormation pila 197
Previsión y supervisión de costos 199
Acerca de la prueba gratuita para gráficos de comportamiento 199
Versión de prueba gratuita para orígenes de datos opcionales 200
Uso y costo de la cuenta de administrador 201
Volumen de ingesta de datos de cada cuenta 201
Costos previstos del gráfico de comportamiento 202

Costo previsto del gráfico de comportamiento ... 202
Volumen de ingesta de datos por paquetes de origen ... 202
Seguimiento del uso de cuentas de miembro ... 203
Volumen de ingesta de cada gráfico de comportamiento ... 203
Costo previsto en todos los gráficos de comportamiento ... 204
Cómo calcula Detective el costo previsto ... 204
Seguridad ... 206
Protección de datos ... 207
Administración de claves ... 208
Identity and Access Management ... 208
Público ... 209
Autenticación con identidades ... 209
Administración de acceso mediante políticas ... 213
Cómo funciona Amazon Detective con IAM ... 215
Ejemplos de políticas basadas en identidades ... 222
AWS políticas gestionadas ... 228
Usar roles vinculados a servicios ... 239
Solución de problemas de identidad y acceso ... 242
Validación de conformidad ... 244
Resiliencia ... 244
Seguridad de la infraestructura ... 245
Prácticas recomendadas de seguridad ... 245
Mejores prácticas para las cuentas de administrador de Detectives ... 246
Prácticas recomendadas para cuentas de miembros ... 246
Registro de API llamadas ... 247
Información de Detectives en CloudTrail ... 247
Comprensión de las entradas del archivo de registro de Detective ... 248
Regiones y cuotas ... 250
Regiones y puntos de conexión de Detectives ... 250
Cuotas de Detective ... 250
Internet Explorer 11 no compatible ... 251
Administrar etiquetas ... 252
Visualización de las etiquetas de un gráfico de comportamiento ... 252
Añadir etiquetas a un gráfico de comportamiento ... 253
Eliminar etiquetas de un gráfico de comportamiento ... 254
Deshabilitación de Amazon Detective ... 255

Deshabilitación de Detective (consola) 255
Desactivar Detective (API de Detective), AWS CLI 255
Desactivación de Detective en todas las regiones (secuencia de comandos de Python activada GitHub) 256
Historial de revisión 257
..... cclxxxvii

¿Qué es Amazon Detective?

Amazon Detective le ayuda a analizar, investigar e identificar rápidamente la causa raíz de resultados de seguridad o actividades sospechosas. Detective recopila automáticamente los datos de registro de sus recursos de AWS . A continuación, utiliza el machine learning, el análisis estadístico y la teoría de grafos para generar visualizaciones que lo ayuden a realizar investigaciones sobre la seguridad con mayor rapidez y de forma más eficaz. Las agregaciones de datos, los resúmenes y los contextos prediseñados de Detective ayudan a analizar y determinar rápidamente la naturaleza y el alcance de los posibles problemas de seguridad.

Con Detective, puede acceder a datos de eventos históricos de hasta un año de antigüedad. Estos datos están disponibles a través de un conjunto de visualizaciones que muestran los cambios en el tipo y el volumen de actividad durante un intervalo de hora seleccionado. El Detective relaciona estos cambios con los GuardDuty hallazgos. Para obtener más información sobre los datos de origen en Detective, consulte the section called “Datos de origen usados en un gráfico de comportamiento”.

Al agregar datos automáticamente y proporcionar herramientas visuales, Amazon Detective le permite llevar a cabo investigaciones de seguridad más rápidas y eficientes. Puede analizar rápidamente los posibles problemas y determinar el alcance de las amenazas a la seguridad.

Temas

- Características de Amazon Detective
- Acceso a Amazon Detective
- Precios de Amazon Detective
- ¿Cómo funciona Detective?
- ¿Quiénes usan Detective?
- Servicios relacionados

Características de Amazon Detective

Estas son algunas de las principales formas en las que Amazon Detective resulta útil para investigar actividades sospechosas en su AWS entorno y analizar los recursos para identificar la causa raíz de los problemas de seguridad.

Detective buscando grupos

La búsqueda de grupos por parte de Detectives le permite examinar múltiples actividades en relación con un posible incidente de seguridad. Puede analizar la causa raíz de los GuardDuty hallazgos de alta gravedad mediante la búsqueda de grupos. Si un agente de amenazas intenta poner en peligro su AWS entorno, normalmente lleva a cabo una secuencia de acciones que generan varios hallazgos de seguridad y comportamientos inusuales.

La página de búsqueda de grupos de Detective muestra todos los grupos de búsqueda relacionados extraídos de su gráfico de comportamiento. Para obtener más información sobre cómo aprovechar la búsqueda de grupos para analizar la causa raíz de los hallazgos de seguridad, consulte Análisis de la búsqueda de grupos en Detective.

Detective proporciona una visualización interactiva de cada grupo de búsqueda para ayudarle a investigar los problemas de seguridad de forma más rápida y exhaustiva. La visualización está diseñada para mostrar las entidades y los hallazgos relacionados con un incidente de seguridad, lo que facilita la comprensión de las conexiones y las causas fundamentales. Le ayuda a investigar los problemas de forma más rápida y exhaustiva con menos esfuerzo. El panel de visualización del grupo de búsqueda muestra los hallazgos y las entidades que participan en un grupo de búsqueda.

Investigación de Detectives para clasificar los hallazgos

Con Detective Investigation, puede investigar a IAM los usuarios y las IAM funciones mediante indicadores de compromiso, que pueden ayudarlo a determinar si un recurso está involucrado en un incidente de seguridad. Un indicador de peligro (IOC) es un artefacto observado en o sobre una red, un sistema o un entorno que puede (con un alto nivel de confianza) identificar una actividad maliciosa o un incidente de seguridad. Con las investigaciones de Detectives, puede maximizar la eficiencia, centrarse en las amenazas a la seguridad y reforzar las capacidades de respuesta a los incidentes.

Detective Investigation utiliza modelos de aprendizaje automático e inteligencia de amenazas para descubrir solo los problemas más críticos y sospechosos, lo que le permite centrarse en investigaciones de alto nivel. Analiza automáticamente los recursos de su AWS entorno para identificar posibles indicadores de peligro o actividad sospechosa. Esto le permite identificar patrones y comprender qué recursos se ven afectados por los eventos de seguridad, ofreciendo un enfoque proactivo para la identificación y mitigación de las amenazas.

Puedes utilizar Iniciar una investigación detectivesca desde la consola de Detectives con Ejecutar una investigación detectivesca. Para ejecutar una investigación mediante programación, utilice

la StartInvestigationoperación del Detective. API Para ejecutar una investigación con el comando AWS Command Line Interface (AWS CLI) ejecute el comando start-investigation.

Integración de Detective con Amazon Security Lake

Detective se integra con Amazon Security Lake, lo que significa que puede consultar y recuperar los datos de registro sin procesar almacenados por Security Lake. Con esta integración, puede recopilar registros y eventos de las siguientes fuentes que Security Lake admite de forma nativa.

- AWS CloudTrail eventos de administración (versión 1.0 y posteriores)
- Amazon Virtual Private Cloud (AmazonVPC) Flow Logs versión 1.0 y versiones posteriores
- Registro de auditoría de Amazon Elastic Kubernetes Service (EKSAmazon) versión 2.0

Tras integrar Detective con Security Lake, Detective comienza a extraer registros sin procesar de Security Lake relacionados con los eventos AWS CloudTrail de administración y Amazon VPC Flow Logs. Puede consultar los registros sin procesar para ver los registros y los eventos en Detective.

Investigue VPC el volumen de flujo

Con Detective, puede examinar de forma interactiva los detalles de la actividad de los flujos de red de la nube privada virtual (VPC) de sus instancias de Amazon Elastic Compute Cloud (AmazonEC2) y los pods de Kubernetes. Detective recopila automáticamente los registros de VPC flujo de sus cuentas monitoreadas, los agrega por EC2 instancia y presenta resúmenes visuales y análisis sobre estos flujos de red.

EC2Por ejemplo, los detalles de la actividad del volumen de VPC flujo total muestran las interacciones entre la EC2 instancia y las direcciones IP durante un intervalo de tiempo seleccionado.

En el caso de un pod de Kubernetes, el volumen de VPC flujo general muestra el volumen total de bytes que entran y salen de la dirección IP asignada al pod de Kubernetes para todas las direcciones IP de destino.

Acceso a Amazon Detective

Amazon Detective está disponible en la mayoría Regiones de AWS. Para obtener una lista de las regiones en las que Detective está disponible actualmente, consulte los puntos de conexión y las cuotas de Amazon Detective en. Referencia general de AWS Para obtener información sobre cómo

gestionar Regiones de AWS su cuenta Cuenta de AWS, consulte Especificar qué Regiones de AWS cuenta puede utilizar en la Guía de AWS Account Management referencia.

En cada región, puedes trabajar con Detective de cualquiera de las siguientes maneras.

AWS Management Console

AWS Management Console Se trata de una interfaz basada en un navegador que puede utilizar para crear y gestionar AWS recursos. Como parte de esa consola, la consola Amazon Detective proporciona acceso a tu cuenta, datos y recursos de Detective. Puede realizar cualquier tarea de Detective mediante la consola Detective: revise las posibles amenazas a la seguridad y analice, investigue e identifique la causa raíz de los hallazgos de seguridad.

AWS herramientas de línea de comandos

Con las herramientas de línea de AWS comandos, puede emitir comandos en la línea de comandos de su sistema para realizar tareas y AWS tareas de Detective. Usar la línea de comandos puede ser más rápido y práctico que usar la consola. Las herramientas de línea de comandos también son útiles si desea crear scripts que realicen tareas.

AWS proporciona dos conjuntos de herramientas de línea de comandos: el AWS Command Line Interface (AWS CLI) y el Herramientas de AWS para PowerShell. Para obtener información sobre la instalación y el uso de AWS CLI, consulte la Guía del AWS Command Line Interface usuario. Para obtener información sobre la instalación y el uso de las herramientas PowerShell, consulte la Guía del Herramientas de AWS para PowerShell usuario.

AWS SDKs

AWS proporciona SDKs bibliotecas y código de muestra para varios lenguajes de programación y plataformas, por ejemplo, Java, Go, Python, C++ y. NET. SDKsProporcionan un acceso cómodo y programático a Detective y otros Servicios de AWS. También permiten realizar tareas como firmar solicitudes criptográficamente, administrar errores y reintentar solicitudes automáticamente. Para obtener información sobre la instalación y el uso de AWS SDKs, consulte Herramientas sobre AWS las que construir.

Amazon Detective REST API

Amazon Detective REST API le ofrece un acceso completo y programático a su cuenta, datos y recursos de Detective. Con estoAPI, puede enviar HTTPS solicitudes directamente al Detective. Sin embargo, a diferencia de las herramientas de línea de AWS comandosSDKs, el uso de estas herramientas API requiere que su aplicación gestione detalles de bajo nivel, como

generar un hash para firmar una solicitud. Para obtener información al respectoAPI, consulte la APIReferencia de Detectives.

Precios de Amazon Detective

Al igual que con otros AWS productos, no hay contratos ni compromisos mínimos para usar Amazon Detective.

Los precios de Detective se basan en varias dimensiones y cobran una tarifa plana escalonada por GB para todos los datos, independientemente de la fuente. Para obtener más información, consulta los precios de Amazon Detective.

Para ayudarlo a comprender y pronosticar el costo de usar Detective, Detective proporciona los costos de uso estimados de su cuenta. Puedes revisar estas estimaciones en la consola Amazon Detective y acceder a ellas con Amazon DetectiveAPI. Según cómo utilice el servicio, es posible que incurra en costes adicionales por utilizar otras funciones Servicios de AWS en combinación con determinadas funciones de Detective, como la integración de Security Lake y Detective Investigations.

Al activar Detective por primera vez, Cuenta de AWS se inscribe automáticamente en la versión de prueba gratuita de 30 días de Detective. Esto incluye cuentas individuales habilitadas como parte de una organización en AWS Organizations. Durante la prueba gratuita, el uso de Detective en la versión correspondiente es gratuita Región de AWS.

Para ayudarlo a comprender y pronosticar el costo de usar Detective una vez que finalice la prueba gratuita, Detective le proporciona una estimación de los costos de uso en función de su uso de Detective durante la prueba. Sus datos de uso también indican el tiempo que queda hasta que finalice la prueba gratuita. Puedes revisar los datos relacionados con el uso de tu cuenta de Detective en la consola de Amazon Detective y acceder a ellos con Amazon DetectiveAPI.

¿Cómo funciona Detective?

Detective extrae automáticamente los eventos en función del tiempo, como los intentos de inicio de sesión, API las llamadas y el tráfico de red, AWS CloudTrail y de los registros de VPC flujo de Amazon. También ingiere los hallazgos detectados por. GuardDuty

A partir de esos eventos, Detective usa el machine learning y la visualización para crear una vista unificada e interactiva del comportamiento de los recursos y de las interacciones entre ellos a lo largo

del tiempo. Puede explorar este gráfico de comportamiento para examinar acciones dispares, como intentos de inicio de sesión fallidos o llamadas sospechosas. API También puedes ver cómo afectan estas acciones a recursos como las AWS cuentas y las EC2 instancias de Amazon. Puede ajustar el alcance y el cronograma del gráfico de comportamiento para diversas tareas:

- Investigue rápidamente cualquier actividad que se salga de la normalidad.
- Identifique patrones que puedan indicar un problema de seguridad.
- Descubra todos los recursos a los que afecta un resultado.

Las visualizaciones personalizadas de Detective proporcionan una base y un resumen de la información de la cuenta. Estos hallazgos pueden ayudar a responder a preguntas como «¿Es una propuesta API inusual para este puesto?» O “¿Se espera un aumento del tráfico a partir de esta instancia?”.

Con Detective, ya no tendrá que organizar los datos ni desarrollar, configurar o adaptar sus propias consultas y algoritmos. No hay costos iniciales y solo pagará por los eventos analizados, sin necesidad de implementar ningún software adicional ni de suscribirse a otras fuentes.

¿Quiénes usan Detective?

Cuando una cuenta habilita Detective, se convierte en la cuenta de administrador de un gráfico de comportamiento. Un gráfico de comportamiento es un conjunto vinculado de datos extraídos y analizados de una o más AWS cuentas. Las cuentas de administrador invitan a cuentas de miembro a contribuir con sus datos al gráfico de comportamiento de la cuenta de administrador.

Detective también está integrado con AWS Organizations. La cuenta de administración de su organización designa una cuenta de administrador de Detective para la organización. La cuenta de administrador de Detective habilita las cuentas de la organización como cuentas de miembro en el gráfico de comportamiento de la organización.

Para obtener información sobre cómo Detective usa los datos de origen de las cuentas de gráficos de comportamiento, consulte the section called “Datos de origen usados en un gráfico de comportamiento”.

Para obtener información sobre cómo las cuentas de administrador tratan los gráficos de comportamiento, consulte Administración de cuentas. Para obtener información sobre cómo las cuentas de miembro administran las invitaciones y pertenencias a sus gráficos de comportamiento,

consulte the section called “Para cuentas de miembros: administración de invitaciones y suscripciones”.

La cuenta de administrador utiliza los análisis y las visualizaciones generados a partir del gráfico de comportamiento para investigar AWS los recursos y los GuardDuty hallazgos. Al utilizar las integraciones de Detective con GuardDuty y AWS Security Hub, puede pasar de un GuardDuty hallazgo en estos servicios directamente a la consola de Detective.

Una investigación de Detective se centra en la actividad relacionada con los recursos de AWS implicados. Para obtener información general sobre el proceso de investigación en Detective, consulte Cómo usar Amazon Detective con fines de investigación en la Guía del usuario de Detective.

Servicios relacionados

Para proteger aún más sus datos, cargas de trabajo y aplicaciones AWS, considere la posibilidad de utilizar lo siguiente Servicios de AWS en combinación con Amazon Detective.

AWS Security Hub

AWS Security Hub le ofrece una visión completa del estado de seguridad de sus AWS recursos y le ayuda a comprobar su AWS entorno según los estándares y las mejores prácticas del sector de la seguridad. Esto lo consigue, en parte, consumiendo, agrupando, organizando y priorizando los hallazgos de seguridad de varios productos Servicios de AWS (incluido Detective) y de AWS Partner Network () compatibles (APN). Security Hub le ayuda a analizar sus tendencias de seguridad e identificar los problemas de seguridad más prioritarios en todo su AWS entorno.

Para obtener más información sobre Security Hub, consulte la AWS Security Hub Guía del usuario.

Amazon GuardDuty

Amazon GuardDuty es un servicio de supervisión de seguridad que analiza y procesa determinados tipos de AWS registros, como los registros de eventos de AWS CloudTrail datos para Amazon S3 y los registros CloudTrail de eventos de administración. Utiliza fuentes de inteligencia sobre amenazas, como listas de direcciones IP y dominios maliciosos, y el aprendizaje automático para identificar actividades inesperadas y potencialmente no autorizadas y maliciosas en su AWS entorno.

Para obtener más información GuardDuty, consulta la Guía del GuardDuty usuario de Amazon.

Amazon Security Lake

Amazon Security Lake es un servicio de lago de datos de seguridad totalmente gestionado. Puede usar Security Lake para centralizar automáticamente los datos de seguridad de los AWS entornos, los proveedores de SaaS, las fuentes locales, las fuentes en la nube y las fuentes de terceros en un lago de datos diseñado específicamente que se almacena en su cuenta. AWS Security Lake le ayuda a analizar los datos de seguridad para que pueda comprender mejor su postura de seguridad en toda la organización. Con Security Lake, también puede mejorar la protección de sus cargas de trabajo, aplicaciones y datos.

Para obtener más información sobre Security Lake, consulte la Guía del usuario de Amazon Security Lake. Para obtener más información sobre el uso conjunto de Detective y Security Lake, consulteIntegración de Detectives con Security Lake.

Para obtener más información sobre los servicios de AWS seguridad adicionales, consulte Seguridad, identidad y conformidad en AWS.

Conceptos y terminología de Amazon Detective

Los siguientes términos y conceptos son importantes para comprender Amazon Detective y su funcionamiento.

Cuenta de administrador

La Cuenta de AWS que posee un gráfico de comportamiento y que lo usa para investigar.

La cuenta de administrador invitar a las cuentas de miembro a contribuir al gráfico de comportamiento con sus datos. Para obtener más información, consulte the section called “Administración de cuentas de miembros invitadas”.

Para el gráfico de comportamiento de la organización, la cuenta de administrador es la cuenta de administrador de Detective designada por la dirección de la organización. Para obtener más información, consulte the section called “Designación de la cuenta de administrador de Detective”. La cuenta de administrador de Detective puede habilitar cualquier cuenta de la organización como cuenta de miembro en el gráfico de comportamiento de la organización. Para obtener más información, consulte the section called “Administrar las cuentas de miembros de la organización”.

Las cuentas de administrador también pueden ver el uso de datos del gráfico de comportamiento, y eliminar cuentas de miembro del gráfico de comportamiento.

Organización del sistema autónomo (ASO)

Organización titulada a la que se le asigna un sistema autónomo. Este sistema autónomo es una red heterogénea o un conjunto de redes que utilizan políticas y lógicas de enrutamiento similares.

Gráfico de comportamiento

Conjunto de datos enlazado generado a partir de datos de origen entrantes que está asociado a uno o más Cuentas de AWS.

Cada gráfico de comportamiento utiliza la misma estructura de resultados, entidades y relaciones.

Cuenta de administrador delegado (AWS Organizations)

En Organizations, la cuenta de administrador delegado de un servicio puede administrar el uso de un servicio para la organización.

En Detective, la cuenta de administrador de Detective también es la cuenta de administrador delegado, a menos que la cuenta de administrador de Detective sea la cuenta de administración

de la organización. La cuenta de administración de la organización no puede ser la cuenta de administrador delegado.

Detective permite la autodelegación. Una cuenta de administración de la organización puede delegar su propia cuenta como administrador delegado de Detective, pero esto solo se registraría o recordaría en el ámbito de Detective, y no en el de las organizaciones.

Cuenta de administrador de Detective

La cuenta designada por la cuenta de administración de la organización como cuenta de administrador para el gráfico de comportamiento de la organización en una región. Para obtener más información, consulte the section called “Designación de la cuenta de administrador de Detective”.

Detective recomienda que la cuenta de administración de la organización elija una cuenta que no sea la suya.

Si la cuenta no es la cuenta de administración de la organización, entonces la cuenta de administrador de Detective es también la cuenta de administrador delegado de Detective en Organizations.

Datos de origen de Detective

Versiones estructuradas y procesadas de información de los siguientes tipos de fuentes:

- Inicia sesión desde AWS servicios, como AWS CloudTrail logs y Amazon VPC Flow Logs
- GuardDuty hallazgos

Detective usa los datos de origen de Detective para rellenar el gráfico de comportamiento. Detective también almacena copias de los datos de origen de Detective para respaldar sus análisis.

Entidad

Elemento extraído de los datos ingeridos.

Cada entidad tiene un tipo, que identifica al tipo de objeto al que representa. Algunos ejemplos de tipos de entidades son las direcciones IP, las EC2 instancias de Amazon y AWS usuarios.

Las entidades pueden ser AWS los recursos que usted administra o las direcciones IP externas que han interactuado con sus recursos.

Para cada entidad, los datos de origen también se utilizan para rellenar las propiedades de entidad. Los valores de las propiedades se pueden extraer directamente de los registros de origen, o se pueden agregar de varios registros.

Resultado

Amazon ha detectado un problema de seguridad GuardDuty.

Grupo de resultados

Conjunto de resultados, entidades y evidencias relacionados que pueden tener que ver con el mismo evento o problema de seguridad. Detective genera grupos de resultados basados en un modelo de machine learning incorporado.

Pruebase de Detective

Detective identifica pruebas adicionales relacionadas con un grupo de resultados basándose en los datos de su gráfico de comportamiento recopilados en los últimos 45 días. Estas evidencias se presentan como un resultado con valor de gravedad Informativa. Las evidencias proporcionan información de apoyo que pone de relieve una actividad inusual o un comportamiento desconocido que puedan resultar sospechosos si se observan dentro de un grupo de resultados. Un ejemplo de ello podrían ser las geolocalizaciones observadas recientemente o las API llamadas observadas durante el tiempo transcurrido desde el momento en que se produjo un hallazgo. En este momento, estos resultados solo se pueden ver en Detective y no se envían a Security Hub.

Descripción general de la búsqueda

Una sola página que proporciona un resumen de la información sobre un resultado.

Una descripción general de resultado contiene una lista de las entidades implicadas en los resultados. Desde la lista, puede pasar al perfil de una entidad.

La descripción general de un resultado también contiene un panel de detalles que contiene los atributos del resultado.

Entidad de gran volumen

Entidad que tiene conexiones hacia o desde un gran número de otras entidades durante un intervalo de tiempo. Por ejemplo, una EC2 instancia puede tener conexiones desde millones de direcciones IP. El número de conexiones supera el umbral que Detective puede admitir.

Cuando el rango temporal actual contiene un intervalo de tiempo de gran volumen, Detective lo notifica al usuario.

Para obtener más información, consulte Ver detalles de entidades de gran volumen en la Guía del usuario de Amazon Detective.

Investigación

Proceso de clasificar una actividad sospechosa o de interés, determinar su alcance, identificar su origen o causa subyacente y, finalmente, determinar cómo proceder.

Cuenta de miembro

Un registro Cuenta de AWS que una cuenta de administrador invitó a aportar datos a un gráfico de comportamiento. En el gráfico de comportamiento de la organización, una cuenta de miembro puede ser una cuenta de organización que la cuenta de administrador de Detective ha habilitado como cuenta de miembro.

Las cuentas de miembro que estén invitadas pueden responder a la invitación del gráfico de comportamiento y eliminar su cuenta del gráfico de comportamiento. Para obtener más información, consulte the section called “Para cuentas de miembros: administración de invitaciones y suscripciones”.

Las cuentas de organización no pueden cambiar su pertenencia al gráfico de comportamiento de la organización.

Todas las cuentas de miembro también pueden ver la información de uso de su cuenta en todos los gráficos de comportamiento a los que contribuyen con datos.

No tienen ningún otro acceso al gráfico de comportamiento.

Gráfico de comportamiento de la organización

Gráfico de comportamiento que pertenece a la cuenta de administrador de Detective. La cuenta de administración de la organización designa la cuenta de administrador de Detective. Para obtener más información, consulte the section called “Designación de la cuenta de administrador de Detective”.

En el gráfico de comportamiento de la organización, la cuenta de administrador de Detective controla si una cuenta de organización es una cuenta de miembro. Una cuenta de organización no se puede eliminar a sí misma del gráfico de comportamiento de la organización.

La cuenta de administrador de Detective también puede invitar a cuentas al gráfico de comportamiento de la organización.

Perfil

Una sola página que proporciona una recopilación de visualizaciones de datos relacionadas con la actividad de una entidad.

En el caso de los resultados, los perfiles ayudan a los analistas a determinar si el resultado es realmente preocupante o si es solo un falso positivo.

Los perfiles proporcionan información que sirve para respaldar la investigación de un resultado o la búsqueda genérica de actividad sospechosa.

Panel de perfil

Una sola visualización de un perfil. Cada panel de perfil está diseñado para ayudar a responder una o varias preguntas específicas para ayudar al analista en una investigación.

Los paneles de perfil pueden contener pares de clave y valor, tablas, cronogramas, gráficos de barras o gráficos de geolocalización.

Relación

Actividad que se produce entre entidades individuales. Las relaciones también se extraen de los datos de origen entrantes.

Al igual que una entidad, una relación tiene un tipo que identifica los tipos de entidades implicadas y el sentido de la conexión. Un ejemplo de un tipo de relación es una dirección IP que se conecta a una EC2 instancia de Amazon.

Rango temporal

Franja horaria que se utiliza para delimitar los datos que se muestran en los perfiles.

El rango temporal predeterminado de un resultado refleja la primera y la última vez que se observó la actividad sospechosa.

El rango temporal predeterminado de un perfil de entidad son las 24 horas anteriores.

Primeros pasos con Amazon Detective

Este tutorial proporciona una introducción a Amazon Detective. Aprenderás cómo activar Detective en tu AWS cuenta. También aprenderás a comprobar que el Detective ha empezado a ingerir y extraer datos de tu AWS cuenta para incluirlos en tu gráfico de comportamiento.

Al habilitar Amazon Detective, este crea un gráfico de comportamiento específico de una región en el que su cuenta es la cuenta de administrador. Inicialmente, es la única cuenta del gráfico de comportamiento. A continuación, la cuenta de administrador podrá invitar a otras AWS cuentas a que contribuyan con sus datos al gráfico de comportamiento. Consulte Administración de cuentas.

Al habilitar Detective en una región por primera vez, se inicia un periodo de prueba gratuita de 30 días para el gráfico de comportamiento. Si la cuenta deshabilita Detective y vuelve a habilitarlo, la prueba gratuita deja de estar disponible. Consulte the section called “Acerca de la prueba gratuita para gráficos de comportamiento”.

Una vez haya concluido la prueba gratuita, se cobrará a cada cuenta del gráfico de comportamiento por los datos que aporten. La cuenta de administrador puede realizar un seguimiento del uso y ver el costo total previsto a lo largo de un periodo típico de 30 días para todo el gráfico de comportamiento. Para obtener más información, consulte the section called “Uso y costo de la cuenta de administrador”. Las cuentas de miembros pueden realizar un seguimiento del uso y del costo previsto de los gráficos de comportamiento a los que pertenecen. Para obtener más información, consulte the section called “Seguimiento del uso de cuentas de miembro”.

Temas

- Configurar tu AWS cuenta
- Requisitos previos para activar Detective
- Recomendaciones para habilitar Detective
- Habilitación de Detective

Configurar tu AWS cuenta

Para habilitar Amazon Detective, necesita tener una Cuenta de AWS. Si no tiene una AWS cuenta, complete los siguientes pasos para crear una.

Inscríbase en una Cuenta de AWS

Si no tiene uno Cuenta de AWS, complete los siguientes pasos para crearlo.

Para suscribirse a una Cuenta de AWS

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

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

   Cuando te registras en un Cuenta de AWS, Usuario raíz de la cuenta de AWSse crea un. 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 te envía un correo electrónico de confirmación una vez finalizado el proceso de registro. En cualquier momento, puede ver la actividad de su cuenta actual y administrarla accediendo a https://aws.amazon.com/y seleccionando Mi cuenta.

Creación de un usuario con acceso administrativo

Después de crear un usuario administrativo Cuenta de AWS, asegúrelo Usuario raíz de la cuenta de AWS AWS IAM Identity Center, habilite y cree un usuario administrativo para no usar el usuario root en las tareas diarias.

Proteja su Usuario raíz de la cuenta de AWS

1. Inicie sesión AWS Management Consolecomo propietario de la cuenta seleccionando el usuario root e introduciendo su dirección de Cuenta de AWS correo electrónico. 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 Habilitar un dispositivo MFA virtual para el usuario Cuenta de AWS raíz (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 su uso Directorio de IAM Identity Center como fuente de identidad, consulte Configurar el acceso de los usuarios con la configuración predeterminada Directorio de IAM Identity Center en la Guía del AWS IAM Identity Center usuario.

Inicio de sesión como usuario con acceso de administrador

- Para iniciar sesión con el usuario de IAM Identity Center, use 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 Centro de identidades de IAM, consulte Iniciar sesión en el portal de AWS acceso en la Guía del AWS Sign-In usuario.

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 .

Requisitos previos para activar Detective

Asegúrese de que se cumplen los siguientes requisitos antes de activar Detective.

Concesión de los permisos requeridos de Detective

Antes de poder habilitar Detective, debe asegurarse de que la entidad principal de IAM cuenta con los permisos requeridos de Detective. La entidad principal puede ser un usuario o rol existente que esté utilizando, aunque también puede crear un nuevo usuario o rol para utilizar Detective.

Cuando se registra en Amazon Web Services (AWS), su cuenta se registra automáticamente para todos los Servicios de AWS, incluido Amazon Detective. Sin embargo, para habilitar y utilizar Detective, primero tiene que configurar permisos que permitan acceder a la consola de Amazon Detective y a las operaciones de la API. Usted o su administrador pueden hacerlo mediante AWS Identity and Access Management (IAM) para adjuntar la política `AmazonDetectiveFullAccess` gestionada a su principal de IAM, lo que permite el acceso a todas las acciones de los Detectives. Sin estos permisos de IAM, es posible que vea la página Introducción a Detective en la AWS consola. Como resultado, la consola no mostrará ningún gráfico activo hasta que se agreguen estos permisos, incluso si el servicio está activado.

AWS Command Line Interface Versión compatible

Para utilizar el AWS CLI para realizar tareas de Detective, la versión mínima requerida es la 1.16.303.

Recomendaciones para habilitar Detective

Considera seguir estas recomendaciones antes de activar Detective

Alineación recomendada con GuardDuty y AWS Security Hub

Si está inscrito en GuardDuty y AWS Security Hub, le recomendamos que su cuenta sea una cuenta de administrador para esos servicios. Si las cuentas de administrador son la misma para los tres servicios, los siguientes puntos de integración funcionan sin problemas.

- En GuardDuty nuestro Security Hub, al ver los detalles de un GuardDuty hallazgo, puede pasar de los detalles del hallazgo al perfil de búsqueda del Detective.
- En Detective, al investigar un GuardDuty hallazgo, puedes elegir la opción de archivarlo.

Si tiene cuentas de administrador diferentes para GuardDuty Security Hub, le recomendamos que alinee las cuentas de administrador en función del servicio que utilice con más frecuencia.

- Si lo usa con GuardDuty más frecuencia, habilite Detective con la cuenta de GuardDuty administrador.

  Si la utiliza AWS Organizations para administrar cuentas, designe la cuenta de GuardDuty administrador como la cuenta de administrador de Detective de la organización.
- Si utiliza Security Hub con mayor frecuencia, habilite Detective con la cuenta de administrador de Security Hub.

  Si utiliza Organizations para administrar cuentas, designe la cuenta de administrador de Security Hub como cuenta de administrador de Detective para la organización.

Si no puede utilizar las mismas cuentas de administrador en todos los servicios, puede crear un rol para varias cuentas después de habilitar Detective. Este rol concede acceso como administrador de cuenta a otras cuentas.

Para obtener información sobre cómo IAM admite este tipo de funciones, consulte Proporcionar acceso a un usuario de IAM en otra AWS cuenta de su propiedad en la Guía del usuario de IAM.

Actualización recomendada de la frecuencia de notificaciones GuardDuty CloudWatch

En GuardDuty, los detectores están configurados con una frecuencia de CloudWatch notificación de Amazon para informar de la aparición posterior de un hallazgo. Esto afecta al envío de notificaciones a Detective.

De forma predeterminada, la frecuencia es de seis horas. Con esta frecuencia, incluso si un resultado se repite muchas veces, las nuevas apariciones no se muestran en Detective hasta seis horas después.

Para reducir el tiempo que tarda Detective en recibir estas actualizaciones, recomendamos que la cuenta de GuardDuty administrador cambie la configuración de sus detectores a 15 minutos. Tenga en cuenta que cambiar la configuración no afecta al coste de uso GuardDuty.

Para obtener información sobre cómo configurar la frecuencia de las notificaciones, consulte Monitoring GuardDuty Findings with Amazon CloudWatch Events en la Guía del GuardDuty usuario de Amazon.

Habilitación de Detective

Puede habilitar Detective desde la consola de Detective, la API de Detective o la AWS Command Line Interface.

Solo se puede habilitar Detective una vez por región. Si su cuenta ya es cuenta de administrador de un gráfico de comportamiento en una región, no puede habilitar Detective de nuevo en esa región.

Console

Habilitación de Detective (consola)

1. Inicie sesión en AWS Management Console. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. Elija Comenzar.
3. En la página Activar Amazon Detective, Align cuentas de administrador (recomendado) explica la recomendación de alinear las cuentas de administrador entre Detective y Amazon GuardDuty y AWS Security Hub. Consulte the section called “Alineación recomendada con GuardDuty y AWS Security Hub”.
4. El botón Adjuntar política de IAM lo lleva directamente a la consola de IAM y abre la política recomendada. Tiene la opción de adjuntar la política recomendada al director que utilice como Detective. Si no tiene permisos para trabajar con la consola de IAM, en Permisos necesarios puede copiar el nombre de recurso de Amazon (ARN) de la política para proporcionarlo al administrador de IAM. El administrador puede asociar la política en su nombre.

   Confirme que la política de IAM necesaria esté asociada.
5. En la sección Agregar etiquetas puede agregar etiquetas al gráfico de comportamiento.

   Para añadir una etiqueta, haga lo siguiente:

   a. Elija Añadir nueva etiqueta.
   b. En Clave, escriba el nombre de la etiqueta.
   c. En Valor, escriba el valor de la etiqueta.

   Para eliminar una etiqueta, elija la opción Eliminar de la etiqueta correspondiente.
6. Elija Habilitar Amazon Detective.

7. Una vez que haya habilitado Detective, puede invitar a cuentas de miembros al gráfico de comportamiento.

   Para acceder a la página Administración de cuentas, elija Agregar miembros ahora. Para obtener información sobre cómo invitar cuentas de miembros, consulte the section called "Administración de cuentas de miembros invitadas".

Detective API, AWS CLI

Puede habilitar Amazon Detective desde la API de Detective o la AWS Command Line Interface.

Para habilitar Detective (API de Detective AWS CLI),

- API de Detective: utilice la operación `CreateGraph`.
- AWS CLI: en la línea de comandos, ejecute el comando `create-graph`.

```
aws detective create-graph --tags '{"tagName": "tagValue"}'
```

El siguiente comando habilita Detective y establece el valor de la etiqueta `Department` en `Security`.

```
aws detective create-graph --tags '{"Department": "Security"}'
```

Python script on GitHub

Puede activar Detective en todas las regiones mediante el script Detective Python de GitHub. Detective proporciona un script de código abierto GitHub que hace lo siguiente:

- Habilita Detective para una cuenta de administrador en una lista especificada de regiones.
- Agrega una lista de cuentas de miembros a cada uno de los gráficos de comportamiento.
- Envía correos electrónicos de invitación a las cuentas de miembros.
- Acepta automáticamente las invitaciones enviadas a las cuentas de miembros.

Para obtener información sobre cómo configurar y utilizar los GitHub scripts, consulte. the section called "Secuencias de comandos Python de Amazon Detective"

Comprobar que el Detective está ingiriendo datos de tu cuenta AWS

Después de activar Detective, comienza a ingerir y extraer datos de tu AWS cuenta para incluirlos en tu gráfico de comportamiento.

Para la extracción inicial, los datos suelen estar disponibles en el gráfico de comportamiento en un plazo de 2 horas.

Una buena forma de comprobar si Detective está extrayendo datos es buscar ejemplos de valores en la página Buscar de Detective.

Comprobación de ejemplos de valores en la página Buscar

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Buscar.
3. En el menú Seleccionar el tipo, elija un tipo de elemento.

   En Ejemplos de sus datos se muestra un conjunto de muestra con identificadores del tipo seleccionado que se encuentran entre los datos del gráfico de comportamiento.

   Si puede ver ejemplos de valores, esto significa que los datos se están ingiriendo y extrayendo en el gráfico de comportamiento.

Datos en un gráfico de comportamiento de un Detective

Amazon Detective permite llevar a cabo investigaciones utilizando los datos de un gráfico de comportamiento de Detective. En esta sección, puede obtener información sobre las fuentes de datos principales que se utilizan en un gráfico de comportamiento de un Detective y cómo el Detective utiliza los datos de origen para rellenarlo.

Un gráfico de comportamiento es un conjunto vinculado de datos generados a partir de los datos de origen de Detective que se ingieren de una o más cuentas de Amazon Web Services (AWS).

El gráfico de comportamiento utiliza los datos de origen para hacer lo siguiente.

- Generar una imagen general de sus sistemas y usuarios, y de las interacciones entre ellos a lo largo del tiempo
- Realizar análisis más detallados de cierta actividad para ayudarle a responder a las preguntas que surjan a medida que realiza las investigaciones
- Correlacionar recopilaciones de resultados, entidades y pruebas que puedan estar relacionados con el mismo evento o problema de seguridad.

Tenga en cuenta que toda la actividad de extracción, modelado y análisis de datos del gráfico de comportamiento tiene lugar individualmente en cada gráfico de comportamiento.

Un gráfico de comportamiento contiene datos de una o varias cuentas. Cuando una cuenta habilita Detective, se convierte en la cuenta de administrador del gráfico de comportamiento y elige las cuentas de miembros para ese gráfico. Un gráfico de comportamiento puede contener hasta 1200 cuentas de miembros. Para obtener información sobre cómo una cuenta de administrador administra las cuentas de los miembros en un gráfico de comportamiento, consulte Administrar cuentas en Detective.

Contenido

- Cómo rellena el Detective un gráfico de comportamiento
- Periodo de formación para nuevos gráficos de comportamiento de los Detectives
- Descripción general de la estructura de datos del gráfico de comportamiento
- Datos fuente utilizados en un gráfico de comportamiento de un Detective

Cómo rellena el Detective un gráfico de comportamiento

Para proporcionar los datos brutos para las investigaciones, Detective reúne datos de todo su entorno de AWS y de fuera de este, incluidos los siguientes:

- Datos de registro, incluidos Amazon Virtual Private Cloud (AmazonVPC) y AWS CloudTrail
- Hallazgos de Amazon GuardDuty
- Hallazgos de AWS Security Hub

Para obtener más información sobre los datos de origen utilizados en un gráfico de comportamiento, consulte Datos de origen utilizados en un gráfico de comportamiento.

Cómo procesa Detective los datos de origen

A medida que llegan nuevos datos, Detective utiliza una combinación de extracción y análisis para completar el gráfico de comportamiento.

Extracción de Detective

La extracción se basa en reglas de mapeo configuradas. Básicamente, una regla de mapeo dice: “Siempre que se encuentre este fragmento de datos, usarlo de esta manera específica para actualizar los datos del gráfico de comportamiento”.

Por ejemplo, un registro de datos de origen de Detective entrante podría incluir una dirección IP. Si lo hace, Detective usa la información de ese registro para crear una nueva entidad de dirección IP o actualizar una entidad de dirección IP existente.

Análisis de Detective

Los análisis son algoritmos más complejos que analizan los datos para proporcionar visibilidad de la actividad asociada a las entidades.

Por ejemplo, un tipo de análisis de Detective analiza la frecuencia con la que se produce la actividad mediante la ejecución de algoritmos. En el caso de las entidades que realizan API llamadas, el algoritmo busca las API llamadas que la entidad no utiliza normalmente. El algoritmo también busca un gran aumento en el número de API llamadas.

Las conclusiones de los análisis respaldan las investigaciones al proporcionar respuestas a preguntas clave de los analistas, y se utilizan con frecuencia para completar los paneles de perfil de resultado y de entidad.

Periodo de formación para nuevos gráficos de comportamiento de los Detectives

Una forma de investigar un resultado consiste en comparar la actividad registrada durante el rango temporal del resultado con la actividad que se produjo antes de que se detectara el resultado. Las actividades que no se han observado antes tienen más probabilidades de ser sospechosas.

Algunos paneles de perfil de Amazon Detective resaltan la actividad no observada durante el periodo de tiempo anterior al resultado. Varios paneles de perfil también muestran un valor de línea de base para mostrar la actividad promedio durante los 45 días anteriores al rango temporal. El tiempo de alcance es el resumen de la actividad de una entidad a lo largo del tiempo.

A medida que se extraen más datos al gráfico de comportamiento, Detective desarrolla una imagen más precisa de qué actividad es normal en su organización y qué actividad es inusual.

Sin embargo, para crear esta imagen, Detective necesita acceso a al menos dos semanas de datos. La madurez del análisis de Detective también aumenta con el número de cuentas que intervienen en el gráfico de comportamiento.

Las dos primeras semanas después de activar Detective se consideran un periodo de aprendizaje o entrenamiento. Durante este periodo, los paneles de perfil que comparan la actividad del rango

temporal con la actividad anterior muestran un mensaje que indica que Detective se encuentra en periodo de aprendizaje.

Durante el período de prueba, el Detective recomienda que añada tantas cuentas de miembros como pueda al gráfico de comportamiento. Esto proporciona a Detective una reserva de datos de mayor tamaño, lo que le permite generar una imagen más precisa de la actividad normal de la organización.

Descripción general de la estructura de datos del gráfico de comportamiento

La estructura de datos del gráfico de comportamiento define la estructura de los datos extraídos y analizados. También define cómo se asignan los datos de origen al gráfico de comportamiento.

Tipos de elementos de la estructura de datos del gráfico de comportamiento

La estructura de datos del gráfico de comportamiento consta de los siguientes elementos de información:

Entidad

Una entidad representa un elemento extraído de los datos de origen de Detective.

Cada entidad tiene un tipo, que identifica el tipo de objeto al que representa. Algunos ejemplos de tipos de entidades son las direcciones IP, las EC2 instancias de Amazon y AWS los usuarios.

En cada entidad, los datos de origen también se utilizan para rellenar las propiedades de la entidad. Los valores de las propiedades pueden extraerse directamente de los registros de origen o agregarse en varios registros.

Algunas propiedades consisten en un único valor escalar o agregado. Por ejemplo, para una EC2 instancia, Detective rastrea el tipo de instancia y el número total de bytes procesados.

Las propiedades de las series temporales rastrean la actividad a lo largo del tiempo. Por ejemplo, por EC2 ejemplo, Detective rastrea a lo largo del tiempo los puertos únicos que utilizó.

Relaciones

Una relación representa la actividad que se produce entre entidades individuales. Las relaciones también se extraen de los datos de origen de Detective.

Al igual que una entidad, una relación tiene un tipo que identifica los tipos de entidades implicadas y el sentido de la conexión. Un ejemplo de un tipo de relación son las direcciones IP que se conectan a EC2 instancias.

Para cada relación individual, como una dirección IP específica que se conecta a una instancia específica, Detective rastrea las apariciones a lo largo del tiempo.

Tipos de entidades de la estructura de datos del gráfico de comportamiento

La estructura de datos del gráfico de comportamiento consta de tipos de entidades y relaciones que hacen lo siguiente:

- Rastrear los servidores, las direcciones IP y los agentes de usuario utilizados
- Realice un seguimiento de los AWS usuarios, las funciones y las cuentas que se utilizan
- Rastrear las conexiones de red y las autorizaciones que se producen en su entorno de AWS

La estructura de datos del gráfico de comportamiento contiene los siguientes tipos de entidad:

AWS cuenta

AWS cuentas que están presentes en los datos de origen del Detective.

Para cada cuenta, Detective responde a varias preguntas:

- ¿Qué API llamadas ha utilizado la cuenta?
- ¿Qué agentes de usuario ha utilizado la cuenta?
- ¿Qué organizaciones del sistema autónomo (ASOs) ha utilizado la cuenta?
- ¿En qué ubicaciones geográficas ha estado activa la cuenta?

AWS rol

AWS funciones que están presentes en los datos de origen del Detective.

Para cada rol, Detective responde a varias preguntas:

- ¿Qué API llamadas ha utilizado el rol?
- ¿Qué agentes de usuario ha utilizado el rol?
- ¿Qué función ASOs ha utilizado?

- ¿En qué ubicaciones geográficas ha estado activo el rol?
- ¿Qué recursos han asumido este rol?
- ¿Qué roles ha asumido este rol?
- ¿En qué sesiones de rol ha intervenido este rol?

AWS usuario

AWS usuarios que están presentes en los datos de origen del Detective.

Para cada usuario, Detective responde a varias preguntas:

- ¿Qué API llamadas ha utilizado el usuario?
- ¿Qué agentes de usuario ha utilizado el usuario?
- ¿En qué ubicaciones geográficas ha estado activo el usuario?
- ¿Qué roles ha asumido este usuario?
- ¿En qué sesiones de rol ha intervenido este usuario?

Usuario federado

Instancias de un usuario federado. Algunos ejemplos de usuarios federados incluyen los siguientes:

- Una identidad que inicia sesión con Security Assertion Markup Language () SAML
- Una identidad que inicia sesión mediante la federación de identidades web

Para cada usuario federado, Detective responde a las siguientes preguntas:

- ¿Con qué proveedor de identidad se autenticó el usuario federado?
- ¿Cuál era la audiencia del usuario federado? La audiencia identifica la aplicación que solicitó el token de identidad web del usuario federado.
- ¿En qué ubicaciones geográficas ha estado activo el usuario federado?
- ¿Qué agentes de usuario ha utilizado el usuario federado?
- ¿Qué ASOs ha utilizado el usuario federado?
- ¿Qué roles ha asumido este usuario federado?
- ¿En qué sesiones de rol ha intervenido este usuario federado?

EC2instancia

EC2instancias que están presentes en los datos de origen del Detective.

Por ejemploEC2, el Detective responde a varias preguntas:

- ¿Qué direcciones IP se han comunicado con la instancia?
- ¿Qué puertos se han utilizado para comunicarse con la instancia?
- ¿Qué volumen de datos se ha enviado a y desde la instancia?
- ¿Qué VPC contiene la instancia?
- ¿Qué API llamadas ha utilizado la EC2 instancia?
- ¿Qué agentes de usuario ha utilizado la EC2 instancia?
- ¿Qué ASOs ha utilizado la EC2 instancia?
- ¿En qué ubicaciones geográficas ha estado activa la EC2 instancia?
- ¿Qué funciones ha asumido la EC2 instancia?

Sesión de rol

Instancias de un recurso que asume un rol. Cada sesión de rol se identifica mediante el identificador de rol y un nombre de sesión.

Para cada rol, Detective responde a varias preguntas:

- ¿Qué recursos intervinieron en esta sesión de rol? En otras palabras, ¿qué rol se asumió y qué recurso lo asumió?

  Tenga en cuenta que para asumir roles entre cuentas, Detective no puede identificar al recurso que asumió el rol.
- ¿Qué API llamadas ha utilizado la sesión de rol?
- ¿Qué agentes de usuario ha utilizado la sesión de rol?
- ¿Qué ASOs ha utilizado la sesión de rol?
- ¿En qué ubicaciones geográficas ha estado activa la sesión de rol?
- ¿Qué usuario o rol inició esta sesión de rol?
- ¿Qué sesiones de rol comenzaron a partir de esta sesión de rol?

Resultado

Hallazgos descubiertos por Amazon GuardDuty que se incluyen en los datos fuente del Detective.

Para cada resultado, Detective rastrea el tipo de resultado, el origen y la franja horaria de la actividad del resultado.

También almacena información específica del resultado, como los roles o las direcciones IP que intervienen en la actividad detectada.

Dirección IP

Direcciones IP que están presentes en los datos de origen de Detective.

Para cada dirección IP, Detective responde a varias preguntas:

- ¿Qué API llamadas ha utilizado la dirección?
- ¿Qué puertos ha utilizado la dirección?
- ¿Qué usuarios y agentes de usuario han utilizado la dirección IP?
- ¿En qué ubicaciones geográficas ha estado activa la dirección IP?
- ¿A qué EC2 instancias se ha asignado esta dirección IP y con qué se ha comunicado?

Bucket de S3

Buckets de S3 que se encuentran en los datos de origen de Detective.

Para cada bucket de S3, Detective responde a estas preguntas:

- ¿Qué entidades principales interactuaron con el bucket de S3?
- ¿Qué API llamadas se realizaron al bucket de S3?
- ¿Desde qué ubicaciones geográficas hacían los directores las API llamadas al depósito de S3?
- ¿Qué agentes de usuario se utilizaron para interactuar con el bucket de S3?
- ¿Qué ASOs se utilizó para interactuar con el depósito de S3?

Puede eliminar un bucket de S3 y, a continuación, crear uno nuevo con el mismo nombre. Como Detective usa el nombre del bucket de S3 para identificar el bucket de S3, los trata como una única entidad de bucket de S3. En el perfil de entidad, la Hora de creación es la primera hora de creación. La Hora de eliminación es la hora de eliminación más reciente.

Para ver todos los eventos de creación y eliminación, defina el rango temporal para que comience con la hora de creación y finalice con la hora de eliminación. En el panel del perfil del volumen general de API llamadas, muestra los detalles de la actividad durante el tiempo determinado. Filtra los API métodos que quieres mostrar `Create` y `Delete` los métodos. Consulte the section called “Volumen total de API llamadas”.

Agente de usuario

Agentes de usuario que están presentes en los datos de origen de Detective.

Para cada agente de usuario, Detective responde preguntas como las siguientes:

- ¿Qué API llamadas ha utilizado el agente de usuario?
- ¿Qué usuarios y roles han utilizado el agente de usuario?
- ¿Qué direcciones IP han utilizado el agente de usuario?

EKSClúster

EKSclústeres que están presentes en los datos de origen del Detective.

> **Note**
>
> Para ver los detalles completos de este tipo de entidad, la fuente de datos de los registros de EKS auditoría opcional debe estar habilitada. Para obtener más información, consulte Orígenes de datos opcionales.

Para cada EKS grupo, el Detective responde a preguntas como las siguientes:

- ¿Qué API llamadas de Kubernetes se han ejecutado en este clúster?
- ¿Qué usuarios y cuentas de servicio (sujetos) de Kubernetes están activos en este clúster?
- ¿Qué contenedores se han lanzado en este clúster?
- ¿Qué imágenes se utilizan para lanzar contenedores en este clúster?

Pod de Kubernetes

Pods de Kubernetes que están presentes en los datos de origen de Detective.

> **Note**
>
> Para ver los detalles completos de este tipo de entidad, debe estar habilitada la fuente de datos de los registros de EKS auditoría opcional. Para obtener más información, consulte Orígenes de datos opcionales.

Para cada pod, Detective responde a preguntas como las siguientes:

- ¿Qué imágenes de contenedor de este pod son comunes en mis cuentas?
- ¿Qué actividad se ha dirigido a este pod?
- ¿Qué contenedores se ejecutan en este pod?

- ¿Son habituales en mis cuentas los registros de contenedor de este pod?
- ¿Qué otros contenedores se ejecutan en los otros pods de la carga de trabajo?
- ¿Hay contenedores anómalos en este pod que no estén en los otros pods de la carga de trabajo?

Imagen de contenedor

Imágenes de contenedor que están presentes en los datos de origen de Detective.

> **Note**
>
> Para ver los detalles completos de este tipo de entidad, la fuente de datos de los registros de EKS auditoría opcional debe estar habilitada. Para obtener más información, consulte Orígenes de datos opcionales.

Para cada imagen de contenedor, Detective responde preguntas como las siguientes:

- ¿Qué otras imágenes de mi entorno comparten el mismo repositorio o registro que esta imagen?
- ¿Cuántas copias de esta imagen se están ejecutando en mi entorno?

Sujeto de Kubernetes

Sujetos de Kubernetes que están presentes en los datos de origen de Detective. Un sujeto de Kubernetes es una cuenta de usuario o de servicio.

> **Note**
>
> Para ver los detalles completos de este tipo de entidad, la fuente de datos de los registros de EKS auditoría opcional debe estar habilitada. Para obtener más información, consulte Orígenes de datos opcionales.

Para cada sujeto, Detective responde preguntas como las siguientes:

- ¿Qué IAM directores se han autenticado como este sujeto?
- ¿Qué resultados están asociados a este sujeto?
- ¿Qué direcciones IP utiliza el sujeto?

Datos fuente utilizados en un gráfico de comportamiento de un Detective

Para rellenar un gráfico de comportamiento, Amazon Detective utiliza datos de origen de la cuenta de administrador del gráfico de comportamiento y de las cuentas de miembro.

Con Detective, puede acceder a datos de eventos históricos de hasta un año de antigüedad. Estos datos están disponibles a través de un conjunto de visualizaciones que muestran los cambios en el tipo y el volumen de actividad durante un intervalo de hora seleccionado. El Detective relaciona estos cambios con los GuardDuty hallazgos.

Para obtener más información sobre la estructura de datos del gráfico de comportamiento, consulte Descripción general de la estructura de datos del gráfico de comportamiento en la Guía del usuario de Detective.

Tipos de orígenes de datos principales en Detective

El Detective ingiere datos de estos tipos de AWS registros:

- AWS CloudTrail registros
- Registros de flujo de Amazon Virtual Private Cloud (AmazonVPC)
  - Ingiere ambos IPv4 IPv6 registros, pero no los MAC registros producidos por los adaptadores de Elastic Fabric.

  - Ingesta los registros de registro cuando el valor del `log-status` campo está en `OK` estado. Para obtener más información, consulta Registros de registro de flujo en la Guía del VPC usuario de Amazon.
  - Ingiere los registros de flujo producidos por las instancias de Amazon Elastic Compute Cloud que se ejecutan VPCs únicamente en esas instancias. No se utilizan otros recursos, como NAT puertas de enlace, RDS instancias o clústeres de Fargate.
  - Ingiere el tráfico aceptado y el rechazado.
- En el caso de las cuentas en las que están inscritas GuardDuty, Detective también ingiere GuardDuty los hallazgos.

Detective consume CloudTrail y VPC registra los eventos mediante flujos y registros de VPC flujo independientes CloudTrail y duplicados. Estos procesos no afectan ni utilizan las configuraciones existentes ni CloudTrail las de registro VPC de flujo. Tampoco afectan al rendimiento de estos servicios ni aumentan sus costos.

Tipos de orígenes de datos opcionales en Detective

Detective ofrece paquetes fuente opcionales además de las tres fuentes de datos que se ofrecen en el paquete principal de Detective (el paquete principal incluye AWS CloudTrail registros, registros de VPC flujo y GuardDuty hallazgos). Se puede iniciar o detener un paquete de orígenes de datos opcional para un determinado gráfico de comportamiento en cualquier momento.

Detective ofrece una prueba gratuita de 30 días para todos los paquetes de orígenes básicos y opcionales por región.

> **Note**
>
> Detective retiene todos los datos recibidos de cada paquete de orígenes de datos durante un máximo de 1 año.

Actualmente están disponibles los siguientes paquetes de orígenes opcionales:

- Registros de auditoría de EKS

  Este paquete de fuentes de datos opcional permite a Detective ingerir información detallada sobre EKS los clústeres de su entorno y añadir esos datos a su gráfico de comportamiento. Detective correlaciona las actividades de los usuarios con los eventos de AWS CloudTrail administración y

la actividad de la red con Amazon VPC Flow Logs sin necesidad de habilitar o almacenar estos registros manualmente. Para obtener más información, consulte Registros EKS de auditoría de Amazon.

- AWS hallazgos de seguridad

  Este paquete de orígenes de datos opcionales permite a Detective ingerir datos de Security Hub, y añade esos datos a su gráfico de comportamiento. Para obtener más información, consulte AWS hallazgos de seguridad.

Iniciar o detener un origen de datos opcional:

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, en Configuración, elija General.
3. En Paquetes de orígenes opcionales, seleccione Actualizar. A continuación, seleccione el origen de datos que desea habilitar, o anule la sección de la casilla de un origen de datos ya habilitado y elija Actualizar para cambiar los paquetes de orígenes de datos que están habilitados.

> **Note**
>
> Si detiene y luego reinicia un origen de datos opcional, verá una brecha en los datos que se muestran en algunos perfiles de entidad. Esta brecha aparecerá en la pantalla de la consola y representará el periodo de tiempo durante el cual se detuvo el origen de datos. Cuando se reinicia un origen de datos, Detective no ingiere datos con carácter retroactivo.

Registros EKS de auditoría de Amazon

Los registros de EKS auditoría de Amazon son un paquete de fuentes de datos opcional que se puede añadir al gráfico de comportamiento de un Detective. Puede ver los paquetes fuente opcionales disponibles y su estado en su cuenta, desde la página de configuración de la consola o a través del DetectiveAPI.

Se ofrece una prueba gratuita de 30 días para este origen de datos. Para obtener más información, consulte Versión de prueba gratuita para orígenes de datos opcionales.

Al habilitar los registros de EKS auditoría de Amazon, Detective puede añadir información detallada sobre los recursos creados con Amazon EKS a su gráfico de comportamiento. Esta fuente de

datos mejora la información proporcionada sobre los siguientes tipos de entidades: EKS Cluster, Kubernetes Pod, Container Image y Kubernetes subject.

Además, si has habilitado los registros de EKS auditoría como fuente de datos en Amazon, GuardDuty podrás ver los detalles de los hallazgos de Kubernetes en. GuardDuty Para obtener más información sobre cómo habilitar esta fuente de datos, GuardDuty consulte Protección de Kubernetes en Amazon. GuardDuty

> **Note**
>
> Este origen de datos está habilitado de forma predeterminada para los gráficos de comportamiento nuevos creados después del 26 de julio de 2022. Para los gráficos de comportamiento creados antes del 26 de julio de 2022, deberá habilitarse manualmente.

Añadir o eliminar los registros EKS de auditoría de Amazon como fuente de datos opcional:

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, en Configuración, elija General.
3. En Paquetes fuente, seleccione los registros de EKS auditoría para habilitar esta fuente de datos. Si ya está habilitada, selecciónela de nuevo para dejar de incluir los registros de EKS auditoría en su gráfico de comportamiento.

AWS hallazgos de seguridad

AWS security findings es un paquete de fuentes de datos opcional que se puede añadir al gráfico de comportamiento de un Detective.

Puede ver los paquetes fuente opcionales disponibles y su estado en su cuenta, desde la página de configuración de la consola o a través del DetectiveAPI.

Se ofrece una prueba gratuita de 30 días para este origen de datos. Para obtener más información, consulte Versión de prueba gratuita para orígenes de datos opcionales.

Al habilitar los hallazgos de AWS seguridad, Detective puede utilizar los hallazgos del Security Hub agregados por el Security Hub de los servicios principales en un formato de hallazgos estándar denominado AWS Security Format (ASFF), lo que elimina la necesidad de realizar esfuerzos de conversión de datos que consumen mucho tiempo. A continuación, correlaciona los resultados ingeridos en los distintos productos para priorizar los más importantes.

Añadir o eliminar los datos AWS de seguridad como fuente de datos opcional:

> **Note**
>
> La fuente de datos sobre los hallazgos de AWS seguridad está habilitada de forma predeterminada para los nuevos gráficos de comportamiento creados después del 16 de mayo de 2023. En el caso de los gráficos de comportamiento creados antes del 16 de mayo de 2023, debe habilitarse manualmente.

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, en Configuración, elija General.
3. En Paquetes fuente, seleccione los resultados AWS de seguridad para habilitar esta fuente de datos. Si ya está habilitada, selecciónela de nuevo para dejar de incluir los resultados del AWS Security Finding Format (ASFF) en su gráfico de comportamiento.

Resultados admitidos actualmente

Detective ingiere todos los ASFF hallazgos de Security Hub de los servicios que son propiedad de Amazon o AWS.

- Para ver la lista de integraciones de servicios compatibles, consulta las integraciones de AWSservicios disponibles en la Guía del AWS Security Hub usuario.
- Para ver la lista de recursos admitidos, consulte Recursos en la Guía del usuario de AWS Security Hub .
- AWS No se incorporan las conclusiones de servicios cuyo estado de conformidad no esté `FAILED` establecido ni las conclusiones agregadas entre regiones.

Cómo Detective ingiere y almacena datos de origen

Cuando Detective está habilitado, comienza a ingerir datos de origen de la cuenta de administrador del gráfico de comportamiento. A medida que se añaden cuentas de miembro al gráfico de comportamiento, Detective también comienza a usar los datos de dichas cuentas de miembro.

Los datos de origen de Detective consisten en versiones estructuradas y procesadas de las fuentes originales. Para respaldar el análisis de Detective, Detective almacena copias de los datos de origen de Detective.

El proceso de ingesta de Detective alimenta datos en buckets de Amazon Simple Storage Service (Amazon S3) en el almacén de datos de origen de Detective. A medida que llegan nuevos datos de origen, otros componentes de Detective recogen los datos e inician los procesos de extracción y análisis. Para obtener más información, consulte Cómo Detective usa los datos de origen para rellenar un gráfico de comportamiento en la Guía del usuario de Detective.

Cómo aplica Detective la cuota de volumen de datos a los gráficos de comportamiento

Detective aplica cuotas estrictas en cuanto al volumen de datos que permite en cada gráfico de comportamiento. El volumen de datos es la cantidad de datos diarios que fluyen al gráfico de comportamiento de Detective.

Detective aplica estas cuotas cuando una cuenta de administrador habilita Detective, y cuando una cuenta de miembro acepta una invitación para contribuir a un gráfico de comportamiento.

- Si el volumen de datos de una cuenta de administrador supera los 10 TB diarios, la cuenta de administrador no podrá habilitar Detective.
- Si el volumen de datos agregado de una cuenta de miembro hace que el gráfico de comportamiento supere los 10 TB diarios, la cuenta de miembro no se podrá habilitar.

El volumen de datos de un gráfico de comportamiento también puede aumentar de forma natural a lo largo del tiempo. Detective comprueba el volumen de datos del gráfico de comportamiento todos los días para asegurarse de que no supere la cuota.

Si el volumen de datos del gráfico de comportamiento se aproxima a la cuota, Detective muestra un mensaje de advertencia en la consola. Para evitar superar la cuota, puede eliminar cuentas de miembro.

Si el volumen de datos de un gráfico de comportamiento supera los 10 TB diarios, no podrá añadir nuevas cuentas de miembro al gráfico de comportamiento.

Si el volumen de datos del gráfico de comportamiento supera los 15 TB diarios, Detective detiene la ingesta de datos al gráfico de comportamiento. La cuota de 15 TB diarios refleja tanto el volumen de datos normal como los picos en el volumen de datos. Cuando se alcanza esta cuota, no se ingieren datos nuevos al gráfico de comportamiento, pero tampoco se eliminan los datos existentes. Puede seguir usando esos datos históricos con fines de investigación. La consola muestra un mensaje para indicar que se ha suspendido la ingesta de datos para el gráfico de comportamiento.

Si se suspende la ingesta de datos, debe trabajar Soporte para volver a habilitarla. Si es posible, antes de contactar Soporte, intenta eliminar las cuentas de los miembros para que el volumen de datos esté por debajo de la cuota. Esto facilita la rehabilitación de la ingesta de datos para el gráfico de comportamiento.

Uso del panel de resumen de Detective

Utilice el panel de resumen de Amazon Detective para identificar entidades e investigar el origen de la actividad durante las últimas 24 horas. El panel Resumen de Amazon Detective le ayuda a identificar las entidades asociadas a tipos específicos de actividad inusual. Es uno de los diferentes puntos de partida posibles de una investigación.

Para mostrar el panel de resumen, en el panel de navegación de Detective, seleccione Resumen. El panel Resumen también se muestra de forma predeterminada cuando se abre por primera vez la consola de Detective.

En el panel de resumen, puede identificar las entidades que cumplen los siguientes criterios:

- Investigaciones que muestran posibles eventos de seguridad identificados por Detective
- Entidades implicadas en una actividad que tuvo lugar en geolocalizaciones observadas recientemente
- Entidades que realizaron el mayor número de API llamadas
- EC2instancias que tuvieron el mayor volumen de tráfico
- Clústeres de contenedor que presentaron el mayor número de contenedores

Desde cada panel del panel de resumen, puede pasar al perfil de la entidad seleccionada.

Al revisar el panel de resumen, puede ajustar el tiempo de alcance para ver la actividad de cualquier período de 24 horas de los 365 días anteriores. Al cambiar la Fecha y hora de inicio, la Fecha y hora de finalización se actualizan automáticamente a 24 horas después de la hora de inicio elegida.

Con Detective, puede acceder a datos de eventos históricos de hasta un año de antigüedad. Estos datos están disponibles a través de un conjunto de visualizaciones que muestran los cambios en el tipo y el volumen de actividad durante un intervalo de hora seleccionado. El Detective relaciona estos cambios con los GuardDuty hallazgos.

Para obtener más información sobre los datos de origen en Detective, consulte Datos de origen utilizados en un gráfico de comportamiento.

Investigaciones

Investigaciones que muestran posibles eventos de seguridad identificados por Detective. En el panel Investigaciones, puede ver las investigaciones críticas y los roles y usuarios correspondientes

de AWS que se han visto afectados por eventos de seguridad durante un período de tiempo determinado. Las investigaciones agrupan los indicadores de riesgo para ayudar a determinar si un AWS recurso está involucrado en una actividad inusual que podría indicar un comportamiento malicioso y su impacto.

Seleccione Ver todas las investigaciones para revisar los resultados y clasificar los grupos de resultados y los detalles de los recursos con el fin de acelerar la investigación de seguridad. Las investigaciones se muestran en función del tiempo de alcance seleccionado. Puede ajustar el tiempo del alcance para ver las investigaciones en un período de 24 horas en los 365 últimos días. Puede pasar directamente a Investigaciones críticas para ver un informe detallado de la investigación.

Si identificas un AWS rol o un usuario que parece tener una actividad sospechosa, puedes pasar directamente del panel de investigaciones al rol o usuario para continuar con la investigación. Seleccione un rol o un usuario y haga clic en Ejecutar investigación para generar un informe de la investigación. Tras realizar una investigación sobre un rol o un usuario, dicho rol o usuario pasa a la pestaña Investigado.

Geolocalizaciones recién observadas

Geolocalizaciones recién observadas destaca las ubicaciones geográficas que fueron el origen de la actividad durante las 24 horas anteriores, pero que no se observaron durante el periodo de línea base anterior.

El panel incluye hasta 100 geolocalizaciones. Las ubicaciones están marcadas en el mapa y se enumeran en la tabla que hay bajo el mapa.

Para cada geolocalización, la tabla muestra el número de API llamadas fallidas y satisfactorias realizadas desde esa geolocalización durante las últimas 24 horas.

Puede ampliar cada geolocalización para mostrar la lista de usuarios y roles que realizaron llamadas desde esa geolocalización. API Para cada entidad principal, la tabla muestra el tipo y la Cuenta de AWS asociada.

Si identifica un usuario o un rol que le parezca sospechoso, puede pasar directamente del panel al perfil del usuario o rol para continuar con la investigación. Para pasar a un perfil, elija el identificador de usuario o rol.

El Detective determina la ubicación de las solicitudes mediante bases de datos de MaxMind GeoIP. MaxMind informa que sus datos son muy precisos a nivel de país, aunque la precisión varía según factores como el país y el tipo de IP. Para obtener más información MaxMind, consulte

Geolocalización MaxMind IP. Si cree que alguno de los datos de GeoIP es incorrecto, puede enviar una solicitud de corrección a Maxmind en MaxMind Correct Geo Data. IP2

Grupos de resultados activos en los últimos 7 días

Grupos de resultados activos en los últimos 7 días muestra agrupaciones correlacionadas de resultados, entidades y evidencias de Detective en su entorno que se produjeron durante un periodo de tiempo determinado. Estas agrupaciones correlacionan actividades inusuales que podrían ser indicio de un comportamiento malintencionado. El panel de resumen muestra hasta cinco grupos ordenados por los grupos que contienen los hallazgos más importantes que estuvieron activos en la última semana.

Puede seleccionar valores en el contenido Táctica, Cuenta, Recuerdo y Resultados para acceder a información más detallada.

Los grupos de resultados se generan diariamente. Si identifica un grupo de resultados de interés, puede seleccionar el título para acceder a una vista detallada del perfil del grupo y continuar con la investigación.

Funciones y usuarios con mayor volumen de API llamadas

Los roles y usuarios con el mayor volumen de API llamadas identifican a los usuarios y roles que han realizado el mayor número de API llamadas durante las últimas 24 horas.

El panel puede incluir hasta 100 usuarios y roles. Para cada usuario o rol, puede ver el tipo (usuario o rol) y la cuenta asociada. También puedes ver el número de API llamadas emitidas por ese usuario o rol durante las últimas 24 horas.

De forma predeterminada, se muestran los roles vinculados a servicios. Los roles vinculados al servicio pueden generar grandes volúmenes de AWS CloudTrail actividad, lo que desplaza a los directores que se desean investigar más a fondo. Puede optar por desactivar Mostrar funciones vinculadas al servicio para filtrar las funciones vinculadas al servicio desde la vista de resumen del panel de control.

Puede exportar un archivo de valores separados por comas (.csv) que contenga los datos de este panel.

También hay un cronograma del volumen de API llamadas de los 7 días anteriores. El cronograma puede ayudarte a determinar si el volumen de API llamadas es inusual para ese director.

Si identificas un usuario o un rol cuyo volumen de API llamadas parece sospechoso, puedes pasar directamente del panel al perfil de usuario o rol para continuar con la investigación. También puede ver el perfil de la cuenta asociada al usuario o rol. Para ver un perfil, elija el usuario, el rol o el identificador de cuenta.

EC2instancias con el mayor volumen de tráfico

EC2las instancias con el mayor volumen de tráfico identifican las EC2 instancias que han tenido el mayor volumen total de tráfico durante las últimas 24 horas.

El panel puede incluir hasta 100 EC2 instancias. Para cada EC2 instancia, puede ver la cuenta asociada y el número de bytes entrantes, salientes y totales de las últimas 24 horas.

Puede exportar un archivo de valores separados por comas (.csv) que contenga los datos de este panel.

También puede ver una cronología que muestre el tráfico entrante y saliente de los últimos 7 días. El cronograma puede ayudar a determinar si el volumen de tráfico es inusual en esa EC2 instancia.

Si identificas una EC2 instancia con un volumen de tráfico sospechoso, puedes ir directamente del panel al perfil de la EC2 instancia para continuar con la investigación. También puedes ver el perfil de la cuenta propietaria de la EC2 instancia. Para ver un perfil, elige el identificador de la EC2 instancia o de la cuenta.

Clústeres de contenedor con mayor número de pods de Kubernetes

Clústeres de contenedor con mayor número de pods de Kubernetes creados identifica los clústeres en los que se han ejecutado más contenedores en las últimas 24 horas.

Este panel incluye hasta 100 clústeres organizados por aquellos que contienen más resultados asociados. Para cada clúster, puede ver la cuenta asociada, el número actual de contenedores del clúster y el número de resultados asociados al clúster en las últimas 24 horas. Puede exportar un archivo de valores separados por comas (.csv) que contenga los datos de este panel.

Si identifica un clúster con resultados recientes, puede pasar directamente del panel al perfil del clúster para continuar con la investigación. También puede cambiar al perfil de la cuenta propietaria del clúster. Para cambiar a un perfil, elija el nombre del clúster o el identificador de la cuenta.

Notificación de valor aproximado

En los roles y los usuarios con el mayor volumen de API llamadas y las EC2 instancias con el mayor volumen de tráfico, si un valor va seguido de un asterisco (*), significa que el valor es una aproximación. El valor verdadero es igual o mayor que el valor mostrado.

Esto se debe al método que utiliza Detective para calcular el volumen de cada intervalo de tiempo. En la página Resumen, el intervalo de tiempo es de una hora.

Para cada hora, Detective calcula el volumen total de los 1000 usuarios, roles o EC2 instancias con el mayor volumen. Excluye los datos de los usuarios, funciones o EC2 instancias restantes.

Si un recurso estaba a veces entre los 1000 primeros y otras no, es posible que el volumen calculado para ese recurso no incluya todos los datos. Se excluyen los datos de los intervalos de tiempo en los que no estaba entre los 1000 primeros.

Tenga en cuenta que esto se aplica solo a la página Resumen. El perfil del usuario, rol o EC2 instancia proporciona detalles precisos.

Cómo usar Detective con fines de investigación

Amazon Detective ayuda a analizar, investigar e identificar rápidamente la causa raíz de un resultado de seguridad o actividad sospechosa. Detective proporciona herramientas para apoyar el proceso general de investigación. En Detective, una investigación puede comenzar a partir de un resultado, un grupo de resultados o una entidad.

Fases de investigación en Detective

Cualquier proceso de investigación de un Detective implica las siguientes fases:

Triaje

El proceso de investigación comienza cuando se le informe de una instancia sospechosa de actividad malintencionada o de alto riesgo. Por ejemplo, se le asigna la tarea de analizar los hallazgos o alertas descubiertos por servicios como Amazon GuardDuty y Amazon Inspector.

En la fase de triaje, debe determinar si la actividad es un positivo real (actividad realmente malintencionada) o un falso positivo (no es una actividad malintencionada ni de alto riesgo). Los perfiles de Detective respaldan el proceso de triaje al proporcionar información sobre la actividad de la entidad implicada.

En el caso de los positivos reales, se avanza a la siguiente fase.

Determinación del alcance

Durante la fase de determinación del alcance, los analistas determinan el alcance de la actividad malintencionada o de alto riesgo y la causa subyacente.

La determinación del alcance responde a los siguientes tipos de preguntas:

- ¿Qué sistemas y usuarios se han visto comprometidos?
- ¿Dónde se originó el ataque?
- ¿Cuánto tiempo ha durado el ataque?
- ¿Hay alguna otra actividad relacionada que descubrir? Por ejemplo, si un atacante está extrayendo datos del sistema, ¿cómo los obtuvo?

Las visualizaciones de Detective pueden ayudarle a identificar otras entidades que han estado implicadas o afectadas.

Respuesta

El último paso consiste en responder al ataque para detenerlo, minimizar el daño y evitar que se repitan ataques similares.

Puntos de partida para una investigación de Detectives

Cada investigación en Detective tiene un punto de partida esencial. Por ejemplo, es posible que se te asigne un Amazon GuardDuty o un AWS Security Hub hallazgo para investigar. O puede que le preocupe cierta actividad inusual en una determinada dirección IP.

Los puntos de partida típicos de una investigación incluyen los hallazgos detectados GuardDuty y las entidades extraídas de los datos de origen del Detective.

Los hallazgos detectados por GuardDuty

GuardDuty utiliza sus datos de registro para descubrir posibles casos de actividad maliciosa o de alto riesgo. Detective proporciona recursos que ayudan a investigar estos resultados.

Para cada resultado, Detective proporciona los detalles relacionados. El Detective también muestra las entidades, como las direcciones IP y AWS las cuentas, que están conectadas al hallazgo.

A continuación, puede examinar la actividad de las entidades implicadas para determinar si la actividad detectada a partir del resultado es realmente motivo de preocupación.

Para obtener más información, consulte the section called “Descripción general del resultado”.

AWS hallazgos de seguridad agregados por Security Hub

AWS Security Hub agrupa los hallazgos de seguridad de varios proveedores de hallazgos en un solo lugar y le proporciona una visión completa del estado de su seguridad. AWS Security Hub elimina la complejidad que supone abordar grandes volúmenes de resultados de varios proveedores. Reduce el esfuerzo necesario para administrar y mejorar la seguridad de todas sus AWS cuentas, recursos y cargas de trabajo. Detective proporciona recursos que ayudan a investigar estos resultados.

Para cada resultado, Detective proporciona los detalles relacionados. El Detective también muestra las entidades, como las direcciones IP y AWS las cuentas, que están conectadas al hallazgo.

Para obtener más información, consulte the section called “Descripción general del resultado”.

Entidades extraídas de los datos de origen de Detective

A partir de la ingesta de datos de origen de Detective, el servicio extrae entidades tales como direcciones IP y usuarios de AWS . Puede usar una de ellas como punto de partida de la investigación.

Detective proporciona detalles generales sobre la entidad, como la dirección IP o el nombre de usuario. También proporciona detalles sobre el historial de actividad. Por ejemplo, Detective puede informar qué otras direcciones IP ha utilizado o con qué otras direcciones IP ha establecido (recibido o enviado) conexiones una entidad.

Para obtener más información, consulte Analizando entidades.

Flujo de investigación de Detectives

Puedes usar Amazon Detective para investigar una entidad, como una EC2 instancia o un AWS usuario. También puede investigar los resultados de seguridad.

En un nivel alto, la siguiente imagen muestra el proceso de una Investigación de Detectives.

Paso 1: selección de la entidad que se va a investigar

Al analizar un hallazgo GuardDuty, los analistas pueden optar por investigar una entidad asociada en Detective. Consulte the section called “Pasar desde otra consola”.

Al seleccionar la entidad, se accede al perfil de la entidad en Detective.

Paso 2: análisis de las visualizaciones de los perfiles

Cada perfil de entidad contiene un conjunto de visualizaciones que se generan a partir del gráfico de comportamiento. El gráfico de comportamiento se crea a partir de los archivos de registro y otros datos introducidos en Detective.

Las visualizaciones muestran la actividad relativa a una entidad. Estas visualizaciones se utilizan para responder preguntas con el fin de determinar si la actividad de la entidad es inusual. Consulte Analizando entidades.

Para ayudar a orientar la investigación, puede usar las directrices de Detective que se proporcionan con cada visualización. La guía describe la información que se muestra, sugiere preguntas que se pueden formular y propone los próximos pasos en función de las respuestas. Consulte the section called “Usar las directrices de los paneles de perfil”.

Cada perfil contiene una lista de los resultados asociados. Puede ver los detalles y la descripción general de un resultado. Consulte the section called “Ver los resultados de una entidad”.

Desde un perfil de una entidad, puede pasar a otros perfiles de entidad y de resultados para investigar más a fondo la actividad de los recursos relacionados.

Paso 3: Tomar medidas

Tome las medidas oportunas en función de los resultados de su investigación.

Si se trata de un resultado falso positivo, puede archivar el resultado. Desde Detective, puede archivar GuardDuty los hallazgos. Para obtener más información, consulta Archivar un GuardDuty hallazgo de Amazon.

De lo contrario, tome las medidas oportunas para abordar la vulnerabilidad y mitigar los daños. Por ejemplo, quizás necesite actualizar la configuración de un recurso.

Investigación de Detectives

Puede utilizar Amazon Detective Investigation para investigar a IAM los usuarios y las IAM funciones mediante indicadores de compromiso, que pueden ayudarle a determinar si un recurso está implicado en un incidente de seguridad. Un indicador de peligro (IOC) es un artefacto observado en o sobre una red, un sistema o un entorno que puede (con un alto nivel de confianza) identificar una actividad maliciosa o un incidente de seguridad. Con Detective Investigations, puede maximizar la eficiencia, centrarse en las amenazas a la seguridad y reforzar las capacidades de respuesta a los incidentes.

Detective Investigation utiliza modelos de aprendizaje automático e inteligencia de amenazas para analizar automáticamente los recursos de su AWS entorno e identificar posibles incidentes de seguridad. Le permite utilizar de forma proactiva, efectiva y eficiente la automatización basada en el gráfico de comportamiento de Detective para mejorar las operaciones de seguridad. Con Detective Investigation puedes investigar las tácticas de ataque, los viajes imposibles, las direcciones IP marcadas y la búsqueda de grupos. Realiza los pasos iniciales de la investigación de seguridad y genera un informe en el que se destacan los riesgos identificados por Detective para ayudar a comprender los eventos de seguridad y responder a posibles incidentes.

Temas

- Llevar a cabo una investigación de Detectives
- Revisión de los informes de Investigaciones de Detectives
- Comprensión de un informe de Investigaciones de Detectives
- Resumen del informe de Investigaciones de Detectives
- Descarga de un informe de Investigaciones de Detectives
- Archivar un informe de Investigaciones de Detectives

Llevar a cabo una investigación de Detectives

Utilice Run investigation para analizar recursos, como IAM los usuarios y las IAM funciones, y para generar un informe de investigación. El informe generado detalla el comportamiento anómalo que indica un posible compromiso.

Console

Sigue estos pasos para ejecutar una investigación detectivesca desde la página de Investigaciones con la consola Amazon Detective.

1. Inicie sesión en la consola AWS de administración. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Investigaciones.
3. En la página de investigaciones, selecciona Ejecutar una investigación en la esquina superior derecha.
4. En la sección Seleccionar un recurso, tienes tres formas de llevar a cabo una investigación. Puede optar por llevar a cabo la investigación para obtener un recurso recomendado por el Detective. Puedes ejecutar la investigación para un recurso específico. También puede investigar un recurso desde la página Búsqueda de Detective.

   1. `Choose a recommended resource`— El Detective recomienda recursos en función de su actividad de búsqueda y búsqueda de grupos. Para ejecutar la investigación de un recurso recomendado por el Detective, en la tabla Recursos recomendados, seleccione el recurso que desee investigar.

      La tabla Recursos recomendados proporciona los siguientes detalles:

      - Recurso ARN: el nombre del recurso de Amazon (ARN) del AWS recurso.
      - Motivo para investigar: muestra los motivos principales para investigar el recurso. Los motivos por los que Detective recomienda investigar un recurso son los siguientes:
        - Si un recurso ha estado implicado en un resultado de gravedad alta en las 24 últimas horas.
        - Si un recurso ha estado implicado en un grupo de resultados observado en los 7 últimos días. Los grupos de resultados de Detective le permiten examinar varias actividades en relación con un posible evento de seguridad. Para obtener más información, consulte the section called “Búsqueda de grupos”.
        - Si un recurso ha estado implicado en un resultado en los 7 últimos días.
      - Resultado más reciente: los resultados más recientes se ordenan por prioridad en la parte superior de la lista.
      - Tipo de recurso: identifica el tipo de recurso. Por ejemplo, un AWS usuario o un AWS rol.

   2. `Specify an AWS role or user with an ARN`— Puede seleccionar un AWS rol o un AWS usuario y realizar una investigación para el recurso específico.

      Siga estos pasos para investigar un tipo de recurso específico.

      a. En la lista desplegable Seleccione el tipo de recurso, elija el AWS rol o AWS el usuario.

b. Introduzca el recurso ARN del IAM recurso. Para obtener más información sobre ResourceARNs, consulte Amazon Resource Names (ARNs) en la Guía del IAM usuario.

3. `Find a resource to investigate from the Search page`— Puedes buscar todos tus IAM recursos en la página de Búsqueda de Detectives.

   Sigue estos pasos para investigar un recurso desde la página de búsqueda.

   a. En el panel de navegación, elija Buscar.

   b. En la página de búsqueda, busque un IAM recurso.

   c. Ve a la página de perfil del recurso y realiza una investigación desde allí.

5. En la sección Tiempo del alcance de la investigación, elija el tiempo del alcance de la investigación para evaluar la actividad del recurso seleccionado. Puede seleccionar una fecha de inicio y una hora de inicio, y una fecha de finalización y una hora de finalización en UTC este formato. El intervalo de tiempo del rango seleccionado puede oscilar entre un mínimo de 3 horas y un máximo de 30 días.

6. Seleccione Ejecutar investigación.

API

Para ejecutar una investigación mediante programación, utilice la StartInvestigationoperación del Detective. API Para ejecutar una investigación con el comando AWS Command Line Interface (AWS CLI) ejecute el comando start-investigation.

En la solicitud, utilice estos parámetros para ejecutar una investigación en Detective:

- `GraphArn`— Especifique el nombre del recurso de Amazon (ARN) del gráfico de comportamiento.
- `EntityArn`— Especifique el nombre único del recurso de Amazon (ARN) del IAM usuario y el IAM rol.
- `ScopeStartTime`: opcionalmente, especifique la fecha y la hora para comenzar la investigación. El valor es una cadena con formato UTC ISO86 01. Por ejemplo, `2021-08-18T16:35:56.284Z`.
- `ScopeEndTime`: opcionalmente, especifique la fecha y la hora para finalizar la investigación. El valor es una cadena con formato UTC ISO86 01. Por ejemplo, `2021-08-18T16:35:56.284Z`.

Este ejemplo está formateado para Linux, macOS o Unix y utiliza el carácter de barra invertida (\) de continuación de línea para mejorar la legibilidad.

```
aws detective start-investigation \
--graph-arn arn:aws:detective:us-
east-1:123456789123:graph:fdac8011456e4e6182facb26dfceade0
 --entity-arn arn:aws:iam::123456789123:role/rolename --scope-start-
time 2023-09-27T20:00:00.00Z
--scope-end-time 2023-09-28T22:00:00.00Z
```

También puede ejecutar una investigación desde las siguientes páginas de Detective:

- Una página de perfil de IAM usuario o IAM rol en Detective.
- Panel de visualización de gráficos de un grupo de resultados.
- Columna de acciones de un recurso implicado.
- IAMusuario o IAM rol en una página de búsqueda.

Cuando Detective ejecuta la investigación de un recurso, se genera un informe de investigación. Para acceder al informe, vaya a Investigaciones desde el panel de navegación.

Revisión de los informes de Investigaciones de Detectives

Los informes de las investigaciones permiten revisar los informes generados para comprobar si hay investigaciones que haya realizado anteriormente en Detective.

Para revisar los informes de las investigaciones

1. Inicie sesión en la consola AWS de administración. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Investigaciones.

Tome nota de los siguientes atributos de un informe de investigación.

- ID: identificador generado del informe de investigación. Puede elegir este ID para leer un resumen del informe de investigación, que contiene los detalles de la investigación.
- Estado: cada investigación está asociada a un Estado en función del estado de finalización de la investigación. Los valores de estado pueden ser En curso, Correcto o Error.

- Gravedad: se asigna una Gravedad a cada investigación. Detective asigna automáticamente la gravedad del resultado.

  La gravedad representa la disposición analizada mediante la investigación de un solo recurso en un rango temporal determinado. La gravedad que indica una investigación no refleja de ningún modo la importancia o la gravedad que pueda tener un recurso afectado para su organización.

  Los valores de gravedad de la investigación pueden ser, de mayor a menor gravedad, Crítica, Alta, Media, Baja o Informativa.

  Se debe dar prioridad a las investigaciones a las que se asigne un valor de gravedad Crítica o Alta para su posterior inspección, ya que es más probable que representen problemas de seguridad de alto impacto identificados por Detective.
- Entidad: la columna Entidad contiene detalles sobre las entidades específicas detectadas en la investigación. Algunas entidades son AWS cuentas, como el usuario y el rol.
- Estado: la columna de fecha de Creación contiene detalles sobre la fecha y la hora en que se creó por primera vez el informe de investigación.

Comprensión de un informe de Investigaciones de Detectives

Un informe de Investigaciones de Detectives incluye un resumen del comportamiento poco común o la actividad maliciosa que indica un compromiso. También indica las recomendaciones que sugiere Detective para mitigar el riesgo de seguridad.

Para ver un informe de investigación con un ID de investigación específico.

1. Inicie sesión en la consola AWS de administración. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Investigaciones.
3. En la tabla Informes, seleccione un ID de investigación.

Detective genera el informe para el tiempo y el rango temporal y el Usuario seleccionados. El informe contiene una sección sobre Indicadores de riesgo con detalles sobre uno o varios de los indicadores de riesgo que figuran a continuación. Al revisar cada indicador de riesgo, si lo desea, puede elegir un elemento para desglosarlo y revisar sus detalles.

- Tácticas. Técnicas y procedimientos: identifica las tácticas, las técnicas y los procedimientos (TTPs) utilizados en un posible incidente de seguridad. El marco MITRE ATT &CK se utiliza para comprender elTTPs. Las tácticas se basan en la matriz MITRE ATT &CK para empresas.
- Direcciones IP marcadas por inteligencia de amenazas: las direcciones IP sospechosas se marcan e identifican como amenazas críticas o graves en función de la inteligencia de amenazas de Detective.
- Viaje imposible: detecta e identifica actividades inusuales e imposibles del usuario en una cuenta. Por ejemplo, este indicador muestra un cambio drástico entre la ubicación de origen y la de destino de un usuario en un breve periodo de tiempo.
- Grupo de resultados relacionados: muestra varias actividades relacionadas con un posible evento de seguridad. Para abordar este problema, Detective utiliza técnicas de análisis gráfico que infiere relaciones entre resultados y entidades, y las agrupa como grupo de resultados.
- Resultados relacionados: actividades relacionadas asociadas con un posible evento de seguridad. Muestra todas las categorías distintas de evidencia que están relacionadas con el recurso o el grupo de resultados.
- Nuevas geolocalizaciones: identifica las nuevas geolocalizaciones utilizadas en el nivel de recurso o de cuenta. Por ejemplo, este indicador muestra una geolocalización observada que es poco frecuente o no utilizada en función de la actividad anterior del usuario.
- Nuevos agentes de usuario: identifica los nuevos agentes de usuario que se utilizan en el nivel de recurso o de cuenta.

- Nuevo ASOs: identifica las nuevas Autonomous System Organizations (ASOs) utilizadas a nivel de recursos o de cuenta. Por ejemplo, este indicador muestra una nueva organización asignada comoASO.

Resumen del informe de Investigaciones de Detectives

El resumen de la investigación destaca los indicadores anómalos que requieren atención para el rango temporal seleccionado. Con el resumen puede identificar más rápidamente la causa raíz de los posibles problemas de seguridad, identificar patrones y comprender los recursos que se ven afectados por eventos de seguridad.

En el resumen detallado del informe de investigación puede ver los siguientes detalles.

Resumen de las investigaciones

En el panel de información general, puedes ver una visualización de IPs una actividad de alta gravedad, que puede proporcionar más contexto sobre la trayectoria de un atacante.

El Detective destaca una actividad inusual en la investigación, por ejemplo, la imposibilidad de que el IAM usuario viaje desde una fuente a un destino lejano.

El Detective mapea las investigaciones con las tácticas, técnicas y procedimientos (TTPs) utilizados en un posible evento de seguridad. El marco MITRE ATT &CK se utiliza para entender elTTPs. Las tácticas se basan en la matriz MITRE ATT &CK para empresas.

Indicadores de investigación

Puede utilizar la información del panel Indicadores para determinar si un recurso de AWS está implicado en una actividad inusual que pueda indicar un comportamiento malintencionado y su impacto. Un indicador de compromiso (IOC) es un artefacto observado en o sobre una red, un sistema o un entorno que puede (con un alto nivel de confianza) identificar una actividad maliciosa o un incidente de seguridad.

Descarga de un informe de Investigaciones de Detectives

Puede descargar el informe de Investigaciones de Detectives en JSON formato para analizarlo más a fondo o guardarlo en la solución de almacenamiento que prefiera, como un bucket de Amazon S3.

Para descargar un informe de investigación de la tabla Informes.

1. Inicie sesión en la consola AWS de administración. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Investigaciones.
3. Seleccione una investigación en la tabla Informes y elija Descargar.

Para descargar un informe de investigación de la tabla de resumen.

1. Inicie sesión en la consola AWS de administración. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Investigaciones.
3. Seleccione una investigación en la tabla Informes.
4. En la página de resumen de las investigaciones, seleccione Descargar.

Archivar un informe de Investigaciones de Detectives

Cuando termine su investigación en Amazon Detective, podrá Archivar el informe de investigación. Una investigación archivada indica que ha terminado de revisar la investigación.

Solo pueden archivar o desarchivar una investigación los administradores de Detective. Detective guardará sus investigaciones archivadas durante 90 días.

Para archivar un informe de investigación de la tabla Informes.

1. Inicie sesión en la consola AWS de administración. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Investigaciones.
3. Seleccione una investigación en la tabla Informes y elija Descargar.

Para archivar un informe de investigación de la tabla de resumen.

1. Inicie sesión en la consola AWS de administración. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Investigaciones.
3. Seleccione una investigación en la tabla Informes.

4. En la página de resumen de las investigaciones, seleccione Archivar.

Análisis de los hallazgos en Amazon Detective

En ciertos contextos, un resultado es una instancia de actividad potencialmente maliciosa u otro riesgo detectado. Amazon GuardDuty y las conclusiones de AWS seguridad se cargan en Amazon Detective para que puedas utilizar Detective para investigar la actividad asociada a las entidades implicadas. GuardDuty los hallazgos forman parte del paquete principal de Detective y se ingieren de forma predeterminada. Todos los demás hallazgos de AWS seguridad agregados por Security Hub se ingieren como una fuente de datos opcional. Consulte Datos de origen utilizados en un gráfico de comportamiento para obtener información más detallada.

En Detective, una descripción general de resultados proporciona información detallada sobre el resultado en cuestión. También muestra un resumen de las entidades implicadas, con enlaces a los perfiles de las entidades asociadas.

Si un resultado está relacionado con una actividad más amplia, Detective le invita a Ir al grupo de resultados. Le recomendamos que utilice grupos de resultados para continuar con la investigación, ya que los grupos de resultados le permiten examinar diferentes actividades relacionadas con un posible evento de seguridad. Consulte the section called “Búsqueda de grupos”.

Amazon Detective proporciona una visualización interactiva de los grupos de resultados. Esta visualización está diseñada para ayudarle a investigar los problemas de forma más rápida y exhaustiva con menos esfuerzo. El panel Visualización del grupo de resultados muestra los resultados y las entidades que intervienen en un grupo de resultados. Puede utilizar esta visualización interactiva para analizar, comprender y clasificar el impacto del grupo de resultados. Este panel ayuda a visualizar la información presentada en las tablas Entidades implicadas Resultados implicados. En la presentación visual, puede seleccionar los resultados o entidades para su posterior análisis. Consulte Buscar una visualización de grupos.

Contenido

- Análisis de una visión general de los hallazgos en Detective
- Análisis de grupos de resultados
- Resumen de grupo de resultados impulsado por IA generativa
- Archivar un hallazgo de Amazon GuardDuty

Análisis de una visión general de los hallazgos en Detective

En Detective, una descripción general de resultados proporciona información detallada sobre el resultado en cuestión. También muestra un resumen de las entidades implicadas, con enlaces a los perfiles de las entidades asociadas.

Rango temporal utilizado para la descripción general del resultado

El rango temporal de la descripción general de un resultado se establece en la franja horaria del resultado. La franja horaria del resultado refleja las horas de la primera y la última vez que se observó la actividad del resultado.

Detalles del resultado

El panel de la derecha contiene los detalles del resultado. Estos son los detalles proporcionados por el proveedor del resultado.

Desde de los detalles del resultado, también puede archivar el resultado. Para obtener más información, consulta Archivar un GuardDuty hallazgo de Amazon.

Entidades relacionadas

La descripción general del resultado contiene una lista de las entidades implicadas en el resultado. La lista proporciona información general sobre cada entidad de la lista. Esta información refleja la información del panel de perfil de detalles de la entidad correspondiente.

Puede filtrar la lista por tipo de entidad. También puede filtrar la lista por el texto del identificador de entidad.

Para pasar al perfil de una entidad, elija Ver perfil. Al pasar al perfil de la entidad, ocurre lo siguiente:

- El rango temporal se establece en la franja horaria del resultado.
- En el panel Resultado relacionado de la entidad, se selecciona el resultado. Los detalles del resultado siguen mostrándose a la derecha del perfil de la entidad.

Solución de problemas de 'Página no encontrada'

Cuando navegue hasta una entidad o un resultado en Detective, es posible que vea el mensaje de error Página no encontrada.

Para resolver este problema, siga uno de estos pasos:

- Asegúrese de que la entidad o el resultado pertenezca a una de sus cuentas de miembro. Para obtener información sobre cómo revisar las cuentas de los miembros, consulta Cómo ver la lista de cuentas.
- Asegúrese de que su cuenta de administrador esté alineada con GuardDuty o con Security Hub para pasar a Detective desde estos servicios. Para ver las recomendaciones, consulte Alineación recomendada con GuardDuty Security Hub.
- Compruebe que el resultado se ha producido después de que la cuenta de miembro haya aceptado su invitación.
- Compruebe que el gráfico de comportamiento de Detective ingiera datos de un paquete de origen de datos opcional. Para obtener más información sobre los datos de origen utilizados en los gráficos de comportamiento de los Detectives, consulte Datos de origen utilizados en un gráfico de comportamiento.

- Para permitir que Detective ingiera datos de Security Hub y los añada a su gráfico de comportamiento, debe habilitar Detective for AWS security findings como paquete de fuentes de datos. Para obtener más información, consulte los hallazgos AWS de seguridad.

- Si está navegando hasta el perfil de una entidad o buscando información general en Detective, asegúrese de que URL esté en el formato correcto. Para obtener más información sobre la formación de un perfilURL, consulte Navegar hasta el perfil de una entidad o buscar información general utilizando. URL

Análisis de grupos de resultados

Los grupos de resultados de Amazon Detective permiten examinar varias actividades relacionadas con un posible evento de seguridad. Un grupo de búsqueda en Amazon Detective se crea cuando Detective detecta un patrón o una relación entre varios hallazgos que sugiere que están relacionados con el mismo posible incidente de seguridad. Esta agrupación ayuda a gestionar e investigar los hallazgos relacionados de forma más eficiente.

Puede analizar la causa raíz de los GuardDuty hallazgos de gravedad elevada mediante la búsqueda de grupos. Si un agente de amenazas intenta poner en peligro su AWS entorno, normalmente lleva a cabo una secuencia de acciones que conducen a varios hallazgos de seguridad y a comportamientos inusuales. Estas acciones a menudo están dispersas en el tiempo y entre entidades. Cuando se

investigan resultados de seguridad de forma aislada, esto puede dar lugar a una interpretación errónea de su importancia y dificultar la identificación de la causa raíz. Para abordar este problema, Amazon Detective aplica una técnica de análisis gráfico que infiere las relaciones entre los resultados y las entidades, y las agrupa entre sí. Recomendamos tratar los grupos de resultados como punto de partida para investigar las entidades implicadas y los resultados.

Detective analiza los datos de los resultados y los agrupa con otros resultados probablemente relacionados basándose en los recursos que comparten. Por ejemplo, es muy probable que los hallazgos relacionados con acciones realizadas por las mismas sesiones de IAM rol o que se originaron en la misma dirección IP formen parte de la misma actividad subyacente. Resulta muy útil investigar los resultados y las pruebas como grupo, incluso aunque las asociaciones realizadas por Detective no estén relacionadas.

Los grupos de búsqueda se crean en función de los siguientes criterios.

- Proximidad temporal: los hallazgos que se producen dentro de un período de tiempo cercano suelen agruparse, ya que es probable que estén relacionados con el mismo incidente.
- Entidades comunes: los hallazgos que involucran a las mismas entidades, como direcciones IP, usuarios o recursos, se agrupan. Esto ayuda a comprender el alcance del incidente en las diferentes partes del entorno.
- Patrones y comportamientos: el Detective analiza los patrones y comportamientos de los hallazgos, como tipos similares de ataques o actividades sospechosas, para determinar las relaciones y agruparlas en consecuencia.
- Tácticas, técnicas y procedimientos (TTPs): los hallazgos que comparten características similaresTTPs, como se describe en marcos como MITRE ATT &CK, se agrupan para destacar los posibles ataques coordinados.

Estos criterios ayudan a agilizar el proceso de investigación para que pueda centrarse en los hallazgos correlacionados que probablemente representen el mismo incidente de seguridad.

Además de los resultados, cada grupo incluye las entidades implicadas en los resultados. Las entidades pueden incluir recursos externos AWS , como direcciones IP o agentes de usuario.

> **Note**
>
> Cuando se produce un GuardDuty hallazgo inicial relacionado con otro hallazgo, el grupo de búsqueda con todos los hallazgos relacionados y todas las entidades implicadas se crea en un plazo de 48 horas.

Explicación de la página de grupos de resultados

La página de búsqueda de grupos muestra todos los grupos de búsqueda recopilados por Amazon Detective a partir de su gráfico de comportamiento. Tome nota de los siguientes atributos de la búsqueda de grupos:

Gravedad de un grupo

A cada grupo de búsqueda se le asigna una gravedad en función de la gravedad de las conclusiones asociadas al formato de valoración de AWS seguridad (ASFF). ASFFencontrar valores de gravedad críticos, altos, medios, bajos o informativos, de mayor a menor gravedad. La gravedad de un grupo es igual al resultado de gravedad más alto entre los resultados de ese grupo.

En las investigaciones, se debe conceder prioridad a los grupos compuestos por resultados de gravedad Crítica o Alta que afecten a un gran número de entidades, ya que es más probable que representen problemas de seguridad de alto impacto.

Título del grupo

En la columna Título, cada grupo tiene un identificador único y un título no exclusivo. Se basan en el ASFF tipo de espacio de nombres del grupo y en el número de hallazgos dentro de ese espacio de nombres del clúster. Por ejemplo, si una agrupación tiene el título: Grupo con: TTP(2), Efecto (1) y Comportamiento inusual (2), incluye cinco hallazgos en total, compuestos por dos hallazgos en el espacio de nombres, un hallazgo en el TTPespacio de nombres Effect y dos hallazgos en el espacio de nombres Comportamiento inusual. Para obtener una lista completa de los espacios de nombres, consulte Taxonomía de tipos para. ASFF

Tácticas de un grupo

La columna Tácticas de un grupo detalla la categoría de tácticas a la que pertenece la actividad. Las categorías de tácticas, técnicas y procedimientos de la siguiente lista se alinean con la matriz de &CK. MITRE ATT

Puede seleccionar una táctica de la cadena para ver una descripción de la táctica. Debajo de la cadena hay una lista de las tácticas detectadas en el grupo. Estas categorías y las actividades que suelen representar son las siguientes:

- Acceso inicial: un adversario intenta entrar en la red de otra persona.
- Ejecución: un adversario intenta entrar en la red de otra persona.
- Persistencia: un adversario intenta mantener su posición.
- Aumento de privilegios: un adversario intenta obtener permisos de nivel superior.
- Evasión de defensa: un adversario intenta evitar ser detectado.
- Acceso a credenciales: un adversario intenta robar nombres y contraseñas de cuentas.
- Detección: un adversario intenta comprender y obtener información sobre un entorno.
- Movimiento lateral: un adversario intenta moverse a través de un entorno.
- Recopilación: un adversario intenta recopilar datos de interés para su objetivo.
- Mando y control: un adversario intenta entrar en la red de otra persona.
- Exfiltración: un adversario intenta robar datos.
- Impacto: un adversario intenta manipular, interrumpir o destruir sus sistemas y datos.
- Otro: indica actividad de un resultado que no se ajusta a las tácticas enumeradas en la matriz.

Entidades de un grupo

La columna Entidades contiene detalles sobre las entidades específicas detectadas dentro de esta agrupación. Seleccione este valor para obtener un desglose de las entidades en función de sus categorías: Identidad, Red, Almacenamiento y Computación. Algunos ejemplos de entidades de cada categoría son:

- Identidad: IAM principios y Cuentas de AWS, por ejemplo, usuario y rol
- Red: dirección IP u otras redes y entidades VPC
- Almacenamiento: cubos de Amazon S3 o DDBs
- EC2Instancias de Amazon de cómputo o contenedores de Kubernetes

Cuentas de un grupo

La columna Cuentas indica qué AWS cuentas pertenecen a las entidades implicadas en los hallazgos del grupo. Las AWS cuentas se enumeran por nombre e AWS identificación para que pueda priorizar las investigaciones de actividades relacionadas con cuentas críticas.

Resultados de un grupo

La columna Resultados contiene una lista de las entidades de un grupo por gravedad. Los hallazgos incluyen los hallazgos de Amazon, GuardDuty los hallazgos del Inspector de Amazon, los hallazgos de AWS seguridad y las pruebas del Detective. Puede seleccionar el gráfico para ver un recuento exacto de los resultados por gravedad.

GuardDuty los hallazgos forman parte del paquete principal de Detective y se ingieren de forma predeterminada. Todos los demás hallazgos de AWS seguridad agregados por Security Hub se ingieren como una fuente de datos opcional. Consulte Datos de origen utilizados en un gráfico de comportamiento para obtener información más detallada.

Resultados informativos en grupos de resultados

Amazon Detective identifica información adicional relativa a un grupo de resultados basándose en los datos del gráfico de comportamiento recopilados en los últimos 45 días. Detective presenta esta información como resultado de gravedad Informativa. Las evidencias proporcionan información de apoyo que pone de relieve una actividad inusual o un comportamiento desconocido que puedan resultar sospechosos si se observan dentro de un grupo de resultados. Esto puede incluir geolocalizaciones recientemente observadas o API llamadas observadas durante el tiempo transcurrido desde el momento en que se produjo un hallazgo. Los hallazgos de evidencia solo se pueden ver en Detective y no se envían a AWS Security Hub.

El Detective determina la ubicación de las solicitudes mediante bases de datos de MaxMind GeoIP. MaxMind informa que sus datos son muy precisos a nivel de país, aunque la precisión varía según factores como el país y el tipo de IP. Para obtener más información MaxMind, consulte Geolocalización de MaxMind IP. Si cree que alguno de los datos de GeoIP es incorrecto, puede enviar una solicitud de corrección a Maxmind en MaxMind Correct Geo Data. IP2

Puede observar la evidencia de diferentes tipos principales (como el IAM usuario o el IAM rol). En el caso de algunos tipos de evidencias, puede observar las evidencias de todas las cuentas. Esto significa que las evidencias afectan a todo el gráfico de comportamiento. Si se observa una prueba para todas las cuentas, también verás al menos una prueba informativa adicional del mismo tipo para una IAM función individual. Por ejemplo, si ve un resultado Nueva geolocalización observada para todas las cuentas, verá otra para el resultado Nueva geolocalización observada para una entidad principal.

Tipos de evidencias en los grupos de resultados

- Nuevas geolocalizaciones observadas
- Se observó una nueva organización del sistema autónomo (ASO)
- Nuevo agente de usuario observado
- Se ha emitido API una nueva convocatoria
- Nueva geolocalización observada para todas las cuentas
- Se observó un nuevo IAM principal en todas las cuentas

Perfiles de grupos de resultados

Al seleccionar el título de un grupo, se abre un perfil de grupo de resultados con detalles adicionales sobre dicho grupo. El panel de detalles de la página de perfil del grupo de resultados permite mostrar hasta 1000 entidades y resultados de grupos de resultados superiores e inferiores.

La página de perfil del grupo muestra el Rango temporal establecido para el grupo. Esta es la fecha y la hora desde el primer resultado o evidencia incluidos en el grupo, hasta el resultado o evidencia actualizados más recientemente en un grupo. También puede ver la Gravedad del grupo de resultados, que es igual a la categoría de gravedad más alta de los resultados del grupo. Otros detalles de este panel de perfil incluyen:

- La cadena Tácticas implicadas, que muestra las tácticas que se atribuyen a los resultados del grupo. Las tácticas se basan en la matriz MITRE ATT &CK para empresas. Las tácticas se muestran en forma de una cadena de puntos de colores que representan la progresión típica de un ataque desde las fases iniciales hasta las finales. Esto significa que los círculos más a la izquierda de la cadena suelen representar actividades menos graves en las que un adversario intenta obtener o mantener acceso a su entorno. Por el contrario, las actividades hacia la derecha son las más graves y pueden incluir la manipulación o destrucción de datos.
- Las relaciones de este grupo con otros grupos. Ocasionalmente, uno o más grupos de resultados previamente desconectados pueden fusionarse en un nuevo grupo sobre la base de un vínculo recién descubierto; por ejemplo, un resultado que implique a entidades de los grupos existentes. En este caso, Amazon Detective desactiva los grupos principales y crea un grupo secundario. Puede rastrear el linaje de cualquier grupo hasta sus grupos principales. Los grupos pueden tener las siguientes relaciones:

- Grupo de resultados secundario: grupo de resultados que se crea cuando un resultado implicado en otros dos grupos de resultados está implicado en un nuevo resultado. Para todos los grupos secundarios se enumeran los grupos principales del resultado.
- Grupo de resultados principal: un grupo de resultados es principal cuando se crear un grupo secundario a partir de él. Si un grupo de resultados es principal, los grupos secundarios relacionados se enumeran junto a él. El estado de un grupo principal pasa a ser Inactivo cuando se fusiona con un grupo secundario Activo.

Hay dos pestañas de información que abren paneles de perfil. Mediante las pestañas Entidades implicadas y Resultados implicados, puede ver más detalles sobre el grupo.

Utilice Ejecutar investigación para generar un informe de la investigación. El informe generado detalla un comportamiento anómalo que indica un compromiso.

Perfil dentro de los grupos

Entidades implicadas

Se centra en las entidades del grupo de resultados, incluidos los resultados del grupo a los que está vinculada cada entidad. También se muestran las etiquetas adjuntas a cada entidad para que pueda identificar rápidamente las entidades importantes en función del etiquetado. Seleccione una entidad para ver su perfil de entidad.

Resultados implicados

Contiene detalles sobre cada resultado, incluida la gravedad del resultado, cada entidad implicada y cuándo se detectó ese resultado por primera y por última vez. Seleccione un tipo de resultado en la lista para abrir un panel de detalles del resultado con información adicional sobre ese resultado. Como parte del panel Resultados implicados, puede ver resultados de gravedad Informativa en función de las evidencias de Detective de su gráfico de comportamiento.

Visualización de grupos de resultados

Amazon Detective proporciona una visualización interactiva de los grupos de resultados. Esta visualización está diseñada para ayudarle a investigar los problemas de forma más rápida y exhaustiva con menos esfuerzo. El panel Visualización del grupo de resultados muestra los resultados y las entidades que intervienen en un grupo de resultados. Puede utilizar esta visualización interactiva para analizar, comprender y clasificar el impacto del grupo de resultados.

Este panel ayuda a visualizar la información presentada en las tablas Entidades implicadas Resultados implicados. En la presentación visual, puede seleccionar los resultados o entidades para su posterior análisis.

Los grupos de resultados de Detective con resultados agregados son un clúster de resultados que están conectados al mismo tipo de recurso. Con los resultados agregados, puede evaluar rápidamente la composición de un grupo de resultados e interpretar los problemas de seguridad con mayor rapidez. El panel de detalles de los grupos de resultados combina resultados similares, y puede ampliar los resultados para ver juntos resultados relativamente similares. Por ejemplo, un nodo de evidencias, que contiene los resultados agregados de gravedad informativa y media del mismo tipo. Actualmente, puede ver el título, el origen, el tipo y la gravedad de los grupos de resultados con resultados agregados.

Desde este panel interactivo, puede:

- Utilice Ejecutar investigación para generar un informe de la investigación. El informe generado detalla un comportamiento anómalo que indica un riesgo. Para obtener más información, consulte Investigaciones de Detectives.
- Vea más detalles sobre grupos de resultados con resultados agregados para analizar las evidencias, las entidades y los resultados implicados.
- Consulte las etiquetas de las entidades y los resultados para identificar las entidades afectadas con posibles problemas de seguridad. Puede desactivar la Etiqueta.
- Reorganice las entidades y los resultados para comprender mejor su interconexión. Aísle las entidades y los resultados de un grupo moviendo el elemento seleccionado dentro del grupo de resultados.
- Seleccione las evidencias, las entidades y los resultados para ver más detalles sobre ellos. Para seleccionar varios elementos, elija **`command/control`** y luego elija los elementos, o arrástrelos y suéltelos con el puntero.
- Ajuste el diseño para que quepan todas las entidades y resultados en la ventana del grupo de resultados. Vea qué tipos de entidades predominan en un grupo de resultados.

> **Note**
>
> El panel Visualización del grupo de resultados permite mostrar grupos de resultados con hasta 100 entidades y resultados.

Puede usar el menú desplegable para ver los hallazgos y las entidades en un diseño radial, circular, dirigido por la fuerza o de cuadrícula. El diseño radial proporciona una visualización mejorada para facilitar la interpretación de los datos. El diseño Por fuerza coloca las entidades y los resultados de manera que los enlaces tengan una longitud uniforme entre los elementos y que los enlaces se distribuyan de manera uniforme. Esto contribuye a evitar los solapamientos. El diseño que seleccione define la posición de los resultados en el panel Visualización.

Diseño de línea de tiempo

El diseño de la línea temporal proporciona una forma dinámica de visualizar la evolución de los grupos de búsqueda a lo largo del tiempo. Esto le permite ver la progresión de los eventos, lo que le ayuda a comprender mejor la secuencia y la posible causalidad de los incidentes de seguridad con Detective.

Utilice el control deslizante de la línea temporal situado en la parte inferior del panel de visualización para seleccionar un punto específico en el tiempo. La visualización se actualizará para mostrar el estado del grupo de búsqueda en ese momento. El botón de reproducción que te permite avanzar automáticamente por la línea temporal. Haga clic en el botón de reproducción para iniciar la animación. La visualización se actualizará en tiempo real y mostrará cómo cambia el grupo de búsqueda con el tiempo. Utilice el botón de pausa para detener la animación en cualquier momento.

Ahora puede filtrar los resultados en función de su nivel de gravedad mediante el menú desplegable Filtro. Al aplicar un filtro, la visualización se actualizará para mostrar solo los hallazgos que coincidan con el nivel de gravedad seleccionado. El filtro solo afecta a los hallazgos que se muestran en la cronología, no a la visualización completa del grupo de búsqueda. Esto te permite centrarte rápidamente en cuestiones de alta prioridad o investigar tipos específicos de hallazgos.

Puede utilizar la función de filtrado en combinación con el diseño del cronograma para ver cómo surgen y evolucionan los hallazgos con distintos niveles de gravedad a lo largo del tiempo.

Flujo de trabajo de investigación mejorado

Con la incorporación del diseño del cronograma y las capacidades de filtrado, ahora puede llevar a cabo investigaciones aún más exhaustivas:

1. Comience por ver todo el grupo de búsqueda utilizando uno de los diseños estáticos (radial, circular, dirigido por la fuerza o cuadrícula).
2. Usa cronogramas para entender cómo se desarrolló la situación a lo largo del tiempo.
3. Usa el botón de reproducción para avanzar automáticamente por la línea temporal y observar los momentos o patrones clave.

4. Haz una pausa en los puntos importantes para seguir investigando.
5. Aplique filtros para centrarse en los hallazgos de niveles de gravedad específicos.
6. Utilice los atajos de teclado y las herramientas de selección para profundizar en las entidades y los hallazgos de interés.

Este flujo de trabajo mejorado permite una investigación más matizada y exhaustiva de escenarios de seguridad complejos. Puede llevar a cabo investigaciones de seguridad más eficientes y efectivas, lo que permite una resolución de incidentes más rápida y una mejor postura general de seguridad.

Métodos abreviados de teclado

Puede utilizar los siguientes atajos de teclado para interactuar con el panel de visualización del grupo de búsqueda:

- Hacer clic: selecciona un solo nodo, deselecciona todos los demás nodos y deselecciona todos los nodos si se hace clic en un espacio en blanco.
- Ctrl + Clic: selecciona un solo nodo, no anula la selección de otros nodos.
- Arrastrar: permite desplazar la vista.
- Ctrl + Arrastrar: el recuadro selecciona otros nodos, no los deselecciona.
- Mayús y arrastre: el recuadro selecciona y deselecciona todos los demás nodos.
- Teclas de flecha: cambia el enfoque entre los nodos.
- Ctrl + Espacio: selecciona o deselecciona el nodo actualmente enfocado.
- Mayús + Teclas de flecha: cambia el enfoque entre los nodos y los selecciona.

La Leyenda dinámica cambia en función de las entidades y los resultados del gráfico actual. Le ayuda a identificar lo que representa cada elemento visual.

Resumen de grupo de resultados impulsado por IA generativa

De forma predeterminada, Amazon Detective proporciona automáticamente resúmenes de un grupo de resultados individual. Los resúmenes están impulsados por modelos de inteligencia artificial generativa (IA generativa) alojados en Amazon Bedrock.

Al utilizar los grupos de resultados, puede examinar varios resultados de seguridad, ya que están relacionados con un posible evento de seguridad, e identificar a posibles actores de amenazas.

Los resúmenes de grupos de resultados se basa en estas capacidades. Los resúmenes de grupos de resultados consumen los datos de un grupo de resultados, analizan rápidamente las relaciones entre resultados y recursos afectados y, a continuación, resumen las posibles amenazas en lenguaje natural. Puede aprovechar estos resúmenes para identificar amenazas de seguridad más importantes, mejorar la eficiencia de la investigación y acortar los plazos de respuesta.

> **Note**
>
> Es posible que los resúmenes de grupos de resultados con tecnología de IA generativa no siempre faciliten información completamente precisa. Consulte AWS Política de IA responsable para obtener más información.

Revisión de resumen del grupo de resultados

El resumen de un grupo de resultados proporciona una explicación clara y detallada de un evento de seguridad. En lenguaje natural, la explicación incluye un breve título, un resumen de los recursos involucrados e información seleccionada sobre esos recursos.

Para revisar un resumen de grupo de resultados

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Grupos de resultados.
3. En la tabla Grupos de resultados, elija el grupo de resultados cuyo resumen desea mostrar. Aparecerá una página de detalles.

En la página de detalles, puede utilizar el panel Resumen para revisar un resumen descriptivo generado de los principales resultados del grupo de resultados. También puede revisar un análisis de los principales eventos de amenaza del grupo de resultados, que luego podrá investigar más a fondo. Para añadir el resumen generado a sus notas o a un sistema de venta de entradas, seleccione el icono de copia del panel. De esta forma se copiará el resumen en el portapeles. También puede compartir sus comentarios sobre el resumen del grupo de resultados en el resumen, lo que puede brindar una mejora de la experiencia en el futuro. Para compartir sus comentarios, seleccione el icono de pulgar hacia arriba o hacia abajo, en función de la naturaleza de los comentarios.

> **Note**
>
> Si envía comentarios sobre el resumen del grupo de resultados, sus comentarios no se utilizarán para ajustar el modelo. Los utilizamos únicamente para ayudar a facilitar que las instrucciones de Detective se diseñen de manera efectiva.

Deshabilitación del resumen de grupo de resultados

De forma predeterminada, el resumen de grupo de resultados está habilitado para grupos de resultados. Puede deshabilitar el resumen de grupo de resultados en cualquier momento. Si lo deshabilita, podrá habilitarlo más adelante.

Deshabilitación del resumen de grupo de resultados

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Preferences (Preferencias).
3. En Resumen de grupo de resultados, seleccione Editar.
4. Desactive Habilitado.
5. Seleccione Guardar.

Deshabilitación del resumen de grupo de resultados

Si ha deshabilitado el resumen de grupo de resultados para grupos de resultados, puede habilitarlo de nuevo en cualquier momento.

Habilitación del resumen de grupo de resultados

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Preferences (Preferencias).
3. En Resumen de grupo de resultados, seleccione Editar.
4. Active Habilitado.
5. Seleccione Guardar.

Regiones admitidas

El resumen de búsqueda de grupos está disponible en los siguientes enlaces AWS Regiones.

- Este de EE. UU. (Norte de Virginia)
- Oeste de EE. UU. (Oregón)
- Asia-Pacífico (Tokio)
- Europe (Fráncfort)

Archivar un hallazgo de Amazon GuardDuty

Cuando termines la investigación de un GuardDuty hallazgo de Amazon, puedes archivarlo en Amazon Detective. Esto te ahorra la molestia de tener que volver GuardDuty a realizar la actualización. Archivar un resultado indica que ha terminado de investigarlo.

Solo puede archivar un GuardDuty hallazgo desde Detective si también es la cuenta de GuardDuty administrador de la cuenta asociada al hallazgo. Si no es una cuenta de GuardDuty administrador e intenta archivar un hallazgo, se GuardDuty mostrará un error.

Para archivar un GuardDuty hallazgo

1. Inicie sesión en la consola AWS de administración. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En la consola de Detective, en el panel de detalles del resultado, elija Archivar resultado.
3. Cuando se le solicite confirmación, elija Archivar.

Puede ver los GuardDuty hallazgos archivados en la GuardDuty consola. Los hallazgos archivados se almacenan GuardDuty durante 90 días y se pueden ver en cualquier momento durante ese período. Para ver los hallazgos suprimidos en la GuardDuty consola, seleccione Archivado en la tabla de hallazgos o GuardDuty API utilice la opción ListFindingsAPICon un findingCriteria criterio de servicio.archivado igual a verdadero. Para obtener más información, consulta las normas de supresión en la Guía del GuardDuty usuario de Amazon.

Análisis de entidades en Amazon Detective

Una entidad es un objeto único extraído de los datos de origen. Los ejemplos incluyen una dirección IP específica, una EC2 instancia de Amazon o AWS una cuenta. Para obtener una lista de los tipos de entidades, consulte the section called “Tipos de entidades de la estructura de datos del gráfico de comportamiento”.

Un perfil de entidad de Amazon Detective es una página única que proporciona información detallada sobre la entidad y su actividad. Puede usar un perfil de entidad para obtener información que respalde una investigación sobre un resultado o como parte de una búsqueda general de actividad sospechosa.

Contenido

- Uso de perfiles de entidades
- Visualización e interacción con los paneles de perfil de Detective
- Desplazarse directamente a un perfil de entidad o a la descripción general de un resultado
- Paso de un panel de perfil a otra consola
- Exploración de los detalles de actividad en un panel de perfil
- Administración del rango temporal
- Visualización de los detalles de los hallazgos asociados en Detective
- Visualización de detalles de entidades de gran volumen en Detective

Uso de perfiles de entidades

Un perfil de entidad se muestra al realizar una de las siguientes acciones:

- Desde la GuardDuty consola de Amazon, elige la opción de investigar una entidad relacionada con un hallazgo seleccionado.

  Consulte the section called “Pasar desde otra consola”.
- Vaya a la URL de Detective correspondiente al perfil de entidad.

  Consulte the section called “Desplazarse mediante una URL”.
- Use la búsqueda de Detective en la consola de Detective para buscar una entidad.

- Elija un enlace al perfil de entidad desde otro perfil de entidad o desde la descripción general de un resultado.

Rango temporal de un perfil de entidad

Cuando se desplaza directamente a un perfil de entidad sin proporcionar el rango temporal, este se establece en las 24 horas anteriores.

Cuando se desplaza a un perfil de entidad desde otro perfil de entidad, se conserva el rango temporal seleccionado.

Cuando se desplaza a un perfil de entidad desde la descripción general de un resultado, el rango temporal se establece en la franja horaria del resultado.

Para obtener información sobre cómo personalizar el tiempo de alcance para limitar los datos que se muestran en los perfiles de las entidades, consulte Gestión del tiempo de alcance.

Identificador y tipo de entidad

En la parte superior del perfil se encuentran el identificador de entidad y el tipo de entidad. Cada tipo de entidad tiene un icono correspondiente, que proporciona una indicación visual del tipo de perfil.

Resultados implicados

Cada perfil contiene una lista de resultados en los que la entidad estuvo implicada durante el rango temporal.

Puede ver los detalles de cada resultado, cambiar el rango temporal para que refleje la franja horaria del resultado, y acceder a la descripción general del resultado para buscar otros recursos implicados.

Consulte the section called “Ver los resultados de una entidad”.

Grupos de resultados que impliquen a esta entidad

Cada perfil contiene una lista de los grupos de resultados en los que está incluida una entidad.

Un grupo de resultados se compone de resultados, entidades y pruebas que Detective recopila en un grupo para proporcionar más contexto sobre posibles problemas de seguridad.

Para obtener más información acerca de los grupos de resultados, consulte the section called “Búsqueda de grupos”.

Paneles de perfil que contienen detalles de entidad y resultados de análisis

Cada perfil de entidad contiene un conjunto de una o varias pestañas. Cada pestaña contiene uno o varios paneles de perfil. Cada panel de perfil contiene texto y visualizaciones que se generan a partir de los datos del gráfico de comportamiento. Las pestañas y los paneles de perfil específicos se adaptan al tipo de entidad.

Para la mayoría de las entidades, el panel situado en la parte superior de la primera pestaña proporciona información avanzada resumida sobre la entidad.

Otros paneles de perfil resaltan diferentes tipos de actividad. En el caso de una entidad implicada en un resultado, la información que figura en los paneles de perfil de entidad puede proporcionar pruebas complementarias que ayuden a completar la investigación. Cada panel de perfil proporciona acceso a directrices sobre cómo usar la información. Para obtener más información, consulte the section called “Usar las directrices de los paneles de perfil”.

Para obtener más información sobre los paneles de perfil, los tipos de datos que contienen y las opciones disponibles para interactuar con ellos, consulte the section called “Paneles de perfiles”.

Navegar por el perfil de una entidad

Un perfil de entidad consta de una o varias pestañas. Cada pestaña contiene uno o varios paneles de perfil. Cada panel de perfil contiene texto y visualizaciones que se generan a partir de los datos del gráfico de comportamiento.

A medida que se desplaza hacia abajo por una pestaña de perfil, la siguiente información permanece visible en la parte superior del perfil:

- Tipo de identidad
- Identificador de la entidad
- Rango temporal

Visualización e interacción con los paneles de perfil de Detective

Cada perfil de entidad de la consola de Amazon Detective consta de un conjunto de paneles de perfil. Un panel de perfil es una visualización que proporciona detalles genéricos o resalta actividad específica asociada a una entidad. Los paneles de perfil usan distintos tipos de visualizaciones para presentar distintos tipos de información. También pueden proporcionar enlaces a detalles adicionales o a otros perfiles.

Cada panel de perfil está diseñado para ayudar a los analistas a encontrar respuestas a preguntas concretas sobre las entidades y su actividad asociada. Las respuestas a esas preguntas ayudan a llegar a una conclusión sobre si la actividad representa una amenaza real.

Los paneles de perfil usan distintos tipos de visualizaciones para presentar distintos tipos de información.

Tipos de información de un panel de perfil

Los paneles de perfil suelen proporcionar los siguientes tipos de datos.

Tipo de datos del panel	Descripción
Información de alto nivel sobre un resultado o una entidad	El tipo de panel más sencillo proporciona cierta información básica acerca de una entidad. Ejemplos de información incluida en un panel de informaci ón incluyen el identificador, el nombre, el tipo y la fecha de creación.

Tipo de datos del panel	Descripción
	 La mayoría de los perfiles de entidad contienen un panel de información para dicha entidad.
Resumen general de actividad a lo largo del tiempo	Muestra un resumen de la actividad de una entidad a lo largo del tiempo. Este tipo de panel proporciona una visión general del comportamiento de una entidad durante el rango temporal. A continuación se muestran algunos ejemplos de datos de resumen que se proporcionan en los paneles de perfil de Detective: • APILlamadas fallidas y exitosas • Volumen entrante y saliente VPC

Tipo de datos del panel	Descripción
Resumen de actividad agrupado por valores	Muestra un resumen de la actividad de una entidad, agrupado por determinados valores. Por ejemplo, puede ver este tipo de panel de perfil en el perfil. EC2 El panel de perfil muestra el volumen promedio de datos del registro de VPC flujo hacia y desde una EC2 instancia para los puertos comunes que están asociados a tipos específicos de servicios.

Tipo de datos del panel	Descripción
Actividad que comenzó justo durante el rango temporal	Durante una investigación, es útil ver qué actividad comenzó a producirse justo durante un periodo de tiempo concreto. Por ejemplo, ¿hay API llamadas, ubicaciones geográficas o agentes de usuario que no se hayan visto antes? Si el gráfico de comportamiento sigue en modo de aprendizaje, el panel de perfil muestra un mensaje de notificación. El mensaje se elimina cuando el gráfico de comportamiento ha acumulado al menos dos semanas de datos. Para obtener más información acerca del modo de aprendizaje, consulte the section called “Periodo de aprendizaje de nuevos gráficos de comportamiento”.

Tipo de datos del panel	Descripción
Actividad que ha cambiado de manera significativa durante el rango temporal	Al igual que los nuevos paneles de actividad, los paneles de perfil también pueden mostrar la actividad que ha cambiado significativamente durante el rango temporal. Por ejemplo, un usuario puede emitir una API llamada determina da con regularidad varias veces a la semana. Si, de repente, el mismo usuario hace la misma llamada varias veces en un mismo día, eso podría ser indicio de una actividad malintenc ionada. Si el gráfico de comportamiento sigue en modo de aprendiza je, el panel de perfil muestra un mensaje de notificación. El mensaje se elimina cuando el gráfico de comportamiento ha acumulado al menos dos semanas de datos. Para obtener más información acerca del modo de aprendizaje, consulte the section called “Periodo de aprendizaje de nuevos gráficos de comportamiento”.

Tipos de visualizaciones de un panel de perfil

El contenido de un panel de perfil puede adoptar una de las siguientes formas:

Tipo de visualización	Descripción
Pares clave-valor	El tipo de visualización más simple es un conjunto de pares de clave-valor. Un panel de información de resultado o entidad es el ejemplo más común de un panel de pares de clave-valor.

Tipo de visualización	Descripción
	 Los pares de clave-valor también se pueden usar para añadir información adicional a otros tipos de paneles. Desde un panel de pares de clave-valor, si un valor es un identificador de una entidad, puede pasar directamente a su perfil.
Tabla	Una tabla es una simple lista de elementos de varias columnas. Puede ordenar, filtrar y desplazarse hacia arriba y hacia abajo por la tabla. Puede cambiar el número de entradas que se muestren en cada página. Consulte the section called “Preferencias de los paneles de perfil”. Si un valor de la tabla es un identificador de una entidad, puede pasar directamente a su perfil.

Tipo de visualización	Descripción
Plazo	Una visualización de cronograma muestra un valor agregado a intervalos definidos a lo largo del tiempo. El cronograma resalta el rango temporal actual e incluye el tiempo periférico adicional antes y después del rango temporal. El tiempo periférico proporciona un contexto para la actividad en el rango temporal. Pase el ratón por encima de un intervalo de tiempo para ver un resumen de los datos de dicho intervalo.

Tipo de visualización	Descripción
Tabla ampliable	Una tabla ampliable combina tablas y cronogramas. La visualización comienza como una tabla. Puede ordenar, filtrar y desplazarse hacia arriba y hacia abajo por la tabla. Puede cambiar el número de entradas que se muestren en cada página. Consulte the section called “Preferencias de los paneles de perfil”. A continuación, puede expandir cada fila para que se muestre una visualización de cronograma específica de esa fila.
Gráfico de barras	Un gráfico de barras muestra valores basándose en agrupaciones. Según el gráfico, tal vez pueda elegir una barra para que se muestre un cronograma de actividades relacionadas.

Tipo de visualización	Descripción
Gráfico de geolocalización	Un gráfico de geolocalización muestra un mapa marcado para resaltar los datos en función de la ubicación geográfica. Puede ir seguido de una tabla con detalles sobre geolocalizaciones individuales. Tenga en cuenta que, al procesar datos geográficos entrantes , Detective redondea los valores de latitud y longitud a un solo punto decimal.

Notas sobre el contenido del panel de perfil

Tenga en cuenta lo siguiente cuando vea el contenido de un panel de perfil:

Advertencia de datos de recuento aproximado

Esta advertencia indica que los elementos con recuentos extremadamente bajos no aparecen debido al volumen de datos aplicables.

Para garantizar un recuento completamente preciso, reduzca la cantidad de datos. La forma más sencilla de hacerlo es reducir la duración del rango temporal. Consulte the section called “Administración del rango temporal”.

Redondear por ubicaciones geográficas

Detective redondea todos los valores de latitud y longitud a un solo punto decimal.

Cambios en la forma en que Detective representa API las llamadas

A partir del 14 de julio de 2021, Detective rastrea el servicio que realizó cada API llamada. Siempre que Detective muestre un API método, también mostrará el servicio asociado. En los paneles de perfil que muestran información sobre las API llamadas, las llamadas siempre se agrupan por servicio. En el caso de los datos ingeridos por Detective antes de esa fecha, el nombre del servicio aparece como Servicio desconocido.

Además, a partir del 14 de julio de 2021, en el caso de las cuentas y los roles, los detalles de la actividad del panel del perfil del volumen general de API llamadas AKID dejarán de mostrar el recurso que emitió la llamada. En el caso de las cuentas, Detective muestra el identificador de la entidad principal (usuario o rol) que emitió la llamada. En el caso de los roles, Detective muestra el identificador de la sesión de rol. En el caso de los datos ingeridos por Detective antes del 14 de julio de 2021, el identificador aparece como Recurso desconocido.

En el caso de los paneles de perfil que muestran una lista de API llamadas, la cronología asociada resalta el período de tiempo durante el cual se produjo esta transición. La información destacada comienza el 14 de julio de 2021 y finaliza cuando la actualización se propagó por completo en Detective.

Establecimiento de las preferencias de un panel de perfil

En el caso de los paneles de perfil, puede personalizar el número de filas que aparecen en cada página de los paneles de perfil y configurar la preferencia de formato de marca horaria.

Establecimiento de la longitud de la tabla

En el caso de los paneles de perfil que contienen tablas o tablas ampliables, puede configurar el número de filas que se mostrarán en cada página.

Defina su preferencia en cuanto al número de entradas por página.

1. Abre la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, en Configuración, elija Preferencias.
3. En la página Preferencias, en Longitud de la tabla, haga clic en Editar.
4. Elija el número de filas de la tabla que desea que se muestren por página.
5. Elija Guardar.

Establecer el formato de marca temporal

Para los paneles de perfil, puede configurar la preferencia de formato de marca de tiempo que se aplicará a todas las marcas de tiempo de cada IAM usuario o rol IAM de Detective.

> **Note**
>
> La preferencia de formato de marca horaria no se aplica a toda la cuenta. AWS

Defina la preferencia para la marca temporal.

1. Abre la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, en Configuración, elija Preferencias.
3. En la página Preferencias, en Preferencias de marca de tiempo, consulte y cambie la visualización preferida para todas las marcas de tiempo.
4. De forma predeterminada, el formato de marca de tiempo está establecido en. UTC Haga clic en Editar para elegir su zona horaria local.

   Ejemplo:

   Example

   UTC- 20/09/22 16:39 UTC

   Local - 20/09/2022 9:39 (- 07:00) UTC
5. Seleccione Guardar.

Desplazarse directamente a un perfil de entidad o a la descripción general de un resultado

Para desplazarse directamente a un perfil de entidad o a la descripción general de un resultado en Amazon Detective, puede usar una de estas opciones.

- Desde Amazon GuardDuty o AWS Security Hub, puedes pasar de un GuardDuty hallazgo al perfil de búsqueda del Detective correspondiente.

- Puede crear una URL de Detective que identifique un resultado o una entidad y establezca el rango temporal que se debe usar.

Pasar al perfil de una entidad o buscar información general en Amazon GuardDuty o AWS Security Hub

Desde la GuardDuty consola de Amazon, puede navegar hasta el perfil de entidad de una entidad relacionada con un hallazgo.

Desde las AWS Security Hub consolas GuardDuty y, también puedes acceder a un resumen de los resultados. Esto también proporciona enlaces a los perfiles de entidad de las entidades implicadas.

Estos enlaces pueden contribuir a agilizar el proceso de investigación. Puede usar Detective rápidamente para ver la actividad de la entidad asociada y decidir los pasos siguientes. A continuación, puede archivar un resultado si se trata de un falso positivo, o examinarlo más a fondo para determinar el alcance del problema.

Cómo pasar a la consola de Amazon Detective

Los enlaces de la investigación están disponibles para ver todos los GuardDuty hallazgos. GuardDuty también le permite elegir si desea acceder al perfil de una entidad o al resumen de los resultados.

Para pasar a Detective desde la consola GuardDuty

1. Abra la GuardDuty consola en https://console.aws.amazon.com/guardduty/.
2. Si es necesario, en el panel de navegación izquierdo, elija Resultados.
3. En la página GuardDuty Hallazgos, elija el hallazgo.

   Se muestra el panel de detalles del resultado a la derecha de la lista de resultados.
4. En el panel de detalles del resultado, elija Investigar en Detective.

   GuardDuty muestra una lista de los elementos disponibles para investigar en Detective.

   La lista contiene tanto las entidades relacionadas (por ejemplo, las direcciones IP o las instancias de EC2), como el resultado.
5. Elija una entidad o el resultado.

La consola de Detective se abre en una pestaña nueva. Se abre la consola para mostrar la entidad o el perfil de resultado.

Si no ha habilitado Detective, la consola se abre en una página de inicio que proporciona información general de Detective. Desde allí, puede optar por habilitar Detective.

Paso a Detective desde la consola de Security Hub

1. Abre la AWS Security Hub consola en https://console.aws.amazon.com/securityhub/.
2. Si es necesario, en el panel de navegación izquierdo, elija Resultados.
3. En la página Conclusiones de Security Hub, selecciona una GuardDuty conclusión.
4. En el panel de detalles, elija Investigar en Detective y, a continuación, elija Investigar resultado.

   Al elegir Investigar resultado, la consola de Detective se abre en una pestaña nueva. La consola se abre con la descripción general del resultado.

   La consola de Detective se abre siempre en la región en la que se originó el resultado, incluso si se cambia la región de agregación. Para obtener más información sobre la agregación de resultados, consulte Aggregating findings across Regions en la Guía del usuario de AWS Security Hub .

   Si no ha habilitado Detective, la consola se abre en la página de inicio de Detective. Desde ella, puede habilitar Detective.

Solución de problemas al pasar de un servicio a otro

Para usar el paso de servicio, se deben cumplir los siguientes criterios:

- Su cuenta debe ser una cuenta de administrador tanto de Detective como del servicio desde el que está pasando.
- Ha asumido un rol entre cuentas que otorga a su cuenta de administrador acceso al gráfico de comportamiento.

Para obtener más información sobre la recomendación de alinear las cuentas de administrador, consulta Alineación recomendada con Amazon GuardDuty y AWS Security Hub.

Si el paso de servicio no funciona, compruebe lo siguiente:

- ¿El resultado pertenece a una cuenta de miembro habilitada en su gráfico de comportamiento? Si la cuenta asociada no fue invitada al gráfico de comportamiento como cuenta de miembro, el gráfico de comportamiento no contiene datos de esa cuenta.

  Si una cuenta de miembro invitada no ha aceptado la invitación, el gráfico de comportamiento no contiene datos de esa cuenta.
- ¿Se ha archivado el resultado? El Detective no recibe los hallazgos archivados de GuardDuty.
- ¿El resultado se produjo antes de que Detective comenzara la ingesta de datos en su gráfico de comportamiento? Si el resultado no están presente en los datos de ingesta de Detective, el gráfico de comportamiento no contiene datos correspondientes.
- ¿El resultado proviene de la región correcta? Cada gráfico de comportamiento es específico de una región. Un gráfico de comportamiento no contiene datos de otras regiones.

Desplazarse al perfil de una entidad o a la descripción general de un resultado mediante una URL

Para desplazarse a un perfil de entidad o a la descripción general de un resultado en Amazon Detective, puede usar una URL que proporcione un enlace directo. La URL identifica el resultado o la entidad. También puede especificar el rango temporal que se utilice en el perfil. Detective mantiene hasta un año de datos de eventos históricos.

Formato de URL de perfil

> **Note**
>
> Si utiliza el formato de URL anterior, Detective le redirigirá automáticamente a la URL nueva. El formato anterior de la URL era el siguiente: https://console.aws.amazon.com/detective/home?region=*Region*#*type*/*namespace*/*instanceID*?*parameters*

El nuevo formato de URL del perfil es el siguiente:

- Para entidades: https://console.aws.amazon.com/detective/home?region=*Region*#*entities*/*namespace*/*instanceID*?*parameters*
- Para resultados: https://console.aws.amazon.com/detective/home?region=*Region*#*findings*/*instanceID*?*parameters*

La URL requiere los siguientes valores:

Region

La región que desea utilizar.

type

El tipo de elemento del perfil al que se está desplazando.

- `entities`: indica que se está desplazando a un perfil de entidad.
- `findings`: indica que se está desplazando a la descripción general de un resultado.

namespace

Para las entidades, el espacio de nombre es el nombre del tipo de entidad.

- `AwsAccount`
- `AwsRole`
- `AwsRoleSession`
- `AwsUser`
- `Ec2Instance`
- `FederatedUser`
- `IpAddress`
- `S3Bucket`
- `UserAgent`
- `FindingGroup`
- `KubernetesSubject`
- `ContainerPod`
- `ContainerCluster`
- `ContainerImage`

instanceID

El identificador de instancia del resultado o entidad.

- En el caso de un GuardDuty hallazgo, el identificador del GuardDuty hallazgo.
- En el caso de una AWS cuenta, el identificador de la cuenta.
- En el caso de los AWS roles y los usuarios, el ID principal del rol o del usuario.

- Para los usuarios federados, el ID de entidad principal del usuario federado. El ID de entidad principal es `<identityProvider>:<username>` o `<identityProvider>:<audience>:<username>`.
- Para las direcciones IP, la dirección IP.
- Para los agentes de usuario, el nombre del agente de usuario.
- Para instancias de EC2, el ID de instancia.
- Para las sesiones de rol, el identificador de sesión. El identificador de sesión del rol utiliza el formato `<rolePrincipalID>:<sessionName>`.
- Para los buckets de S3, el nombre del bucket.
- Para FindingGroups un UUID. Por ejemplo, `ca6104bc-a315-4b15-bf88-1c1e60998f83`
- Para los recursos de EKS, use los siguientes formatos:
  - Clúster de EKS: `<clusterName>~<accountId>~EKS`
  - `Módulo de Kubernetes: ~ ~ ~EKS` <podUid><clusterName><accountId>
  - Sujeto de Kubernetes: `<subjectName>~<clusterName>~<accountId>`
  - Imagen de contenedor: `<registry>/<repository>:<tag>@<digest>`

  El resultado o entidad deben estar asociados a una cuenta habilitada en el gráfico de comportamiento.

La URL también puede incluir los siguientes parámetros opcionales, que se usan para establecer el rango temporal. Para obtener más información sobre el rango temporal y cómo se usa en los perfiles, consulte the section called “Administración del rango temporal”.

`scopeStart`

Hora de inicio del rango temporal que se usará en el perfil. La hora de inicio debe situarse entre los últimos 365 días.

El valor es la marca temporal en formato de tiempo Unix.

Si proporciona una hora de inicio pero no una hora de finalización, el rango temporal finaliza a la hora actual.

`scopeEnd`

Hora de finalización del rango temporal que se usará en el perfil.

El valor es la marca temporal en formato de tiempo Unix.

Si proporciona una hora de finalización, pero no una hora de inicio, el rango temporal incluye todo el tiempo anterior a la hora de finalización.

Si no especifica el rango temporal, se usará el rango temporal predeterminado.

- En el caso de los resultados, el rango temporal predeterminado usa la primera y la última vez que se observó la actividad del resultado.
- En el caso de las entidades, el rango temporal predeterminado son las 24 horas anteriores.

A continuación se muestra un ejemplo de una URL de Detective:

```
https://console.aws.amazon.com/detective/home?region=us-east-1#entities/
IpAddress/192.168.1.1?scopeStart=1552867200&scopeEnd=1552910400
```

La URL de este ejemplo proporciona las siguientes instrucciones:

- Muestra el perfil de entidad de la dirección IP 192.168.1.
- Use un rango temporal que empiece el lunes, 18 de marzo de 2019 a las 12:00:00 AM GMT y finalice el lunes, 18 de marzo de 2019 a las 12:00:00 PM GMT.

Solución de problemas de URL

Si la URL no muestra el perfil esperado, compruebe primero que la URL usa el formato correcto y que se han introducido los valores correctos.

- ¿Se ha empezado con la URL correcta (`findings` o `entities`)?
- ¿Se ha especificado el espacio de nombre correcto?
- ¿Se ha proporcionado el identificador correcto?

Si los valores son correctos, también puede comprobar lo siguiente:

- ¿El resultado o la entidad pertenecen a una cuenta de miembro habilitada en su gráfico de comportamiento? Si la cuenta asociada no fue invitada al gráfico de comportamiento como cuenta de miembro, el gráfico de comportamiento no contiene datos de esa cuenta.

  Si una cuenta de miembro invitada no ha aceptado la invitación, el gráfico de comportamiento no contiene datos de esa cuenta.

- En el caso de un resultado, ¿se ha archivado el resultado? El Detective no recibe los hallazgos archivados de Amazon GuardDuty.
- ¿El resultado o la entidad se produjeron antes de que Detective comenzara la ingesta de datos en su gráfico de comportamiento? Si el resultado o la entidad no están presentes en los datos de ingesta de Detective, el gráfico de comportamiento no contiene datos correspondientes.
- ¿El resultado o la entidad provienen de la región correcta? Cada gráfico de comportamiento es específico de una región. Un gráfico de comportamiento no contiene datos de otras regiones.

Añadir URL de resultados de Detective a Splunk

El proyecto Splunk Trumpet le permite enviar datos desde los servicios a Splunk. AWS

Puedes configurar el proyecto Trumpet para generar URL de Detectives para los hallazgos de Amazon GuardDuty . A continuación, puede utilizar estas URL para pasar directamente de Splunk a los perfiles de resultado correspondientes de Detective.

El proyecto Trumpet está disponible en https://github.com/splunk/. GitHub splunk-aws-project-trumpet

En la página de configuración del proyecto Trumpet, en AWS CloudWatch Eventos, selecciona GuardDuty URL de Detectives.

Paso de un panel de perfil a otra consola

EC2En el caso de las instancias, IAM los usuarios y los IAM roles, puede navegar directamente desde el panel del perfil de detalles hasta la consola correspondiente. La información disponible en la consola puede proporcionar información adicional para su investigación de seguridad.

En el EC2 panel de perfil de detalles de la EC2 instancia, el identificador de la instancia está vinculado a la EC2 consola de Amazon.

En el panel del perfil de detalles del usuario, el nombre de usuario está vinculado a la IAM consola.

En el panel del perfil de detalles del rol, el nombre del rol está vinculado a la IAM consola.

Paso de un panel de perfil al perfil de otra entidad

Cuando un panel de perfil contiene un identificador de una entidad diferente, suele tratarse de un enlace al perfil de esa entidad. Las excepciones son los enlaces a Amazon EC2 y a IAM las consolas

en los perfiles de EC2 instancias, IAM usuarios y IAM roles. Consulte the section called “Pasar a otra consola”.

Por ejemplo, a partir de una lista de direcciones IP, es posible que pueda ver el perfil de una dirección IP específica. De esa forma, podrá ver si hay alguna otra información disponible que le ayude a completar la investigación.

Exploración de los detalles de actividad en un panel de perfil

Durante una investigación, es posible que desee investigar más a fondo el patrón de actividad de una entidad.

En los siguientes paneles de perfil, puede ver un resumen de los detalles de actividad:

- Volumen total de API llamadas, excepto en el panel de perfil del perfil del agente de usuario
- Geolocalizaciones recién observadas
- Volumen VPC de flujo total
- VPCvolumen de flujo hacia y desde la dirección IP de búsqueda, para las búsquedas asociadas a una sola dirección IP
- Detalles del contenedor
- VPCvolumen de flujo para clústeres
- Actividad general de Kubernetes API

Los detalles de actividad pueden responder a este tipo de preguntas:

- ¿Qué direcciones IP se utilizaron?
- ¿Dónde estaban ubicadas esas direcciones IP?
- ¿Qué API llamadas realizó cada dirección IP y desde qué servicios las realizó?
- ¿Qué identificadores principales o de clave de acceso (AKIDs) se utilizaron para realizar las llamadas?
- ¿Qué recursos se utilizaron para realizar esas llamadas?
- ¿Cuántas llamadas se hicieron? ¿Cuántas tuvieron éxito y cuántas fracasaron?
- ¿Qué volumen de datos del registro de VPC flujo se envió a o desde cada dirección IP?
- ¿Qué contenedores estaban activos para un determinado clúster, imagen o pod?

Temas

- Detalles de la actividad del volumen total de API llamadas
- Detalles de actividad de una geolocalización
- Detalles de la actividad del volumen VPC de flujo total
- Actividad general de Kubernetes relacionada API con el clúster EKS

Detalles de la actividad del volumen total de API llamadas

Los detalles de la actividad del volumen total de API llamadas muestran las API llamadas que se emitieron durante un intervalo de tiempo seleccionado.

Para ver los detalles de un único intervalo de tiempo, elija el intervalo de tiempo en el gráfico.

Para ver los detalles de actividad del rango temporal actual, elija Mostrar detalles del rango temporal.

Tenga en cuenta que Detective comenzó a almacenar y mostrar el nombre del servicio para API las llamadas a partir del 14 de julio de 2021. Esa fecha aparece resaltada en el cronograma del panel de perfil. En el caso de las actividades que se produzcan antes de esa fecha, el nombre del servicio es Servicio desconocido.

Contenido de los detalles de la actividad (usuarios, funciones, cuentas, sesiones de funciones, EC2 instancias, segmentos de S3)

Para IAM los usuarios, los IAM roles, las cuentas, las sesiones de roles, EC2 las instancias y los buckets de S3, los detalles de la actividad contienen la siguiente información:

- Cada pestaña proporciona información sobre el conjunto de API llamadas que se emitieron durante el intervalo de tiempo seleccionado.

  En el caso de los buckets S3, la información refleja API las llamadas que se realizaron al bucket S3.

  Las API llamadas se agrupan según los servicios que las llamaron. En el caso de los buckets de S3, el servicio es siempre Amazon S3. Si Detective no puede determinar el servicio que emitió la llamada, la llamada aparece como Servicio desconocido.
- Para cada entrada, los detalles de actividad muestran el número de llamadas correctas y fallidas. La pestaña Direcciones IP observadas también muestra la ubicación de cada dirección IP.

- Cada entrada muestra información sobre quién realizó las llamadas. En el caso de las cuentas, los detalles de actividad identifican a los usuarios o roles. En el caso de los roles, los detalles de actividad identifican las sesiones de los roles. En el caso de los usuarios y las sesiones de roles, los detalles de la actividad identifican los identificadores de las claves de acceso (AKIDs).

  Tenga en cuenta que, a partir del 14 de julio de 2021, en el caso de los perfiles de las cuentas, los detalles de la actividad muestran los usuarios o los roles en lugar deAKIDs. En el caso de los perfiles de rol, los detalles de la actividad muestran las sesiones de rol en lugar deAKIDs. En el caso de la actividad que se produjo antes del 14 de julio de 2021, el llamante aparece como Recurso desconocido.

Los detalles de actividad contienen las siguientes pestañas:

Direcciones IP observadas

Muestra inicialmente la lista de direcciones IP utilizadas para emitir API llamadas.

Puede ampliar cada dirección IP para mostrar la lista de API llamadas que se emitieron desde esa dirección IP. Las API llamadas se agrupan por los servicios que las han llamado. En el caso de los buckets de S3, el servicio es siempre Amazon S3. Si Detective no puede determinar el servicio que emitió la llamada, la llamada aparece como Servicio desconocido.

A continuación, puede ampliar cada API llamada para mostrar la lista de personas que llaman desde esa dirección IP. Según el perfil, la persona que llama puede ser un usuario, un rol, una sesión de rol o. AKID

APImétodo por servicio

Muestra inicialmente la lista de API llamadas emitidas. Las API llamadas se agrupan por los servicios que las emitieron. En el caso de los buckets de S3, el servicio es siempre Amazon S3. Si Detective no puede determinar el servicio que emitió la llamada, la llamada aparece como Servicio desconocido.

Puede ampliar cada API método para mostrar la lista de direcciones IP desde las que se emitieron las llamadas.

A continuación, puede expandir cada dirección IP para mostrar la lista de las AKIDs API llamadas emitidas desde esa dirección IP.

ID de recurso o clave de acceso

Muestra inicialmente la lista de usuarios, roles, sesiones de rol o AKIDs que se utilizaron para realizar API llamadas.

Puede ampliar cada persona que llama para mostrar la lista de direcciones IP desde las que la persona que llama ha realizado llamadas. API

A continuación, puede ampliar cada dirección IP para mostrar la lista de API llamadas emitidas desde esa dirección IP por la persona que llamó. Las API llamadas se agrupan por los servicios que las emitieron. En el caso de los buckets de S3, el servicio es siempre Amazon S3. Si Detective no puede determinar el servicio que emitió la llamada, la llamada aparece como Servicio desconocido.

Contenido de los detalles de actividad (direcciones IP)

En el caso de las direcciones IP, los detalles de actividad contienen la siguiente información:

- Cada pestaña proporciona información sobre el conjunto de API llamadas que se emitieron durante el intervalo de tiempo seleccionado. Las API llamadas se agrupan según los servicios que las emitieron. Si Detective no puede determinar el servicio que emitió la llamada, la llamada aparece como Servicio desconocido.
- Para cada entrada, los detalles de actividad muestran el número de llamadas correctas y fallidas.

Los detalles de actividad contienen las siguientes pestañas:

Recurso

Muestra inicialmente la lista de recursos que emitieron API llamadas desde la dirección IP.

Para cada recurso, la lista incluye el nombre del recurso, el tipo y la AWS cuenta.

Puede ampliar cada recurso para mostrar la lista de API llamadas que el recurso emitió desde la dirección IP. Las API llamadas se agrupan por los servicios que las emitieron. Si Detective no puede determinar el servicio que emitió la llamada, la llamada aparece como Servicio desconocido.

APImétodo por servicio

Muestra inicialmente la lista de API llamadas emitidas. Las API llamadas se agrupan por los servicios que las emitieron. Si Detective no puede determinar el servicio que emitió la llamada, la llamada aparece como Servicio desconocido.

Puede ampliar cada API llamada para mostrar la lista de recursos que emitieron la API llamada desde la dirección IP durante el período de tiempo seleccionado.

Ordenar los detalles de actividad

Puede ordenar los detalles de actividad por cualquiera de las columnas de la lista.

Al ordenar utilizando la primera columna, solo se ordena la lista de nivel superior. Las listas de nivel inferior siempre se ordenan según el número de API llamadas realizadas correctamente.

Filtrar los detalles de actividad

Puede utilizar las opciones de filtrado para centrarse en subconjuntos o aspectos específicos de la actividad representados en los detalles de actividad.

En todas las pestañas, puede filtrar la lista por cualquiera de los valores de la primera columna.

Para añadir un filtro

1. Elija el cuadro de filtros.
2. En Propiedades, elija la propiedad que desee utilizar para el filtrado.
3. Proporcione el valor que se va a utilizar para el filtrado. El filtro admite valores parciales. Por ejemplo, si filtra por API método, si filtra por**`Instance`**, los resultados incluyen cualquier API operación que tenga `Instance` su nombre. Por lo tanto, ambos `ListInstanceAssociations` y `UpdateInstanceInformation` coincidirían.

   Para los nombres, API métodos y direcciones IP de los servicios, puede especificar un valor o elegir un filtro integrado.

   En APISubcadenas comunes, elija la subcadena que represente el tipo de operación, como `ListCreate`, o. `Delete` APIEl nombre de cada método comienza por el tipo de operación.

   En el caso de CIDRlos patrones, puede optar por incluir solo direcciones IP públicas, direcciones IP privadas o direcciones IP que coincidan con un CIDR patrón específico.
4. Elige una opción booleana ***`Resource`*** o bien ***`Service`***: Contiene o! : No contiene; o ***`IP address`*** = es igual a ***`API method`*** o! : No equivale a configurar filtros.

Para eliminar un filtro, elija el icono x de la parte superior derecha.

Para borrar los filtros seleccionados, elija Borrar filtros.

Selección del intervalo de tiempo para los detalles de actividad

Cuando se muestran los detalles de actividad por primera vez, el intervalo de tiempo es el rango temporal o un intervalo de tiempo seleccionado. Puede cambiar el intervalo de tiempo de los detalles de actividad.

Para cambiar el intervalo de tiempo de los detalles de actividad

1. Elija Editar.
2. En Editar franja horaria, elija las horas de inicio y de finalización que desea usar.

   Para configurar la franja horaria con el rango temporal predeterminado del perfil, elija Establecer el rango temporal predeterminado.
3. Elija Actualizar periodo.

El intervalo de tiempo para los detalles de actividad aparece resaltado en los gráficos del panel de perfil.

Consulta de registros sin procesar

Amazon Detective se integra con Amazon Security Lake, lo que permite consultar y recuperar datos de registros sin procesar almacenados por Security Lake. Para obtener más información sobre esta integración, consulte Integración de Detectives con Security Lake.

Con esta integración puede recopilar y consultar registros y eventos de los siguientes orígenes que Security Lake admite de forma nativa.

- AWS CloudTrail eventos de gestión de la versión 1.0 y posteriores

- Amazon Virtual Private Cloud (AmazonVPC) Flow Logs versión 1.0 y versiones posteriores
- Registro de auditoría de Amazon Elastic Kubernetes Service (EKSAmazon) versión 2.0

> **Note**
>
> No hay recargos adicionales por consultar registros de datos sin procesar en Detective. Los cargos por uso de otros AWS servicios, incluido Amazon Athena, se seguirán aplicando a las tarifas publicadas.

Para consultar registros sin procesar

1. Elija Mostrar los detalles del rango de tiempo.
2. Desde aquí puede empezar a Consultar registros sin procesar.
3. En la tabla Vista previa del registro sin procesar puede ver los registros y los eventos recuperados consultando datos de Security Lake. Para obtener más información sobre los registros de eventos sin procesar, puede ver los datos que se muestran en Amazon Athena.

   En la tabla Registros de consulta sin procesar, puede Cancelar solicitud de consulta, Ver resultados en Amazon Athena y Descargar resultados como archivo de valores separados por comas (.csv).

Si ve registros en Detective, pero la consulta no devuelve resultados, podría deberse a los siguientes motivos.

- Es posible que los registros sin procesar pasen a estar disponibles en Detective antes de mostrarse en tablas de registros de Security Lake. Inténtelo de nuevo más tarde.
- Es posible que falten registros en Security Lake. Si esperó durante un período prolongado, significa que faltan registros en Security Lake. Póngase en contacto con el administrador de Security Lake para solucionar el problema.

Detalles de actividad de una geolocalización

Los detalles de la actividad de las geolocalizaciones observadas recientemente muestran las API llamadas que se emitieron desde una geolocalización durante ese período. Las API llamadas incluyen todas las llamadas emitidas desde la geolocalización. No se limitan a las llamadas que

utilizaron la entidad de resultado o perfil. En el caso de los grupos S3, las llamadas de actividad son API llamadas realizadas al segmento S3.

El Detective determina la ubicación de las solicitudes mediante bases de datos de MaxMind GeoIP. MaxMind informa que sus datos son muy precisos a nivel de país, aunque la precisión varía según factores como el país y el tipo de IP. Para obtener más información MaxMind, consulte Geolocalización de MaxMind IP. Si cree que alguno de los datos de GeoIP es incorrecto, puede enviar una solicitud de corrección a Maxmind en MaxMind Correct Geo Data. IP2

Las API llamadas se agrupan por los servicios que las emitieron. En el caso de los buckets de S3, el servicio es siempre Amazon S3. Si Detective no puede determinar el servicio que emitió la llamada, la llamada aparece como Servicio desconocido.

Para mostrar los detalles de actividad, realice una de las siguientes acciones:

- En el mapa, elija una geolocalización.
- En la lista, elija Detalles para una geolocalización.

Los detalles de actividad sustituyen a la lista de geolocalización. Para volver a la lista de geolocalización, elija Volver a todos los resultados.

Tenga en cuenta que Detective comenzó a almacenar y mostrar el nombre del servicio para API las llamadas a partir del 14 de julio de 2021. En el caso de las actividades que se produzcan antes de esa fecha, el nombre del servicio es Servicio desconocido.

Contenido de los detalles de actividad

Cada pestaña proporciona información sobre todas las API llamadas que se emitieron desde la geolocalización durante ese período.

Para cada dirección IP, recurso y API método, la lista muestra el número de llamadas correctas y fallidasAPI.

Los detalles de actividad contienen las siguientes pestañas:

Direcciones IP observadas

Muestra inicialmente la lista de direcciones IP que se utilizaron para emitir API llamadas desde la geolocalización seleccionada.

Puede ampliar cada dirección IP para mostrar los recursos que emitieron API llamadas desde esa dirección IP. La lista muestra el nombre del recurso. Para ver el ID de la entidad principal, coloque el cursor sobre el nombre.

A continuación, puede expandir cada recurso para mostrar las API llamadas específicas que ese recurso emitió desde esa dirección IP. Las API llamadas se agrupan por los servicios que las emitieron. En el caso de los buckets de S3, el servicio es siempre Amazon S3. Si Detective no puede determinar el servicio que emitió la llamada, la llamada aparece como Servicio desconocido.

Resource

Muestra inicialmente la lista de recursos que emitieron API llamadas desde la geolocalización seleccionada. La lista muestra el nombre del recurso. Para ver el ID de la entidad principal, haga una pausa en el nombre. Para cada recurso, la pestaña Recurso también muestra el asociado Cuenta de AWS.

Puede ampliar cada usuario o rol para mostrar la lista de API llamadas emitidas por ese recurso. Las API llamadas se agrupan por los servicios que las emitieron. En el caso de los buckets de S3, el servicio es siempre Amazon S3. Si Detective no puede determinar el servicio que emitió la llamada, la llamada aparece como Servicio desconocido.

A continuación, puede ampliar cada API llamada para mostrar la lista de direcciones IP desde las que el recurso emitió la API llamada.

Ordenar los detalles de actividad

Puede ordenar los detalles de actividad por cualquiera de las columnas de la lista.

Al ordenar utilizando la primera columna, solo se ordena la lista de nivel superior. Las listas de nivel inferior siempre se ordenan según el número de llamadas realizadas correctamente. API

Filtrar los detalles de actividad

Puede utilizar las opciones de filtrado para centrarse en subconjuntos o aspectos específicos de la actividad representados en los detalles de actividad.

En todas las pestañas, puede filtrar la lista por cualquiera de los valores de la primera columna.

Para añadir un filtro

1. Elija el cuadro de filtros.
2. En Propiedades, elija la propiedad que desee utilizar para el filtrado.
3. Proporcione el valor que se va a utilizar para el filtrado. El filtro admite valores parciales. Por ejemplo, si filtra por API método, si filtra por**`Instance`**, los resultados incluyen cualquier API operación que tenga `Instance` su nombre. Por lo tanto, ambos `ListInstanceAssociations` y `UpdateInstanceInformation` coincidirían.

   Para los nombres, API métodos y direcciones IP de los servicios, puede especificar un valor o elegir un filtro integrado.

En APISubcadenas comunes, elija la subcadena que represente el tipo de operación, como `ListCreate`, o. `Delete` APIEl nombre de cada método comienza por el tipo de operación.

En el caso de CIDRlos patrones, puede optar por incluir solo direcciones IP públicas, direcciones IP privadas o direcciones IP que coincidan con un CIDR patrón específico.

4. Si tiene varios filtros, elija una opción booleana para establecer cómo se conectan esos filtros.

5. Para eliminar un filtro, elija el icono x de la parte superior derecha.
6. Para borrar los filtros seleccionados, elija Borrar filtros.

Detalles de la actividad del volumen VPC de flujo total

EC2Por ejemplo, los detalles de la actividad del volumen de VPC flujo total muestran las interacciones entre la EC2 instancia y las direcciones IP durante un intervalo de tiempo seleccionado.

En el caso de un pod de Kubernetes, el volumen de VPC flujo general muestra el volumen total de bytes que entran y salen de la dirección IP asignada al pod de Kubernetes para todas las direcciones IP de destino. La dirección IP del pod de Kubernetes no es única cuando. `hostNetwork:true` En este caso, el panel muestra el tráfico hacia otros pods con la misma configuración y el nodo que los aloja.

En el caso de una dirección IP, los detalles de la actividad del volumen de VPC flujo total muestran las interacciones entre la dirección IP y las EC2 instancias durante un intervalo de tiempo seleccionado.

Para ver los detalles de un único intervalo de tiempo, elija el intervalo de tiempo en el gráfico.

Para ver los detalles de actividad para el rango temporal actual, elija Mostrar detalles del rango temporal.

Contenido de los detalles de actividad

El contenido refleja la actividad durante el intervalo de tiempo seleccionado.

EC2Por ejemplo, los detalles de la actividad contienen una entrada para cada combinación única de dirección IP, puerto local, puerto remoto, protocolo y dirección.

En el caso de una dirección IP, los detalles de la actividad contienen una entrada para cada combinación única de EC2 instancia, puerto local, puerto remoto, protocolo y dirección.

Cada entrada muestra el volumen del tráfico entrante, el volumen del tráfico saliente y si la solicitud de acceso se ha aceptado o rechazado. Al buscar perfiles, la columna Anotaciones indica si una dirección IP está relacionada con el resultado actual.

Ordenar los detalles de actividad

Puede ordenar los detalles de actividad por cualquiera de las columnas de la tabla.

De forma predeterminada, los detalles de actividad se ordenan primero por las anotaciones y, a continuación, por el tráfico entrante.

Filtrar los detalles de actividad

Para centrarse en una actividad específica, puede filtrar los detalles de actividad por los siguientes valores:

- Dirección o EC2 instancia IP
- Puerto local o remoto
- Dirección
- Protocolo
- Si la solicitud fue aceptada o rechazada

Para añadir y eliminar filtros

1. Elija el cuadro de filtros.

2. En Propiedades, elija la propiedad que desee utilizar para el filtrado.
3. Proporcione el valor que se va a utilizar para el filtrado. El filtro admite valores parciales.

   Para filtrar por dirección IP, puede especificar un valor o elegir un filtro integrado.

   En el caso de CIDRlos patrones, puedes elegir incluir solo direcciones IP públicas, direcciones IP privadas o direcciones IP que coincidan con un CIDR patrón específico.
4. Si tiene varios filtros, elija una opción booleana para establecer cómo se conectan esos filtros.

5. Para eliminar un filtro, elija el icono x de la parte superior derecha.
6. Para borrar los filtros seleccionados, elija Borrar filtros.

Selección del intervalo de tiempo para los detalles de actividad

Cuando se muestran los detalles de actividad por primera vez, el intervalo de tiempo es el rango temporal o un intervalo de tiempo seleccionado. Puede cambiar el intervalo de tiempo de los detalles de actividad.

Para cambiar el intervalo de tiempo de los detalles de actividad

1. Elija Editar.
2. En Editar franja horaria, elija las horas de inicio y de finalización que desea usar.

   Para configurar la franja horaria con el rango temporal predeterminado del perfil, elija Establecer el rango temporal predeterminado.
3. Elija Actualizar periodo.

El intervalo de tiempo para los detalles de actividad aparece resaltado en los gráficos del panel de perfil.

Muestra el volumen de tráfico de las filas seleccionadas

Al identificar las filas que son de interés, puede mostrar en los gráficos principales el volumen de tráfico de esas filas a lo largo del tiempo.

Para cada fila que desee añadir a los gráficos, seleccione la casilla de verificación. Para cada fila seleccionada, el volumen se muestra como una línea en los gráficos entrantes o salientes.

Para centrarse en el volumen de tráfico de las entradas seleccionadas, puede ocultar el volumen total. Para mostrar u ocultar el volumen de tráfico total, active la opción Tráfico total.

Mostrar el tráfico VPC de flujo de los EKS clústeres

Detective puede ver los registros de flujo de Amazon Virtual Private Cloud (AmazonVPC), que representan el tráfico que atraviesa los clústeres de Amazon Elastic Kubernetes Service (Amazon).

EKS En el caso de los recursos de Kubernetes, el contenido de los registros de VPC flujo depende de la interfaz de red de contenedores () implementada en el clúster. CNI EKS

Un EKS clúster con una configuración predeterminada usa el VPC CNI complemento Amazon. Para obtener más información, consulta Administrar VPC CNI en la Guía del EKS usuario de Amazon. El VPC CNI complemento Amazon envía el tráfico interno con la dirección IP del pod y traduce la dirección IP de origen a la dirección IP del nodo para la comunicación externa. Detective puede capturar y correlacionar el tráfico interno con el pod correcto, pero no puede hacer lo mismo con el tráfico externo.

Si quieres que Detective pueda ver el tráfico externo de tus pods, habilita la Traducción de direcciones de red de origen externo (SNAT). SNATLa activación tiene limitaciones e inconvenientes. Para obtener más información, consulta SNATlos pods en la Guía del EKS usuario de Amazon.

Si utilizas un CNI complemento diferente, Detective tiene una visibilidad limitada a los pods con`hostNetwork:true`. En el caso de estos pods, el panel VPCFlow muestra todo el tráfico dirigido a la dirección IP del pod. Esto incluye el tráfico al nodo host y a cualquier pod del nodo con la `hostNetwork:true` configuración.

Detective muestra el tráfico en el panel de VPCflujo de un EKS pod para las siguientes configuraciones de EKS clúster:

- En un clúster con el VPC CNI complemento Amazon, cualquier pod con la configuración `hostNetwork:false` envía tráfico dentro VPC del clúster.
- En un clúster con el VPC CNI complemento Amazon y la configuración`AWS_VPC_K8S_CNI_EXTERNALSNAT=`**`true`**, cualquier pod que `hostNetwork:false` envíe tráfico fuera VPC del clúster.
- Cualquier pod con la configuración. `hostNetwork:true` El tráfico del nodo se mezcla con el tráfico de otros pods que tienen la configuración`hostNetwork:true`.

El Detective no muestra el tráfico en el panel de VPCflujo durante:

- En un clúster con el VPC CNI complemento Amazon y la configuración`AWS_VPC_K8S_CNI_EXTERNALSNAT=false`, cualquier pod con la configuración `hostNetwork:false` envía tráfico fuera VPC del clúster.
- En un clúster sin el VPC CNI complemento de Amazon para Kubernetes, cualquier pod con la configuración. `hostNetwork:false`
- Cualquier pod que envíe tráfico a otro pod que esté alojado en el mismo nodo.

Mostrar el VPC flujo de tráfico de Amazon compartido VPCs

Detective puede ver sus registros de flujo de Amazon Virtual Private Cloud (AmazonVPC) para compartirlosVPCs:

- Si una cuenta miembro de Detective tiene una cuenta de Amazon compartida VPC y hay otras cuentas que no son de Detective que utilizan la cuenta compartidaVPC, Detective monitorea todo el tráfico procedente de esa VPC cuenta y proporciona una visualización de todo el flujo de tráfico dentro de laVPC.
- Si tienes una EC2 instancia de Amazon dentro de un Amazon compartido VPC y el VPC propietario compartido no es miembro de Detective, Detective no supervisará el tráfico procedente delVPC. Si quieres ver el flujo de tráfico dentro delVPC, debes añadir al VPC propietario de Amazon como miembro de tu gráfico de Detectives.

Actividad general de Kubernetes relacionada API con el clúster EKS

Los detalles de la actividad general de Kubernetes API relacionada con el EKS clúster muestran el número de API llamadas de Kubernetes realizadas con éxito y sin éxito durante un intervalo de tiempo seleccionado.

Para ver los detalles de un único intervalo de tiempo, elija el intervalo de tiempo en el gráfico.

Para ver los detalles de actividad del rango temporal actual, elija Mostrar detalles del rango temporal.

Contenido de los detalles de actividad (clúster, pod, usuario, rol, sesión de rol)

Para un clúster, pod, usuario, rol o sesión de rol, los detalles de actividad contienen la siguiente información:

- Cada pestaña proporciona información sobre el conjunto de API llamadas que se emitieron durante el intervalo de tiempo seleccionado.

  En el caso de los clústeres, API las llamadas se produjeron dentro del clúster.

  En el caso de los pods, las API llamadas se dirigían al pod.

  En el caso de los usuarios, los roles y las sesiones de rol, las API llamadas las emitieron los usuarios de Kubernetes que se autenticaron como ese usuario, rol o sesión de rol.
- Para cada entrada, los detalles de actividad muestran el número de llamadas correctas, fallidas, no autorizadas y prohibidas.

- La información incluye la dirección IP, el tipo de llamada de Kubernetes, la entidad afectada por la llamada y el sujeto (cuenta de servicio o usuario) que realizó la llamada. A partir de los detalles de actividad, puede pasar a los perfiles de la dirección IP, el asunto y la entidad afectada.

Los detalles de actividad contienen las siguientes pestañas:

Asunto

Muestra inicialmente la lista de cuentas de servicio y usuarios que se utilizaron para realizar llamadas. API

Puede ampliar cada cuenta de servicio y usuario para mostrar la lista de direcciones IP desde las que la cuenta o el usuario realizaron API llamadas.

A continuación, puedes expandir cada dirección IP para mostrar las API llamadas de Kubernetes que realizó esa cuenta o usuario desde esa dirección IP.

Amplía la API llamada de Kubernetes para ver e identificar la acción `requestURI` que se realizó.

Dirección IP

Muestra inicialmente la lista de direcciones IP desde las que se realizaron las API llamadas.

Puede ampliar cada llamada para que se muestre la lista de sujetos de Kubernetes (cuentas de servicio y usuarios) que realizaron la llamada.

A continuación, puede ampliar cada asunto para incluir una lista de los tipos de API llamadas realizadas por el sujeto durante el período de tiempo establecido.

Amplía el tipo de API llamada para ver la solicitud URI para identificar la acción que se realizó.

llamada de Kubernetes API

Muestra inicialmente la lista de verbos de llamada de KubernetesAPI.

Puedes expandir cada API verbo para mostrar el asociado a esa acción. requestURIs

A continuación, puedes ampliar cada solicitud URI para ver el asunto de Kubernetes (cuentas de servicio y usuarios) que realizó la llamada. API

Amplía el asunto para ver cuál usó IPs ese sujeto para realizar la llamada. API

Ordenar los detalles de actividad

Puede ordenar los detalles de actividad por cualquiera de las columnas de la lista.

Al ordenar utilizando la primera columna, solo se ordena la lista de nivel superior. Las listas de nivel inferior siempre se ordenan según el número de API llamadas realizadas correctamente.

Filtrar los detalles de actividad

Puede utilizar las opciones de filtrado para centrarse en subconjuntos o aspectos específicos de la actividad representados en los detalles de actividad.

En todas las pestañas, puede filtrar la lista por cualquiera de los valores de la primera columna.

Selección del intervalo de tiempo para los detalles de actividad

Cuando se muestran los detalles de actividad por primera vez, el intervalo de tiempo es el rango temporal o un intervalo de tiempo seleccionado. Puede cambiar el intervalo de tiempo de los detalles de actividad.

Para cambiar el intervalo de tiempo de los detalles de actividad

1. Elija Editar.
2. En Editar franja horaria, elija las horas de inicio y de finalización que desea usar.

   Para configurar la franja horaria con el rango temporal predeterminado del perfil, elija Establecer el rango temporal predeterminado.
3. Elija Actualizar periodo.

El intervalo de tiempo para los detalles de actividad aparece resaltado en los gráficos del panel de perfil.

Usar las directrices de los paneles de perfil durante una investigación

Cada panel de perfil está diseñado para proporcionar respuestas a preguntas específicas que surjan al llevar a cabo una investigación y analizar la actividad de las entidades relacionadas.

Las directrices proporcionadas para cada panel de perfil le ayudan a encontrar estas respuestas.

Las directrices de los paneles de perfil comienzan con una sola frase en el propio panel. Estas directrices proporcionas una breve explicación de los datos presentados en el panel.

Para ver directrices más detalladas de un panel, elija Más información en el encabezado del panel. Estas directrices ampliadas aparecen en el panel de ayuda.

Las directrices pueden proporcionar estos tipos de información:

- Una descripción general del contenido del panel
- Cómo usar el panel para responder a las preguntas pertinentes
- Pasos siguientes recomendados según las respuestas

Administración del rango temporal

Personalice el rango temporal utilizado para limitar los datos que se muestran en los perfiles de entidad.

Los gráficos, los cronogramas y otros datos que se muestran en los perfiles de entidad se basan en el rango temporal actual. El rango temporal es el resumen de actividad de una entidad a lo largo del tiempo. Este aparece en la parte superior derecha de cada perfil en la consola de Amazon Detective. Los datos que se muestran en esos gráficos, cronogramas y otras visualizaciones se basan en el rango temporal. En algunos paneles de perfil, se añade tiempo adicional antes y después del rango temporal para proporcionar contexto. En Detective, todas las marcas temporales se muestran en UTC de forma predeterminada. Para seleccionar su zona horaria local, cambie las Preferencias de marca temporal. Para actualizar la Preferencia de marca temporal, consulte the section called “Establecer el formato de marca temporal”.

El análisis de Detective utiliza el rango temporal para comprobar si existe actividad inusual. El proceso de análisis obtiene la actividad durante el rango temporal y, a continuación, la compara con la actividad durante los 45 días anteriores al rango temporal. También utiliza ese periodo de 45 días para generar líneas de base de actividad.

En la descripción general de un resultado, el rango temporal refleja la primera y la última vez que se observó el resultado. Para obtener más información sobre la descripción general de un resultado, consulte the section called “Descripción general del resultado”.

A medida que avance en una investigación, puede ajustar el rango temporal. Por ejemplo, si el análisis original se basaba en la actividad de un solo día, quizás desee ampliarlo a una semana o un mes. La ampliación del periodo podría ayudar a entender mejor si la actividad se ajusta a un patrón normal o si es inusual.

También puede configurar el rango temporal para que coincida con un resultado asociado de la entidad actual.

Al cambiar el rango temporal, Detective repite su análisis y actualiza los datos mostrados en función del nuevo rango temporal.

El rango temporal no puede ser inferior a una hora ni superior a un año. La hora de inicio y de finalización deben comenzar en una hora.

Establecer fechas y horas de inicio y de finalización específicas

Puede establecer las fechas de inicio y de finalización del rango temporal desde la consola de Detective.

Para establecer horas específicas de inicio y de finalización para el nuevo rango temporal

1. Abra la consola de Amazon Detective, en https://console.aws.amazon.com/detective/.
2. En un perfil de entidad, elija el rango temporal.
3. En el panel Editar el rango temporal, en Iniciar, elija la nueva fecha y hora de inicio del rango temporal. Para la nueva hora de inicio, puede elegir solo la hora.
4. En Finalizar, elija la nueva fecha y hora de finalización para el rango temporal. Para la nueva hora de finalización, puede elegir solo la hora. La hora de finalización debe finalizar al menos una hora después de la hora de inicio.
5. Cuando termine de editar, para guardar los cambios y actualizar los datos que se muestran, seleccione Actualizar rango temporal.

Edición de la duración del rango temporal

Cuando se establece una duración de rango temporal, Detective establece el rango temporal en esa cantidad de tiempo desde la hora actual.

Para editar la duración del rango temporal

1. Abra la consola de Amazon Detective, en https://console.aws.amazon.com/detective/.
2. En un perfil de entidad, elija el rango temporal.
3. En el panel Editar rango temporal, junto a Histórico, elija la duración del rango temporal.

   Al especificar un intervalo de tiempo, se actualizan los ajustes de Inicio y Finalización.
4. Cuando termine de editar, para guardar los cambios y actualizar los datos que se muestran, seleccione Actualizar rango temporal.

Establecer el rango temporal en una franja horaria de resultados.

Cada resultado tiene una franja horaria asociada, que refleja la primera y la última vez que se observó el resultado. Al visualizar la descripción general de un resultado, el rango temporal cambia a la franja horaria del resultado.

Desde un perfil de entidad, puede alinear el rango temporal con la franja horaria de un resultado asociado. Esto le permite investigar la actividad que se produjo durante ese tiempo.

Para alinear el rango temporal con la franja horaria de un resultado, en el panel Resultados asociados, elija el resultado que desea utilizar.

Detective rellena los detalles del resultado y establece el rango temporal en la franja horaria del resultado.

Establecer el rango temporal en la página de resumen

Mientras revisa la página Resumen, puede ajustar el rango temporal para ver la actividad de cualquier periodo de 24 horas de los 365 días anteriores.

Para establecer el rango temporal en la página Resumen

1. Abra la consola de Amazon Detective, en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Resumen.
3. En el panel Rango temporal, junto a Resumen, puede cambiar la Fecha y hora de inicio. La hora de inicio debe situarse entre los últimos 365 días.

   Al cambiar la Fecha y hora de inicio, la Fecha y hora de finalización se actualizan automáticamente a 24 horas después de la hora de inicio elegida.

> **Note**
>
> Con Detective, puede acceder a datos de eventos históricos de hasta un año de antigüedad. Para obtener más información sobre los datos de origen en Detective, consulte Datos de origen utilizados en un gráfico de comportamiento.

4. Cuando termine de editar, para guardar los cambios y actualizar los datos que se muestran, seleccione Actualizar rango temporal.

Visualización de los detalles de los hallazgos asociados en Detective

Cada perfil de entidad contiene un panel de resultados asociados en el que se enumeran los resultados que implicaron a la entidad durante el rango temporal actual. Un indicio de que una entidad se ha visto comprometida es su implicación en varios resultados. El tipo de resultado también puede proporcionar información sobre el tipo de actividad que es motivo de preocupación.

El panel de resultados asociados se muestra inmediatamente debajo del panel de perfil de detalles de la entidad.

La tabla incluye la siguiente información para cada resultado:

- El título del resultado, que también es un enlace a la descripción general del resultado.
- La AWS cuenta asociada al hallazgo, que también es un enlace al perfil de la cuenta
- El tipo de resultado
- La hora en la que se observó el resultado por primera vez
- La hora más reciente en la que se observó el resultado
- La gravedad del resultado

Para ver los detalles de un resultado, presione el botón de opción correspondiente. Detective completa el panel de detalles del resultado situado a la derecha de la página. Detective también cambia el rango temporal para que sea la franja horaria del resultado. Esto le permite centrarse en la actividad que se produjo durante ese tiempo.

Si ha accedido al perfil de la entidad desde una vista general de resultado, dicho resultado se selecciona automáticamente y se muestran los detalles del resultado.

En los detalles del resultado, para volver a la descripción general del resultado, seleccione Ver todas las entidades relacionadas.

También puede archivar el resultado. Para obtener más información, consulta Archivar un GuardDuty hallazgo de Amazon.

Visualización de detalles de entidades de gran volumen en Detective

En el gráfico de comportamiento, Amazon Detective hace un seguimiento de las relaciones entre entidades. Por ejemplo, cada gráfico de comportamiento registra cuándo un AWS usuario crea un AWS rol y cuándo una EC2 instancia se conecta a una dirección IP.

Cuando una entidad tiene demasiadas relaciones durante un periodo de tiempo, Detective no puede almacenar todas las relaciones. Cuando esto ocurre durante el rango temporal actual, Detective lo notifica. Detective también proporciona una lista de apariciones de entidades de gran volumen.

¿Qué es una entidad de gran volumen?

Durante un intervalo de tiempo dado, una entidad puede ser el origen o el destino de un número extremadamente elevado de conexiones. Por ejemplo, una EC2 instancia puede tener conexiones desde millones de direcciones IP.

Detective mantiene un límite del número de conexiones que puede admitir durante cada intervalo de tiempo. Si una entidad supera ese límite, Detective descarta las conexiones correspondientes a ese intervalo de tiempo.

Por ejemplo, supongamos que el límite es de 100 000 000 de conexiones por intervalo de tiempo. Si una EC2 instancia está conectada por más de 100 000 000 de direcciones IP durante un intervalo de tiempo, el Detective descarta las conexiones de ese intervalo de tiempo.

No obstante, es posible que pueda analizar la actividad en función de la entidad situada en el otro extremo de la relación. Para continuar con el ejemplo, si bien una EC2 instancia puede estar conectada desde millones de direcciones IP, una sola dirección IP se conecta a muchas menos instancias. EC2 Cada perfil de direcciones IP proporciona detalles sobre las EC2 instancias a las que se conectó la dirección IP.

Ver la notificación de entidad de gran volumen en un perfil

Detective muestra un aviso en la parte superior del perfil de un resultado o entidad si el rango temporal incluye un intervalo de tiempo en el que la entidad tiene un gran volumen. En el caso de los perfiles de resultado, el aviso es para la entidad implicada.

El aviso incluye la lista de relaciones que tienen intervalos de tiempo de gran volumen. Cada entrada de la lista contiene una descripción de la relación y el inicio del intervalo de tiempo de gran volumen.

Un intervalo de tiempo de gran volumen puede ser un indicador de actividad sospechosa. Para saber qué otra actividad se produjo al mismo tiempo, puede centrar su investigación en un intervalo de tiempo de gran volumen. El aviso de entidad de gran volumen incluye una opción para establecer el rango temporal en ese intervalo de tiempo.

Para establecer el rango temporal en un intervalo de tiempo de gran volumen

1. En el aviso de entidad de gran volumen, elija el intervalo de tiempo.
2. En el menú emergente, elija Aplicar rango temporal.

Ver la lista de entidades de gran volumen para el rango temporal actual

La página Entidades de gran volumen contiene una lista de intervalos de tiempo y entidades de gran volumen durante el rango temporal actual.

Visualización de la página Entidades de gran volumen

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Entidades de gran volumen.

Cada entrada de la lista contiene la siguiente información:

- El inicio del intervalo de tiempo de gran volumen
- El identificador y el tipo de entidad
- La descripción de la relación, como «EC2instancia conectada desde una dirección IP»

Puede filtrar y ordenar la lista por cualquiera de las columnas. También puede desplazarse al perfil de la entidad implicada.

Navegación al perfil de una entidad

1. En la lista Entidades de gran volumen, elija la fila desde la que desea desplazarse.
2. Seleccione Ver perfil con rango de tiempo de gran volumen.

Cuando se utiliza esta opción para desplazarse a un perfil de entidad, el rango temporal se establece de la siguiente manera:

- El rango temporal comienza 30 días antes del intervalo de tiempo de gran volumen.
- El rango temporal finaliza al final del intervalo de tiempo de gran volumen.

Buscando un hallazgo o entidad en Detective

Con la función de búsqueda de Amazon Detective, puede buscar un resultado o una entidad. Desde los resultados de búsqueda, puede desplazarse hasta el perfil de una entidad o la descripción general de un resultado. Si la búsqueda arroja más de 10 000 resultados, se mostrarán solo los 10 000 primeros. Al cambiar el orden de clasificación, cambian los resultados devueltos.

Puede exportar los resultados de búsqueda a un archivo de valores separados por comas (.csv). Este archivo contiene los datos devueltos en la página de búsqueda. Los datos se exportan en formato de valores separados por comas (CSV). El nombre de archivo de los datos exportados sigue el patrón del formato detective-page-panel-yyyy -mm-dd.csv. Puede enriquecer sus investigaciones de seguridad manipulando los datos mediante otros AWS servicios, aplicaciones de terceros o programas de hojas de cálculo que CSV admitan la importación.

> **Note**
>
> Si hay una exportación en curso, espere a que se complete antes de intentar exportar datos adicionales.

Completar la búsqueda

Para completar la búsqueda, elija el tipo de entidad que desea buscar. A continuación, proporcione el identificador exacto o el identificador con caracteres comodín `*` o `?`. Para buscar un rango de direcciones IP, también puedes usar anotaciones CIDR o puntos. Vea los siguientes ejemplos de cadenas de búsqueda:

Para las direcciones IP:

- `1.0.*.*`
- `1.0.133.*`
- `1.0.0.0/16`
- `0.239.48.198/31`

Para todos los demás tipos de entidades:

- `Admin`

- `ad*`
- `ad*n`
- `ad*n*`
- `adm?n`
- `a?m*`
- `*min`

Se admiten los siguientes identificadores para cada tipo de entidad:

- En el caso de Findings, el identificador de búsqueda o el nombre del recurso de búsqueda de Amazon (ARN).
- En el AWS caso de las cuentas, el identificador de la cuenta.
- Para los AWS roles y AWS los usuarios, el ID principal, el nombre o elARN.
- En el caso de los clústeres de contenedores, el nombre del clúster oARN.
- Para las imágenes de contenedor, el repositorio o el resumen completo de la imagen de contenedor.
- En el caso de los pods o las tareas de contenedores, el nombre UID del pod o el del pod.
- Por EC2 ejemplo, el identificador de la instancia o elARN.
- Para un grupo de resultados, el identificador del grupo de resultados.
- En el caso de las direcciones IP, la dirección en CIDR notación de puntos.
- Para los sujetos de Kubernetes (cuentas de servicio o usuarios), el nombre.
- Para una sesión de rol, puede usar cualquiera de los siguientes valores de búsqueda:
  - El identificador de sesión del rol.

    El identificador de sesión del rol utiliza el formato `<rolePrincipalID>:<sessionName>`.

    A continuación se muestra un ejemplo: `AROA12345678910111213:MySession`.
  - Sesión de rol ARN
  - Nombre de la sesión
  - ID de entidad principal del rol asumido
  - Nombre del rol asumido
- En el caso de los buckets de S3, el nombre del bucket o bucketARN.

- Para los usuarios federados, el ID de la entidad principal o el nombre de usuario. El ID de entidad principal es `<identityProvider>:<username>` o `<identityProvider>:<audience>:<username>`.
- Para los agentes de usuario, el nombre del agente de usuario.

Búsqueda de un resultado o entidad

1. Inicie sesión en. AWS Management Console A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Buscar.
3. En el menú Elegir tipo, elija el tipo de elemento que está buscando.

   Tenga en cuenta que, al elegir Usuario, puede buscar un usuario de AWS o un usuario federado.

   Ejemplos de sus datos contiene un conjunto de muestra de identificadores del tipo seleccionado que se encuentran en los datos del gráfico de comportamiento. Para ver el perfil de uno de los ejemplos, elija su identificador.
4. Introduzca el identificador exacto o un identificador con caracteres comodín que desea buscar.

   La búsqueda distingue entre mayúsculas y minúsculas.
5. Elija Buscar o presione Intro.

Uso de los resultados de búsqueda

Al completar la búsqueda, Detective muestra una lista de hasta 10 000 resultados coincidentes. Las búsquedas que utilizan un identificador único devuelven una única coincidencia.

En los resultados, para ir al perfil de entidad o a la descripción general del resultado, elija el identificador.

En el caso de los hallazgos, las funciones, los usuarios y las EC2 instancias, los resultados de la búsqueda incluyen la cuenta asociada. Para desplazarse hasta el perfil de la cuenta, elija el identificador de la cuenta.

Solución de problemas de búsqueda

Si Detective no encuentra el resultado o la entidad, compruebe primero que ha introducido el identificador correcto. Si el identificador es correcto, también puede comprobar lo siguiente:

- ¿El resultado o la entidad pertenecen a una cuenta de miembro habilitada en el gráfico de comportamiento? Si la cuenta asociada no fue invitada al gráfico de comportamiento como cuenta de miembro, el gráfico de comportamiento no contiene datos de esa cuenta.

  Si una cuenta de miembro invitada no ha aceptado la invitación, el gráfico de comportamiento no contiene datos de esa cuenta.
- En el caso de un resultado, ¿se ha archivado el resultado? El Detective no recibe los hallazgos archivados de Amazon GuardDuty.
- ¿El resultado o la entidad se produjeron antes de que Detective comenzara la ingesta de datos en su gráfico de comportamiento? Si el resultado o la entidad no están presentes en los datos de ingesta de Detective, el gráfico de comportamiento no contiene datos correspondientes.
- ¿El resultado o la entidad provienen de la región correcta? Cada gráfico de comportamiento es específico de un Región de AWS. Un gráfico de comportamiento no contiene datos de otras regiones.

Gestión de cuentas en Detective

Cuando una cuenta habilita Detective, se convierte en la cuenta de administrador del gráfico de comportamiento y elige las cuentas de miembros para ese gráfico. Una cuenta de administrador puede invitar a las cuentas a unirse a un gráfico de comportamiento. Cuando la cuenta acepta la invitación, Detective la habilita como cuenta de miembro. Las cuentas de miembros que se agregan por invitación pueden eliminarse del gráfico de comportamiento.

Cuando una cuenta se habilita como cuenta de miembro, Detective comienza a ingerir y extraer los datos de la cuenta de miembro para el gráfico de comportamiento.

Un gráfico de comportamiento contiene datos de una o varias cuentas. Un gráfico de comportamiento puede contener hasta 1200 cuentas de miembros.

Si está integrado con AWS Organizations, la cuenta de administración de la organización designa la cuenta de administrador de Detectives de la organización. La cuenta de administrador de Detective se convierte en la cuenta de administrador del gráfico de comportamiento de la organización. La cuenta de administrador de Detective puede habilitar cualquier cuenta de la organización como cuenta de miembro en el gráfico de comportamiento de la organización. Las cuentas de la organización no pueden eliminarse del gráfico de comportamiento de la organización.

Detective cobra a todas las cuentas por los datos que aportan a cada gráfico de comportamiento. Para obtener información sobre el seguimiento del volumen de datos de cada cuenta en un gráfico de comportamiento, consulte Previsión y supervisión de los costes de Amazon Detective.

Contenido

- Restricciones de cuentas y recomendaciones en Detective
- Uso de Organizations para gestionar cuentas con gráficos de comportamiento
- Designación del Detective administrador de una organización
- Acciones disponibles para las cuentas
- Visualización de la lista de cuentas
- Administrar las cuentas de la organización como cuentas de miembros de Detectives
- Administrar las cuentas de los miembros invitados en Detective
- Para cuentas de miembros: administración de las invitaciones y suscripciones a gráficos de comportamiento
- Efecto de las acciones de la cuenta sobre los gráficos de comportamiento

- Uso de scripts de Detective Python para administrar cuentas

Restricciones de cuentas y recomendaciones en Detective

Tenga en cuenta las siguientes restricciones y recomendaciones cuando administre cuentas en Amazon Detective.

Número máximo de cuentas miembro

Detective permite hasta 1200 cuentas de miembros en cada gráfico de comportamiento.

Si lo usas AWS Organizations para administrar cuentas, Detective muestra de forma predeterminada hasta 5000 cuentas de miembros en la página de administración de cuentas. Si desea ver todas las cuentas, seleccione Cargar todas las cuentas. Es posible que se tarden varios minutos en devolver todos los resultados.

Cuentas y regiones

Si se usa AWS Organizations para administrar cuentas, la cuenta de administración de la organización designa una cuenta de administrador de Detective para la organización. La cuenta de administrador de Detective se convierte en la cuenta de administrador del gráfico de comportamiento de la organización.

La cuenta de administrador de Detective debe ser la misma en todas las regiones. La cuenta de administración de la organización designa la cuenta de administrador de Detective de cada región por separado. Esto quiere decir que la cuenta de administrador de Detective también administra los gráficos de comportamiento de la organización y las cuentas de miembros de cada región por separado.

En el caso de las cuentas de miembros creadas mediante invitación, la asociación entre administrador y miembros se crea únicamente en la región desde la que se envía la invitación. La cuenta de administrador debe habilitar Detective en cada región, cada una con su correspondiente gráfico de comportamiento. A continuación, la cuenta de administrador invita a cada cuenta a asociarse como cuenta miembro en esa región.

Una cuenta puede ser cuenta de miembro en varios gráficos de comportamiento de la misma región. Una cuenta solo puede ser la cuenta de administrador de un gráfico de comportamiento por región. Una cuenta puede ser cuenta de administrador en distintas regiones.

Alineación de las cuentas de administrador con Security Hub y GuardDuty

Para garantizar que las integraciones con Amazon AWS Security Hub y Amazon GuardDuty funcionen sin problemas, recomendamos que la misma cuenta sea la cuenta de administrador en todos estos servicios.

Consulte the section called “Alineación recomendada con GuardDuty y AWS Security Hub”.

Concesión de los permisos necesarios para cuentas de administrador

Para asegurarte de que una cuenta de administrador tiene los permisos necesarios para gestionar su gráfico de comportamiento, adjunta la política `AmazonDetectiveFullAccess` gestionada a la cuenta IAM principal.

Reflejo de las actualizaciones en una organización en Detective

Los cambios que se efectúan en una organización no se reflejan de inmediato en Detective.

Para la mayoría de los cambios, como la inclusión y eliminación de cuentas de la organización, Detective tarda hasta una hora en recibir la notificación.

Los cambios que se producen en la cuenta de administrador de Detective designada en Organizations tardan menos tiempo en reflejarse.

Uso de Organizations para gestionar cuentas con gráficos de comportamiento

Es posible que ya disponga de un gráfico de comportamiento con cuentas de miembros que aceptaron una invitación manual. Si está inscrito AWS Organizations, siga los siguientes pasos para usar Organizations para habilitar y administrar las cuentas de los miembros en lugar de utilizar el proceso de invitación manual:

1. Designar la cuenta de administrador de Detective para una organización. En este paso, se crea el gráfico de comportamiento de la organización

   Si la cuenta de administrador de Detective ya dispone de un gráfico de comportamiento, ese gráfico de comportamiento se convierte en el gráfico de comportamiento de la organización.
2. Habilitar cuentas de la organización como cuentas de miembros en el gráfico de comportamiento de la organización.

Si el gráfico de comportamiento de la organización tiene cuentas de miembros que son cuentas de la organización, esas cuentas se habilitan automáticamente

El siguiente diagrama muestra información general de la estructura de un gráfico de comportamiento antes de la transición, la configuración en Organizations y la estructura de cuentas del gráfico de comportamiento después de la transición.

Designación de una cuenta de administrador de Detective para la organización

La cuenta de administración de la organización designa la cuenta de administrador de Detective para su organización. Consulte the section called “Designación de la cuenta de administrador de Detective”.

Para simplificar la transición, Detective recomienda que seleccione la cuenta de administrador actual como cuenta de administrador de Detective para la organización.

Si hay una cuenta de administrador delegado para Detective en Organizations, debe utilizar esa cuenta o la cuenta de administración de la organización como cuenta de administrador de Detective

De lo contrario, la primera vez que designa una cuenta de administrador de Detective que no sea la cuenta de administración de la organización, Detective indica a Organizations que convierta a esa cuenta en la cuenta de administrador delegado para Detective.

Habilitación de cuentas de la organización como cuentas de miembros

La cuenta de administrador de Detective es la cuenta de administrador del gráfico de comportamiento de la organización. La cuenta de administrador de Detective elige cuentas de la organización para habilitarlas como cuentas de miembros en el gráfico de comportamiento de la organización. Consulte the section called “Administrar las cuentas de miembros de la organización”.

En la página Cuentas, la cuenta de administrador de Detective ve todas las cuentas de la organización.

Si la cuenta de administrador de Detective ya es la cuenta de administrador de un gráfico de comportamiento, ese gráfico de comportamiento se convierte en el gráfico de comportamiento de la organización. Las cuentas de la organización que son cuentas de miembros en ese gráfico de comportamiento se habilitan automáticamente como cuentas de miembros. El estado del resto de cuentas de la organización será No es miembro.

Las cuentas de la organización son del tipo Por organización incluso si anteriormente eran cuentas miembro por invitación.

Las cuentas de miembros que no pertenecen a la organización son del tipo Por invitación.

En la página Administración de cuentas, la opción Habilitar automáticamente las nuevas cuentas de la organización permite habilitar automáticamente las nuevas cuentas a medida que se agregan a la organización. Consulte the section called “Habilitar nuevas cuentas de organización”. De forma predeterminada, esta opción está desactivada.

La primera vez que la cuenta de administrador de Detective abre la página Administración de cuentas se muestra un mensaje que contiene el botón Habilitar todas las cuentas de organización. Al elegir Habilitar todas las cuentas de organización, Detective lleva a cabo las siguientes acciones:

- Habilita todas las cuentas de la organización como cuentas de miembros.
- Activa la opción para habilitar automáticamente las nuevas cuentas de la organización.

La opción Habilitar todas las cuentas de organización también aparece en la lista de cuentas de miembros.

Designación del Detective administrador de una organización

En el gráfico de comportamiento de la organización, la cuenta de administrador de Detective gestiona la suscripción al gráfico de comportamiento de todas las cuentas de la organización.

Cómo se administra la cuenta de administrador de Detectives: la cuenta de administración de la organización designa la cuenta de administrador de Detectives de la organización en cada Región de AWS.

Establecer la cuenta de administrador de Detective como la cuenta de administrador delegado: la cuenta de administrador de Detective también se convierte en la cuenta de administrador delegado de Detective en AWS Organizations. La excepción es si la cuenta de administración de la organización se designa a sí misma como la cuenta de administrador de Detective. La cuenta de administración de la organización no puede ser un administrador delegado en Organizations.

Una vez configurada la cuenta de administrador delegado en Organizations, la cuenta de administración de la organización solo puede elegir la cuenta de administrador delegado o su propia cuenta como cuenta de administrador de Detective. Le recomendamos que elija la cuenta de administrador delegado en todas las regiones.

Creación y administración del gráfico de comportamiento de la organización: cuando la cuenta de administración de la organización elige una cuenta de administrador de detectives, Detective crea un nuevo gráfico de comportamiento para esa cuenta. Ese gráfico de comportamiento es el gráfico de comportamiento de la organización.

Si la cuenta de administrador de Detective es una cuenta de administrador para un gráfico de comportamiento existente, ese gráfico de comportamiento se convierte en el gráfico de comportamiento de la organización.

La cuenta de administrador de Detective elige cuentas de la organización para habilitarlas como cuentas de miembros en el gráfico de comportamiento de la organización.

La cuenta de administrador de Detective también puede enviar invitaciones a cuentas que no pertenecen a la organización. Para obtener más información, consulte the section called "Administrar las cuentas de miembros de la organización" y the section called "Administración de cuentas de miembros invitadas".

Permisos necesarios para configurar la cuenta de administrador de Detective: para garantizar que la cuenta de administración de la organización pueda configurar la cuenta de administrador de Detective, puede adjuntar la política `AmazonDetectiveOrganizationsAccess` gestionada a su AWS Identity and Access Management (IAM) entidades.

Designación de un administrador de Detectives

La cuenta de administración de la organización puede utilizar la consola de Detective para designar la cuenta de administrador de Detective.

No es necesario habilitar Detective para administrar la cuenta de administrador de Detective. Puede administrar la cuenta de administrador de Detective desde la página Habilitar Detective.

Enable Detective page (Console)

Para designar un administrador de Detectives desde la página Activar Detective, sigue estos pasos.

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.

2. Elija Comenzar.
3. En el panel Permisos necesarios para las cuentas de administrador, conceda los permisos necesarios a la cuenta para que pueda trabajar como administrador de Detective, con pleno acceso a todas las acciones de Detective. Para trabajar como administrador, se recomienda asociar la política `AmazonDetectiveFullAccess` a la entidad principal.
4. Seleccione Adjuntar política desde IAM para ver la política recomendada directamente en la IAM consola.
5. En función de si tiene permisos en la IAM consola, proceda de la siguiente manera:
   - Si tiene permisos para operar en la IAM consola, adjunte la política recomendada al director que utilice como Detective.
   - Si no tiene permisos para operar en la IAM consola, copie el nombre del recurso de Amazon (ARN) de la política y entréguelo a su IAM administrador. El administrador puede asociar la política en su nombre.
6. En Administrador delegado, elija la cuenta de administrador de Detective.

   Habrá unas opciones disponibles u otras en función de si ha designado o no una cuenta de administrador delegado para Detective en Organizations.

   - Si no tiene una cuenta de administrador delegado para Detective en Organizations, introduzca el identificador de la cuenta para designarla como cuenta de administrador de Detective.

     Es posible que ya tenga una cuenta de administrador y un gráfico de comportamiento a raíz del proceso de invitación manual. En ese caso, se recomienda designar esa cuenta como cuenta de administrador de Detective.

     Si tienes una cuenta de administrador delegado en Organizations for Amazon GuardDuty, AWS Security Hub, o Amazon Macie, luego Detective le pedirá que seleccione una de esas cuentas. También puede introducir una cuenta diferente.
   - Si tiene una cuenta de administrador delegado para Detective en Organizations, se le solicitará que elija esa cuenta o su propia cuenta. Le recomendamos que elija la cuenta de administrador delegado en todas las regiones.
7. Elija Delegar.

Si tiene Detective habilitado o su cuenta es una cuenta de miembro en un gráfico de comportamiento, puede designar la cuenta de administrador de Detective en la página General.

General page (Console)

Para designar un administrador de Detectives desde la página General, sigue estos pasos.

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, vaya a Configuración y elija General.
3. En el panel Políticas administradas, puede obtener más información sobre todas las políticas administradas que admite Detective. Puede conceder los permisos necesarios a una cuenta en función de las acciones que quiera permitir a los usuarios en Detective. Para trabajar como administrador, se recomienda asociar la política `AmazonDetectiveFullAccess` a la entidad principal.
4. En función de si tiene permisos en la IAM consola, proceda de la siguiente manera:
   - Si tiene permisos para operar en la IAM consola, adjunte la política recomendada al director que utilice como Detective.
   - Si no tiene permisos para operar en la IAM consola, copie el nombre del recurso de Amazon (ARN) de la política y entréguelo a su IAM administrador. El administrador puede asociar la política en su nombre.

   Habrá unas opciones disponibles u otras en función de si ha designado o no una cuenta de administrador delegado para Detective en Organizations.

   - Si no tiene una cuenta de administrador delegado para Detective en Organizations, introduzca el identificador de la cuenta para designarla como cuenta de administrador de Detective.

     Es posible que ya tenga una cuenta de administrador y un gráfico de comportamiento a raíz del proceso de invitación manual. En ese caso, se recomienda designar esa cuenta como cuenta de administrador de Detective.

     Si tienes una cuenta de administrador delegado en Organizations for Amazon GuardDuty, AWS Security Hub, o Amazon Macie, luego Detective le pedirá que seleccione una de esas cuentas. También puede introducir una cuenta diferente.

- Si tiene una cuenta de administrador delegado para Detective en Organizations, se le solicitará que elija esa cuenta o su propia cuenta. Le recomendamos que elija la cuenta de administrador delegado en todas las regiones.

5. Elija Delegar.

Detective API, AWS CLI

Para designar la cuenta de administrador de Detective, puede utilizar una API llamada o el AWS Command Line Interface. Debe usar las credenciales de la cuenta de administración de la organización.

Si ya tiene una cuenta de administrador delegado para Detective en Organizations, debe elegir esa cuenta o su propia cuenta. Se recomienda que elija la cuenta de administrador delegado.

Para designar la cuenta de administrador de Detective (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `EnableOrganizationAdminAccount`operación. Debe proporcionar el AWS identificador de cuenta de la cuenta del administrador del Detective. Para obtener el identificador de la cuenta, utilice la operación `ListOrganizationAdminAccounts`.
- AWS CLI: En la línea de comandos, ejecute el `enable-organization-admin-account`comando.

```
aws detective enable-organization-admin-account --account-id <admin account ID>
```

Ejemplo

```
aws detective enable-organization-admin-account --account-id 777788889999
```

Eliminación de la cuenta de administrador de Detective

La cuenta de administración de la organización puede eliminar la cuenta de administrador delegado en una región. Al eliminar la cuenta de administrador de Detective, Detective solo la elimina de la región actual. No cambia la cuenta de administrador delegado en Organizations.

Cuando la cuenta de administración de la organización elimina la cuenta de administrador de Detective en una región, Detective elimina el gráfico de comportamiento de la organización. Detective se deshabilita en la cuenta de administrador de Detective eliminada.

Para eliminar la cuenta de administrador delegado actual de Detective, utilice OrganizationsAPI. Al eliminar la cuenta de administrador delegado de Detective en Organizations, Detective elimina todos los gráficos de comportamiento de la organización en las que la cuenta de administrador delegado es la cuenta de administrador de Detective. Los gráficos de comportamiento de la organización que tienen la cuenta de administración de la organización como cuenta de administrador de Detective no se ven afectados.

Console

En la consola de Detective, puede eliminar la cuenta de administrador de Detective.

Al eliminar la cuenta de administrador de Detective, Detective se deshabilita en la cuenta y se elimina el gráfico de comportamiento de la organización. La cuenta de administrador de Detective solo se elimina en la región actual.

> **Important**
>
> Eliminar una cuenta de administrador de Detective no afecta a la cuenta de administrador delegado en Organizations.

Eliminación de la cuenta de administrador de Detective (página Habilitar Detective)

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. Elija Comenzar.
3. En Administrador delegado, elija Deshabilitar Amazon Detective.
4. En el cuadro de diálogo de confirmación, introduzca **`disable`** y, a continuación, elija Deshabilitar Amazon Detective.

Eliminación de una cuenta de administrador de Detective (página General)

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, vaya a Configuración y elija General.
3. En Administrador delegado, elija Deshabilitar Amazon Detective.
4. En el cuadro de diálogo de confirmación, introduzca **`disable`** y, a continuación, elija Deshabilitar Amazon Detective.

Detective API, AWS CLI

Para eliminar la cuenta de administrador de Detective, puede utilizar una API llamada o el AWS CLI. Debe usar las credenciales de la cuenta de administración de la organización.

Al eliminar la cuenta de administrador de Detective, Detective se deshabilita en la cuenta y se elimina el gráfico de comportamiento de la organización.

> **Important**
>
> Eliminar una cuenta de administrador de Detective no afecta a la cuenta de administrador delegado en Organizations.

Para eliminar la cuenta de administrador de Detective (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `DisableOrganizationAdminAccount`operación.

  Cuando utilizas el Detective API para eliminar la cuenta de administrador de Detective, solo se elimina en la región en la que se emitió la API llamada o la orden.

- AWS CLI: En la línea de comandos, ejecute el `disable-organization-admin-account`comando.

  ```
  aws detective disable-organization-admin-account
  ```

Eliminar la cuenta de administrador delegado

Al eliminar una cuenta de administrador de Detective no se elimina automáticamente la cuenta de administrador delegado en Organizations. Para eliminar la cuenta de administrador delegado de Detective, puede utilizar OrganizationsAPI.

Al eliminar la cuenta de administrador delegado, se eliminan todos los gráficos de comportamiento de la organización en las que la cuenta de administrador delegado es la cuenta de administrador de Detective. También se deshabilita Detective para la cuenta en esas regiones.

Para eliminar la cuenta de administrador delegado (OrganizationsAPI, AWS CLI)

- OrganizationsAPI: utilice la `DeregisterDelegatedAdministrator`operación. Debe proporcionar el identificador de la cuenta de administrador de Detective y la entidad principal del servicio de Detective, que es `detective.amazonaws.com`.
- AWS CLI: En la línea de comandos, ejecute el `deregister-delegated-administrator`comando.

```
aws organizations deregister-delegated-administrator --account-id <Detective
 administrator account ID> --service-principal <Detective service principal>
```

Ejemplo

```
aws organizations deregister-delegated-administrator --account-id 777788889999 --
service-principal detective.amazonaws.com
```

Acciones disponibles para las cuentas

Las cuentas de administrador y de miembros tienen acceso a las siguientes acciones de Detective. En la tabla, los valores tienen los siguientes significados:

- Cualquiera: la cuenta puede realizar la acción para todas las cuentas en la misma cuenta de administrador de Detective.
- Auto: la cuenta solo puede realizar la acción en su propia cuenta.
- Raya (–): la cuenta no puede realizar la acción.

En el gráfico de comportamiento de la organización, la cuenta de administrador de Detective elige cuentas de la organización para habilitarlas como cuentas de miembros. La cuenta de administrador puede configurar Detective para que habilite las nuevas cuentas de la organización automáticamente o habilitarlas manualmente.

Una cuenta de administrador puede invitar cuentas para que sean cuentas de miembros en un gráfico de comportamiento. Cuando una cuenta de miembro acepta la invitación y se habilita, Amazon Detective empieza a ingerir y extraer datos de la cuenta de miembro para el gráfico de comportamiento.

Si el gráfico de comportamiento no es el gráfico de comportamiento de la organización, todas las cuentas de miembros son cuentas invitadas.

La siguiente tabla refleja los permisos predeterminados para las cuentas de administrador y de miembros. Puede utilizar IAM políticas personalizadas para restringir aún más el acceso a las características y funciones de Detective.

Acción	Cuenta de administrador (organización)	Cuenta de administrador (invitación)	Miembro (organización)	Miembro (invitación)
Ver cuentas	Cualquiera	Cualquiera	Auto (ver cuentas de administrador)	Auto (ver cuentas de administrador)
Eliminar cuenta de miembros	Cualquiera Se eliminan las cuentas de invitados Las cuentas de la organización están desvinculadas	Cualquiera	–	Propia
Agregar o eliminar paquetes de origen de datos opcionales	Cualquiera (la configuración se aplica a todas las cuentas de los miembros)	Cualquiera (la configuración se aplica a todas las cuentas de los miembros)	–	–
Deshabilitar Detective	Auto	Auto	–	–
Ver los datos del gráfico de comportamiento	Cualquiera	Cualquiera	–	–

Acción	Cuenta de administrador (organización)	Cuenta de administrador (invitación)	Miembro (organización)	Miembro (invitación)
Habilitar o deshabilitar paquetes de origen de datos opcionales	Todos	Todos	–	–

Visualización de la lista de cuentas

La cuenta de administrador puede usar la consola de Detective o API ver una lista de cuentas. Esta lista puede incluir lo siguiente:

- Cuentas a las que la cuenta de administrador ha invitado a unirse al gráfico de comportamiento. Estas cuentas son del tipo Por invitación.
- Para el gráfico de comportamiento de la organización, todas las cuentas de la organización. Estas cuentas son del tipo Por organización.

Entre los resultados no se incluyen las cuentas de miembros invitadas que han rechazado una invitación o las cuentas que la cuenta de administrador ha eliminado del gráfico de comportamiento. Solo se incluyen cuentas con los siguientes estados.

Verificación en curso

Si se trata de una cuenta invitada, Detective está verificando la dirección de correo electrónico de la cuenta antes de enviar la invitación.

Si se trata de una cuenta de la organización, Detective está verificando que la cuenta pertenece a la organización. Asimismo, Detective verifica que la cuenta de administrador de Detective es quien ha habilitado la cuenta.

Error en la verificación

Se ha producido un error en la verificación. No se ha enviado la invitación o no se ha habilitado la cuenta de la organización como miembro.

Invitado

Este estado se muestra para cuentas invitadas. Se ha enviado la invitación, pero la cuenta de miembro aún no ha respondido.

No es miembro

Este estado se muestra para cuentas de la organización en el gráfico de comportamiento de la organización. La cuenta de la organización no es cuenta de miembro. No aporta datos al gráfico de comportamiento de la organización.

Habilitado

Si se trata de una cuenta invitada, la cuenta de miembro ha aceptado la invitación y aporta datos al gráfico de comportamiento.

Si se trata de una cuenta de la organización en el gráfico de comportamiento de la organización, la cuenta de administrador de Detective ha habilitado la cuenta como cuenta de miembro. La cuenta aporta datos al gráfico de comportamiento de la organización.

No habilitado

Si se trata de una cuenta invitada, la cuenta de miembro ha aceptado la invitación, pero no se ha podido habilitar.

Si se trata de una cuenta de la organización en el gráfico de comportamiento de la organización, la cuenta de administrador de Detective ha intentado habilitar la cuenta, pero la cuenta no se puede habilitar.

En el caso de las cuentas invitadas, el Detective comprueba el número de cuentas de los miembros. El número máximo de cuentas de miembros que se admite en un gráfico de comportamiento es 1200. Si el gráfico de comportamiento ya contiene 1200 cuentas de miembros, no se pueden habilitar cuentas nuevas.

El Detective comprueba si su volumen de datos está dentro de la cuota de Detective. El volumen de datos aportados a un gráfico de comportamiento debe ser inferior al volumen máximo que permite Detective. Si el volumen actual ingerido supera el límite de 10 TB por día para el volumen de datos de Behavior Graph, Detective no le permitirá añadir cuentas de miembros adicionales.

Listado de cuentas (consola)

Puede usarlo AWS Management Console para ver y filtrar su lista de cuentas.

Visualización de la lista de cuentas (consola)

1. Inicie sesión en AWS Management Console. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Administración de cuentas.

   La lista de cuentas de miembros contiene las siguientes cuentas:

   - Su cuenta
   - Cuentas a las que ha invitado a aportar datos al gráfico de comportamiento
   - En el gráfico de comportamiento de la organización, todas las cuentas de la organización

   Para cada cuenta, la lista muestra la información siguiente:

   - El identificador AWS de la cuenta.
   - Si se trata de una cuenta de la organización, el nombre de la cuenta.
   - El tipo de cuenta (Por invitación o Por organización).
   - Si se trata de una cuenta invitada, la dirección de correo electrónico del usuario raíz de la cuenta.
   - El estado de la cuenta.
   - El volumen de datos diario de la cuenta. Detective no puede obtener el volumen de datos de las cuentas que no están habilitadas como cuentas de miembros.
   - La fecha de la última actualización del estado de la cuenta.

Puede utilizar las pestañas de la parte superior de la tabla para filtrar la lista en función del estado de las cuentas de miembros. En cada pestaña se muestra el número de cuentas de miembros con el estado correspondiente.

- Elija Todos para ver todas las cuentas de miembros.
- Elija Habilitado para ver las cuentas cuyo estado es Habilitado.
- Elija No habilitado para ver las cuentas cuyo estado no sea Habilitado.

También puede agregar otros filtros a la lista de cuentas de miembros.

Adición de un filtro a la lista de cuentas del gráfico de comportamiento (consola)

1. Elija el cuadro de filtros.
2. Elija la columna por la que quiera filtrar la lista.
3. En la columna especificada, elija el valor para el filtro.
4. Para eliminar un filtro, elija el icono x de la parte superior derecha.
5. Para actualizar la lista con la información más reciente sobre el estado, elija el icono de actualización de la parte superior derecha.

Listar sus cuentas de miembros (DetectiveAPI, AWS CLI)

Puede utilizar una API llamada o la AWS Command Line Interface para ver una lista de las cuentas de los miembros en su gráfico de comportamiento.

Para obtener tu gráfico ARN de comportamiento y usarlo en la solicitud, usa la `ListGraphs`operación.

Para recuperar una lista de las cuentas de los miembros (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `ListMembers`operación. Para identificar el gráfico de comportamiento deseado, especifique el gráfico de comportamientoARN.

  Tenga en cuenta que `ListMembers` no devuelve las cuentas de la organización que no ha habilitado como cuentas de miembros o que ha desasociado del gráfico de comportamiento de la organización.
- AWS CLI: en la línea de comandos, ejecute el comando `list-members`.

  ```
  aws detective list-members --graph-arn <behavior graph ARN>
  ```

  Ejemplo:

  ```
  aws detective list-members --graph-arn arn:aws:detective:us-
  east-1:111122223333:graph:123412341234
  ```

Para recuperar detalles sobre cuentas de miembros específicas en tu gráfico de comportamiento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `GetMembers`operación. Especifique el gráfico de comportamiento ARN y la lista de identificadores de cuenta para las cuentas de los miembros.
- AWS CLI: en la línea de comandos, ejecute el comando `get-members`.

```
aws detective get-members --account-ids <member account IDs> --graph-arn <behavior
 graph ARN>
```

Ejemplo:

```
aws detective get-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Administrar las cuentas de la organización como cuentas de miembros de Detectives

En el gráfico de comportamiento de la organización, la cuenta de administrador de Detective elige cuentas de la organización para habilitarlas como cuentas de miembros. De forma predeterminada, las nuevas cuentas de la organización no están habilitadas como cuentas de miembros. Su estado es No es miembro. La cuenta de administrador de Detective puede configurar Detective para que habilite automáticamente las nuevas cuentas de la organización como cuentas de miembros en el gráfico de comportamiento de la organización.

El administrador de Detective puede configurar Detective para que habilite automáticamente las nuevas cuentas de la organización como cuentas de miembros. Si elige habilitar las cuentas de la organización automáticamente, Detective comienza a habilitar las nuevas cuentas como cuentas de miembros a medida que se agregan a la organización. Detective no habilita las cuentas de la organización existentes que aún no estén habilitadas.

El Detective puede habilitar las cuentas de la organización como cuentas de miembros manualmente, si no desea habilitar automáticamente las nuevas cuentas de la organización. También pueden habilitar manualmente las cuentas de la organización disociadas. El administrador del Detective no puede habilitar una cuenta de la organización como cuenta de miembro si el gráfico de comportamiento de la organización ya tiene un máximo de 1200 cuentas habilitadas. En ese caso, el estado de la cuenta de la organización sigue siendo No es miembro.

El administrador del Detective también puede disociar las cuentas de la organización del gráfico de comportamiento de la organización. Puede desasociar una cuenta de la organización para dejar de ingerir datos de esta en el gráfico de comportamiento de la organización. Los datos que ya haya aportado la cuenta permanecerán en el gráfico de comportamiento.

Contenido

- Habilitar nuevas cuentas de la organización como cuentas de miembros de Detectives
- Habilitar las cuentas de la organización como cuentas de miembros de Detectives
- Disociar las cuentas de la organización de las cuentas de los miembros de los Detectives

Habilitar nuevas cuentas de la organización como cuentas de miembros de Detectives

La cuenta de administrador de Detective puede configurar Detective para que habilite automáticamente las nuevas cuentas de la organización como cuentas de miembros en el gráfico de comportamiento de la organización.

Cuando se añaden nuevas cuentas a la organización, se agregan a la lista de la página Administración de cuentas. En el caso de las cuentas de la organización, el Tipo es Por organización.

De forma predeterminada, las nuevas cuentas de la organización no están habilitadas como cuentas de miembros. Su estado es No es miembro.

Si elige habilitar las cuentas de la organización automáticamente, Detective comienza a habilitar las nuevas cuentas como cuentas de miembros a medida que se agregan a la organización. Detective no habilita las cuentas de la organización existentes que aún no estén habilitadas.

El Detective solo puede habilitar las cuentas de la organización como cuentas de miembros si el número máximo de cuentas de miembros para un gráfico de comportamiento es 1200. Si el gráfico de comportamiento ya contiene 1200 cuentas de miembros, no se pueden habilitar nuevas cuentas.

Console

En la página Administración de cuentas, la opción Habilitar automáticamente las nuevas cuentas de la organización permite determinar si las cuentas se habilitan automáticamente a medida que se agregan a la organización.

Habilitación automática de nuevas cuentas de la organización como cuentas de miembros

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Administración de cuentas.
3. Active Habilitar automáticamente las nuevas cuentas de la organización.

DetectiveAPI/AWS CLI

Para determinar si se deben habilitar automáticamente las nuevas cuentas de la organización como cuentas de miembros de Detective, la cuenta de administrador puede usar Detective API o AWS Command Line Interface.

Para ver y administrar la configuración, debe proporcionar el gráfico de comportamientoARN. Para obtenerlaARN, utilice la `ListGraphs`operación.

Visualización de la configuración actual para habilitar automáticamente cuentas de la organización

- DetectiveAPI: Utilice la `DescribeOrganizationConfiguration`operación.

  En la respuesta, si las nuevas cuentas de la organización se habilitan automáticamente, `AutoEnable` es `true`.
- AWS CLI: en la línea de comandos, ejecute el comando `describe-organization-configuration`.

  ```
  aws detective describe-organization-configuration --graph-arn <behavior graph ARN>
  ```

  Ejemplo

  ```
  aws detective describe-organization-configuration --graph-arn
   arn:aws:detective:us-east-1:111122223333:graph:123412341234
  ```

Habilitación automática de las nuevas cuentas de la organización

- DetectiveAPI: Utilice la `UpdateOrganizationConfiguration`operación. Para habilitar automáticamente nuevas cuentas de la organización, ajuste `AutoEnable` a `true`.
- AWS CLI: en la línea de comandos, ejecute el comando `update-organization-configuration`.

```
aws detective update-organization-configuration --graph-arn <behavior graph ARN>
 --auto-enable | --no-auto-enable
```

Ejemplo

```
aws detective update-organization-configuration --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --auto-enable
```

Habilitar las cuentas de la organización como cuentas de miembros de Detectives

Si no habilita automáticamente las nuevas cuentas de la organización, puede habilitar esas cuentas manualmente. También debe habilitar manualmente las cuentas que haya desasociado.

Comprobación de los requisitos de habilitación de una cuenta

No puede habilitar una cuenta de la organización como cuenta de miembro si el gráfico de comportamiento de la organización ya contiene el número máximo permitido de cuentas habilitadas (1200). En ese caso, el estado de la cuenta de la organización sigue siendo No es miembro. La cuenta no aporta datos al gráfico de comportamiento.

En el preciso momento en el que la cuenta de miembro puede habilitarse, Detective cambia automáticamente su estado a Habilitado. Por ejemplo, el estado de la cuenta de miembro cambia a Habilitada si la cuenta de administrador elimina las cuentas de otros miembros para dejar espacio para una cuenta.

Console

Desde la página Administración de cuentas, puede habilitar cuentas de la organización como cuentas de miembros.

Habilitación de cuentas de la organización como cuentas de miembros

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Administración de cuentas.
3. Para ver una lista con las cuentas no habilitadas, elija No habilitado.

4. Puede seleccionar cuentas de la organización específicas o habilitar todas las cuentas de la organización.

   Para habilitar cuentas de la organización seleccionadas:

   a. Seleccione todas las cuentas de la organización que desee habilitar.
   b. Elija Habilitar cuentas.

   Para habilitar todas las cuentas de la organización, elija Habilitar todas las cuentas de organización.

Detective API/AWS CLI

Puede utilizar el Detective API o el AWS Command Line Interface para habilitar las cuentas de la organización como cuentas de miembros en el gráfico de comportamiento de la organización. Para obtener tu gráfico ARN de comportamiento y usarlo en la solicitud, usa la `ListGraphs`operación.

Cómo habilitar cuentas de la organización como cuentas miembro

- DetectiveAPI: Utilice la `CreateMembers`operación. Debe proporcionar el gráficoARN.

  Especifique el identificador de cada cuenta. Las cuentas de la organización que están incluidas en el gráfico de comportamiento no reciben ninguna invitación. No necesita proporcionar una dirección de correo electrónico ni otros datos de la invitación.

- AWS CLI: en la línea de comandos, ejecute el comando `create-members`.

```
aws detective create-members --accounts AccountId=<AWS account ID> --graph-
arn <behavior graph ARN>
```

  Ejemplo

```
aws detective create-members --accounts AccountId=444455556666
 AccountId=123456789012 --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Disociar las cuentas de la organización de las cuentas de los miembros de los Detectives

Puede desasociar una cuenta de la organización para dejar de ingerir datos de esta en el gráfico de comportamiento de la organización. Los datos que ya haya aportado la cuenta permanecerán en el gráfico de comportamiento.

Al desasociar una cuenta de la organización, el estado cambia a No es miembro. Detective deja de ingerir datos de esa cuenta, aunque la cuenta permanece en la lista

Console

Desde la página Administración de cuentas, puede desasociar cuentas de la organización como cuentas de miembros.

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Administración de cuentas.
3. Para ver la lista de cuentas habilitadas, elija Habilitado.
4. Marque la casilla para cada cuenta que quiera desasociar
5. Elija Actions. A continuación, elija Desactivar cuentas.

   El estado de las cuentas desasociadas cambia a No es miembro.

Detective API/AWS CLI

Para obtener el gráfico ARN de comportamiento que se utilizará en la solicitud, utilice la `ListGraphs`operación.

Para disociar las cuentas de la organización del gráfico de comportamiento de la organización

- DetectiveAPI: Utilice la `DeleteMembers`operación. Especifique el gráfico ARN y la lista de identificadores de cuentas para las cuentas de los miembros que se van a desasociar.
- AWS CLI:: en la línea de comandos, ejecute el comando `delete-members`.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

Ejemplo

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Administrar las cuentas de los miembros invitados en Detective

Una cuenta de administrador de Detective puede invitar a las cuentas a ser cuentas miembros en su gráfico de comportamiento. Un gráfico de comportamiento puede contener hasta 1200 cuentas de miembros. Cuando una cuenta de miembro acepta la invitación y se habilita, Amazon Detective empieza a ingerir y extraer datos de la cuenta de miembro para el gráfico de comportamiento.

Para invitar a cuentas individuales, puede especificar manualmente las cuentas de los miembros a las que desea invitar a contribuir con sus datos a un gráfico de comportamiento. Si quieres añadir una lista de cuentas de miembros, puedes optar por proporcionar un archivo.csv que contenga una lista de cuentas de miembros para incluirlas en tu gráfico de comportamiento.

En el caso de los gráficos de comportamiento distintos del gráfico de comportamiento de la organización, todas las cuentas de los miembros son cuentas invitadas. La cuenta del administrador Detective también puede invitar a cuentas que no son cuentas de la organización al gráfico de comportamiento de la organización.

En general, el proceso para invitar a cuentas para que aporten datos a un gráfico de comportamiento funciona de la siguiente manera.

1. Para añadir cada cuenta de miembro, la cuenta de administrador proporciona el identificador de la AWS cuenta y la dirección de correo electrónico del usuario raíz.
2. Detective valida que la dirección de correo electrónico es la misma que la del usuario raíz de la cuenta. Si la información de la cuenta es válida, Detective envía la invitación a la cuenta de miembro.

   Detective no realiza esta validación ni envía invitaciones por correo electrónico a las cuentas de los miembros en las siguientes regiones:

   - AWS GovCloud Región (EE. UU. Este)
   - AWS GovCloud Región (EEUU-Oeste)

   Para otras regiones, puedes `DisableEmailNotification` usar la CreateMembersoperación del DetectiveAPI. Si `DisableEmailNotification` se establece en True, Detective no enviará

invitaciones a las cuentas de los miembros. Esta configuración es útil para las cuentas que se administran de forma centralizada.

3. La cuenta de miembro acepta o rechaza la invitación.

   Incluso si la cuenta de administrador no envía correos electrónicos de invitación, la cuenta de miembro debe responder a la invitación.

4. Una vez que la cuenta del miembro acepta la invitación, el Detective comienza a incorporar los datos de la cuenta del miembro al gráfico de comportamiento.
5. En el preciso momento en el que la cuenta de miembro puede habilitarse, Detective cambia automáticamente su estado a Habilitado.

   Por ejemplo, el estado de la cuenta de miembro cambia a Habilitada si la cuenta de administrador elimina las cuentas de otros miembros para dejar espacio para una cuenta.

   Si hay más de una cuenta con el estado No habilitado, Detective habilita las cuentas en el orden en el que han recibido la invitación. El proceso que comprueba si se puede habilitar una cuenta con el estado No habilitado se ejecuta cada hora.

   La cuenta de administrador también puede habilitar cuentas manualmente, en vez de esperar al proceso automático. Por ejemplo, es posible que la cuenta de administrador quiera seleccionar ciertas cuentas para habilitarlas. Para obtener información sobre cómo habilitar una cuenta de miembro, consultethe section called “Habilitación de una cuenta de miembro con el estado No habilitado”.

   Tenga en cuenta que Detective empezó a habilitar automáticamente las cuentas con el estado No habilitado a partir del 12 de mayo de 2021. Las cuentas cuyo estado era No habilitado antes de esa fecha no se habilitaron automáticamente. Por tanto, la cuenta de administrador debe habilitarlas manualmente.

La cuenta de administrador puede eliminar cuentas de miembros invitadas del gráfico de comportamiento. Detective no elimina ningún dato del gráfico de comportamiento, que se encarga de agregar datos de todas las cuentas de miembros.

Contenido

- Cómo invitar a las cuentas individuales a un gráfico de comportamiento
- Incluir una lista de las cuentas de los miembros en un gráfico de comportamiento
- Habilitación de una cuenta de miembro con el estado No habilitado

- Eliminar las cuentas de los miembros de un gráfico de comportamiento

Cómo invitar a las cuentas individuales a un gráfico de comportamiento

Puede especificar manualmente las cuentas de miembros que desea invitar para que aporten datos a un gráfico de comportamiento.

Console

Para seleccionar manualmente las cuentas de los miembros a las que invitar mediante la consola de Detective.

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Administración de cuentas.
3. Elija Acciones. A continuación, seleccione Invitar a cuentas.
4. En Agregar cuentas, elija Agregar cuentas individuales.
5. Para agregar una cuenta de miembro a la lista de invitaciones, siga los siguientes pasos.
   a. Elija Agregar cuenta.
   b. En el AWS campo ID de cuenta, introduzca el ID de AWS cuenta.
   c. En Dirección de email, escriba la dirección de correo electrónico del usuario raíz de la cuenta.
6. Para eliminar una cuenta de la lista, elija Eliminar para dicha cuenta.
7. En Personalizar el email de invitación, agregue contenido personalizado para incluirlo en el correo electrónico de invitación.

   Por ejemplo, puede utilizar este campo para proporcionar información de contacto O utilízalo para recordar a la cuenta del miembro que debe adjuntar la IAM política requerida a su usuario o rol antes de poder aceptar la invitación.
8. La IAMpolítica de cuentas de miembros contiene el texto de la IAM política obligatoria para las cuentas de miembros. El correo electrónico de invitación incluye este texto de política. Para copiarlo, elija Copiar.
9. Elija Invitar.

Detective API/AWS CLI

Puedes usar el Detective API o el AWS Command Line Interface para invitar a las cuentas de los miembros a contribuir con sus datos a un gráfico de comportamiento. Para obtener tu gráfico ARN de comportamiento y usarlo en la solicitud, usa la `ListGraphs`operación.

Para invitar a las cuentas de los miembros a un gráfico de comportamiento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `CreateMembers`operación. Debe proporcionar el gráficoARN. Para cada cuenta, especifique el identificador de la cuenta y la dirección de correo electrónico del usuario raíz.

  Si no quiere que se envíen correos electrónicos de invitación a cuentas de miembros, establezca `DisableEmailNotification` en “true”. El valor predeterminado de `DisableEmailNotification` es “false”.

  Si decide enviar correos electrónicos de invitación, puede proporcionar texto personalizado para agregarlo al correo electrónico de invitación.
- AWS CLI:: en la línea de comandos, ejecute el comando `create-members`.

  ```
  aws detective create-members --accounts AccountId=<AWS account
   ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --
  message "<Custom message text>"
  ```

  Ejemplo

  ```
  aws detective create-members --accounts
   AccountId=444455556666,EmailAddress=mmajor@example.com
   AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
   arn:aws:detective:us-east-1:111122223333:graph:123412341234 --message "This
   is Paul Santos. I need to add your account to the data we use for security
   investigation in Amazon Detective. If you have any questions, contact me at
   psantos@example.com."
  ```

  Para indicar que no se envíen correos electrónicos de invitación a cuentas de miembros, incluya `--disable-email-notification`.

```
aws detective create-members --accounts AccountId=<AWS account
 ID>,EmailAddress=<root user email address> --graph-arn <behavior graph ARN> --
disable-email-notification
```

Ejemplo

```
aws detective create-members --accounts
 AccountId=444455556666,EmailAddress=mmajor@example.com
 AccountId=123456789012,EmailAddress=jstiles@example.com --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234 --disable-email-
notification
```

Incluir una lista de las cuentas de los miembros en un gráfico de comportamiento

Desde la consola de Detective puede proporcionar un archivo `.csv` que contenga una lista de las cuentas de miembros que desea invitar a un gráfico de comportamiento.

La primera línea del archivo es el encabezado. A continuación se muestra una cuenta por línea. Cada entrada de la cuenta de un miembro contiene el ID de la AWS cuenta y la dirección de correo electrónico del usuario raíz de la cuenta.

Ejemplo:

```
Account ID,Email address
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Cuando Detective procesa el archivo, ignora las cuentas ya invitadas, excepto si el estado de la cuenta es Error en la verificación. Ese estado indica que la dirección de correo electrónico proporcionada para la cuenta no coincide con la dirección de correo electrónico del usuario raíz de la cuenta. En ese caso, Detective elimina la invitación original y vuelve a intentar verificar la dirección de correo electrónico para enviar la invitación.

Con esta opción también se incluye una plantilla para que cree su propia lista de cuentas.

Invitación de cuentas de miembros desde una lista .csv (consola)

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Administración de cuentas.
3. Elija Acciones. A continuación, seleccione Invitar a cuentas.
4. En Agregar cuentas, elija Agregar desde .csv.
5. Para descargar un archivo de plantilla con el que empezar a trabajar, elija Descargar la plantilla CSV.
6. Para seleccionar el archivo que contiene la lista de cuentas, elija Elegir un archivo CSV.
7. En Revisar cuentas miembro, verifique la lista de cuentas de miembros que Detective ha encontrado en el archivo.
8. En Personalizar el email de invitación, agregue contenido personalizado para incluirlo en el correo electrónico de invitación.

   Por ejemplo, puede proporcionar información de contacto o recordar a la cuenta del miembro la IAM política requerida.
9. La IAMpolítica de cuentas de miembros contiene el texto de la IAM política obligatoria para las cuentas de miembros. El correo electrónico de invitación incluye este texto de política. Para copiarlo, elija Copiar.
10. Elija Invitar.

Añadir una lista de cuentas de miembros en todas las regiones

Detective proporciona un script de Python de código abierto GitHub que le permite hacer lo siguiente:

- Agregar una lista especificada de cuentas de miembros al gráfico de comportamiento de una cuenta de administrador en una lista especificada de regiones.
- Si la cuenta de administrador no cuenta con un gráfico de comportamiento en una región, el script también habilita Detective y crea el gráfico de comportamiento en dicha región.
- Enviar correos electrónicos de invitación a cuentas de miembros.
- Aceptar automáticamente las invitaciones enviadas a cuentas de miembros.

Para obtener información sobre cómo configurar y utilizar los GitHub scripts, consultethe section called “Secuencias de comandos Python de Amazon Detective”.

Habilitación de una cuenta de miembro con el estado No habilitado

Cuando una cuenta de miembro acepta una invitación, Amazon Detective comprueba el número de cuentas de miembros. El número máximo de cuentas de miembros que se admite en un gráfico de comportamiento es 1200. Si el gráfico de comportamiento ya contiene 1200 cuentas de miembros, no se pueden habilitar nuevas cuentas. Si Detective no puede habilitar la cuenta de miembro, establece el estado de la cuenta de miembro en No habilitado.

Las cuentas de miembros con el estado No habilitado no aportan datos al gráfico de comportamiento.

Detective habilita automáticamente las cuentas a medida que el gráfico de comportamiento puede aceptarlas.

También tiene la opción de habilitar manualmente las cuentas de miembros con el estado No habilitado. Por ejemplo, puede eliminar cuentas de miembros para reducir el volumen de datos. En lugar de esperar al proceso automático encargado de habilitar cuentas, puede intentar habilitar las cuentas de miembros con el estado No habilitado.

Console

La lista de cuentas de miembros incluye una opción para habilitar las cuentas de miembros con el estado No habilitado.

Habilitación de una cuenta de miembro con el estado No habilitado

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Administración de cuentas.
3. En Mis cuentas miembro, marque la casilla para cada cuenta de miembro que desee habilitar.

   Solo puede habilitar las cuentas de miembros cuyo estado es No habilitado.
4. Elija Habilitar cuentas.

Detective determina si la cuenta de miembro se puede habilitar. Si se puede habilitar, el estado cambia a Habilitado.

Detective API/CLI

Puede utilizar una API llamada o la AWS Command Line Interface para habilitar una cuenta de un solo miembro que no esté habilitada. Para obtener su gráfico ARN de comportamiento y usarlo en la solicitud, use la `ListGraphs`operación.

Habilitación de una cuenta de miembro con el estado No habilitado

- DetectiveAPI: Utilice la `StartMonitoringMember`APIoperación. Debe proporcionar el gráfico de comportamientoARN. Para identificar la cuenta del miembro, utilice el identificador de la AWS cuenta.
- AWS CLI: Ejecute el `start-monitoring-member`comando.

```
start-monitoring-member --graph-arn <behavior graph ARN> --account-id <AWS account
 ID>
```

Por ejemplo:

```
start-monitoring-member --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --account-id 444455556666
```

Eliminar las cuentas de los miembros de un gráfico de comportamiento

La cuenta de administrador puede eliminar las cuentas de los miembros invitados de un gráfico de comportamiento en cualquier momento.

Detective elimina automáticamente las cuentas de los miembros canceladas en AWS, excepto en las regiones AWS GovCloud (EE. UU. Este) y AWS GovCloud (EE. UU. Oeste).

Cuando se elimina una cuenta de miembro invitada de un gráfico de comportamiento, ocurre lo siguiente.

- La cuenta de miembro se elimina de Mis cuentas miembro.
- Amazon Detective deja de ingerir datos de la cuenta eliminada.

Detective no elimina ningún dato del gráfico de comportamiento, que se encarga de agregar datos de todas las cuentas de miembros.

Console

Puedes utilizarla AWS Management Console para eliminar las cuentas de miembros invitados de tu gráfico de comportamiento.

Eliminación de cuentas de miembros (consola)

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Administración de cuentas.
3. En la lista de cuentas, marque la casilla de cada cuenta de miembro que desee eliminar.

   No puede eliminar su propia cuenta de la lista.
4. Elija Actions. A continuación, elija Desactivar cuentas.

Detective API/CLI

Puedes usar el Detective API o el AWS Command Line Interface para eliminar las cuentas de los miembros invitados de tu gráfico de comportamiento. Para obtener tu gráfico ARN de comportamiento y usarlo en la solicitud, usa la `ListGraphs`operación.

Para eliminar las cuentas de los miembros invitados de tu gráfico de comportamiento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `DeleteMembers`operación. Especifique el gráfico ARN y la lista de identificadores de cuentas para las cuentas de los miembros que desee eliminar.
- AWS CLI: en la línea de comandos, ejecute el comando `delete-members`.

```
aws detective delete-members --account-ids <account ID list> --graph-arn <behavior
 graph ARN>
```

Ejemplo:

```
aws detective delete-members --account-ids 444455556666 123456789012 --graph-arn
 arn:aws:detective:us-east-1:111122223333:graph:123412341234
```

Python script

Detective proporciona un script de código abierto en GitHub. que le permite eliminar una lista especificada de cuentas de miembros de un gráfico de comportamiento de una cuenta de administrador en una lista especificada de regiones.

Para obtener información sobre cómo configurar y utilizar los GitHub scripts, consultethe section called “Secuencias de comandos Python de Amazon Detective”.

Para cuentas de miembros: administración de las invitaciones y suscripciones a gráficos de comportamiento

Amazon Detective cobra a todas las cuentas de miembros por los datos ingeridos en cada gráfico de comportamiento al que aportan datos.

Desde la página Administración de cuentas, las cuentas de miembros pueden ver las cuentas de administrador de cada gráfico de comportamiento del que son miembros.

Las cuentas de miembros invitadas a un gráfico de comportamiento pueden ver sus invitaciones y responder a estas. También pueden eliminar su cuenta de un gráfico de comportamiento.

En el caso del gráfico de comportamiento de la organización, las cuentas de la organización no pueden controlar si su cuenta es una cuenta de miembro. La cuenta de administrador de Detective elige cuentas de la organización para habilitarlas o deshabilitarlas como cuentas de miembros.

Contenido

- IAMPolítica obligatoria para una cuenta de miembro
- Visualización de la lista de invitaciones a gráficos de comportamiento
- Respuesta a una invitación de un gráfico de comportamiento
- Eliminación de la cuenta de un gráfico de comportamiento

IAMPolítica obligatoria para una cuenta de miembro

Para que la cuenta de un miembro pueda ver y administrar las invitaciones, debe adjuntar la IAM política requerida a su director. La entidad principal puede ser un usuario o rol existente, aunque también puede crear un nuevo usuario o rol para utilizar Detective.

Lo ideal es que el IAM administrador adjunte la política requerida a la cuenta de administrador.

La IAM política de cuentas de miembros otorga acceso a las acciones de las cuentas de miembros en Amazon Detective. La invitación por correo electrónico para contribuir a un gráfico de comportamiento incluye el texto de esa IAM política.

Para usar esta política, *<behavior graph ARN>* sustitúyala por el gráficoARN.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:DisassociateMembership",
        "detective:RejectInvitation"
      ],
      "Resource": "<behavior graph ARN>"
    },
   {
    "Effect":"Allow",
    "Action":[
        "detective:BatchGetMembershipDatasources",
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations"
    ],
    "Resource":"*"
   }
 ]
}
```

Tenga en cuenta que las cuentas de la organización del gráfico de comportamiento de la organización no reciben invitaciones y no pueden desasociar su cuenta de dicho gráfico de comportamiento. Si no pertenecen a otros gráficos de comportamiento, tan solo necesitan el permiso `ListInvitations`. `ListInvitations` permite a las cuentas de la organización ver la cuenta de administración del gráfico de comportamiento. Los permisos para administrar invitaciones y desasociar suscripciones solo se aplican a las suscripciones por invitación.

Visualización de la lista de invitaciones a gráficos de comportamiento

Desde la consola de Amazon DetectiveAPI, Detective o AWS Command Line Interface la cuenta de un miembro pueden ver sus invitaciones con gráficos de comportamiento.

Visualización de invitaciones a gráficos de comportamiento (consola)

Puede ver las invitaciones con gráficos de comportamiento desde AWS Management Console.

Visualización de invitaciones a gráficos de comportamiento (consola)

1. Inicie sesión en AWS Management Console. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Administración de cuentas.

En la página Administración de cuentas, la sección Mis cuentas de administrador recoge las invitaciones abiertas y aceptadas a gráficos de comportamiento de la región actual. Si, además, se trata de una cuenta de la organización, la sección Mis cuentas de administrador incluye el gráfico de comportamiento de la organización.

Si la cuenta se encuentra en el período de prueba gratuita, la página muestra el número de días restantes de la prueba gratuita.

La lista no contiene las invitaciones que ha rechazado, las suscripciones que ha ignorado o las suscripciones que ha eliminado el administrador de la cuenta.

Para cada invitación, se muestra el número de la cuenta de administrador, la fecha en la que se aceptó la invitación y su estado actual.

- El estado de las invitaciones a las que todavía no ha respondido es Invitado.
- El estado de las invitaciones que ha aceptado puede ser Habilitado o No habilitado.

  Si el estado es Habilitado, la cuenta aporta datos al gráfico de comportamiento.

  Si el estado es No habilitado, la cuenta no aporta datos al gráfico de comportamiento.

  El estado de su cuenta se establece inicialmente como No habilitada, mientras que el Detective comprueba si la ha GuardDuty activado y, de ser así, si su cuenta provocaría que el volumen de datos del gráfico de comportamiento superara la cuota de Detective.

Si la cuenta no provocaría que el gráfico de comportamiento superase la cuota, Detective actualiza el estado de la cuenta a Habilitado. De lo contrario, el estado sigue siendo No habilitado.

Siempre que el gráfico de comportamiento puede aceptar el volumen de datos de la cuenta, Detective actualiza automáticamente el estado a Habilitado. Es posible que la cuenta de administrador tenga que eliminar otras cuentas de miembros para habilitar su cuenta. Asimismo, la cuenta de administrador puede habilitar su cuenta manualmente.

Visualización de invitaciones con gráficos de comportamiento (DetectiveAPI, AWS CLI)

Puede enumerar las invitaciones del Detective API o del AWS Command Line Interface.

Para recuperar una lista de invitaciones abiertas y aceptadas a gráficos de comportamiento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `ListInvitations`operación.
- AWS CLI: en la línea de comandos, ejecute el comando `list-invitations`.

```
aws detective list-invitations
```

Respuesta a una invitación de un gráfico de comportamiento

Tras aceptar una invitación, el Detective comprueba el número de cuentas de los miembros. El número máximo de cuentas de miembros que se admite en un gráfico de comportamiento es 1200. Si el gráfico de comportamiento ya contiene 1200 cuentas de miembros, no se pueden habilitar nuevas cuentas.

Tras aceptar la invitación, Detective estará activado en tu cuenta. El Detective comprueba si su volumen de datos está dentro de la cuota de Detective. El volumen de datos aportados a un gráfico de comportamiento debe ser inferior al volumen máximo que permite Detective. Si el volumen ingerido actualmente supera el límite de 10 TB por día, no podrá añadir más cuentas y el Detective deshabilitará la ingesta adicional de datos. La consola de Detective muestra una notificación para indicar que el volumen de datos es demasiado grande y el estado sigue siendo No activado.

Si rechaza la invitación, esta se elimina de su lista de invitaciones y Detective no utiliza los datos de la cuenta en el gráfico de comportamiento.

Respuesta a una invitación de un gráfico de comportamiento (consola)

Puede utilizarla AWS Management Console para responder a la invitación por correo electrónico, que incluye un enlace a la consola de Detective. Solo puede responder a una invitación si su estado es Invitado.

Respuesta a una invitación de un gráfico de comportamiento (consola)

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Administración de cuentas.
3. En Mis cuentas de administrador, elija Aceptar invitación para aceptar la invitación y comenzar a aportar datos al gráfico de comportamiento.

   Para rechazar la invitación y eliminarla de la lista, elija Rechazar.

Responder a una invitación con un gráfico de comportamiento (DetectiveAPI, AWS CLI)

Puede responder a las invitaciones del Detective API o del AWS Command Line Interface.

Para aceptar una invitación con un gráfico de comportamiento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `AcceptInvitation`operación. Debe especificar el gráficoARN.
- AWS CLI: en la línea de comandos, ejecute el comando `accept-invitation`.

```
aws detective accept-invitation --graph-arn <behavior graph ARN>
```

Ejemplo:

```
aws detective accept-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Rechazar una invitación con un gráfico de comportamiento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `RejectInvitation`operación. Debe especificar el gráficoARN.
- AWS CLI: en la línea de comandos, ejecute el comando `reject-invitation`.

```
aws detective reject-invitation --graph-arn <behavior graph ARN>
```

Ejemplo:

```
aws detective reject-invitation --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Eliminación de la cuenta de un gráfico de comportamiento

Después de aceptar una invitación, puede eliminar su cuenta de un gráfico de comportamiento en cualquier momento. Cuando elimina su cuenta de un gráfico de comportamiento, Amazon Detective deja de ingerir datos de su cuenta para el gráfico de comportamiento. Los datos que ya haya aportado permanecerán en el gráfico de comportamiento.

Solo las cuentas invitadas pueden eliminar su cuenta de un gráfico de comportamiento. Las cuentas de la organización no pueden eliminar su cuenta del gráfico de comportamiento de la organización.

Eliminación de la cuenta de un gráfico de comportamiento (consola)

Puede utilizarla AWS Management Console para eliminar su cuenta de un gráfico de comportamiento.

Eliminación de la cuenta de un gráfico de comportamiento (consola)

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, elija Administración de cuentas.
3. En Mis cuentas de administrador, elija Renunciar para el gráfico de comportamiento del que quiera eliminar su cuenta.

Eliminar tu cuenta de un gráfico de comportamiento (DetectiveAPI, AWS CLI)

Puedes usar el Detective API o el AWS Command Line Interface para eliminar tu cuenta de un gráfico de comportamiento.

Para eliminar tu cuenta de un gráfico de comportamiento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `DisassociateMembership`operación. Debe especificar el gráficoARN.

- AWS CLI: en la línea de comandos, ejecute el comando `disassociate-membership`.

```
aws detective disassociate-membership --graph-arn <behavior graph ARN>
```

Ejemplo:

```
aws detective disassociate-membership --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Efecto de las acciones de la cuenta sobre los gráficos de comportamiento

Estas acciones producen los siguientes efectos en los datos de Amazon Detective y en el acceso al servicio.

Deshabilitación de Detective

Cuando una cuenta de administrador deshabilita Detective, ocurre lo siguiente:

- Se elimina el gráfico de comportamiento.
- Detective deja de ingerir datos de la cuenta de administrador y de las cuentas de miembros de ese gráfico de comportamiento.

Eliminación de una cuenta de miembro del gráfico de comportamiento

Cuando se elimina una cuenta de miembro de un gráfico de comportamiento, Detective deja de ingerir datos de esa cuenta.

Los datos existentes en el gráfico de comportamiento no se ven afectados.

Si se trata de una cuenta invitada, la cuenta se elimina de la lista Mis cuentas miembro.

En el caso de las cuentas de una organización en el gráfico de comportamiento de esta, el estado de la cuenta cambia a No es miembro.

Abandono de la organización por parte de una cuenta de miembro

Cuando una cuenta de miembro abandona una organización, ocurre lo siguiente:

- Se elimina la cuenta de la lista Mis cuentas miembro del gráfico de comportamiento de la organización.
- Detective deja de ingerir datos de esa cuenta.

Los datos existentes en el gráfico de comportamiento no se ven afectados.

AWS cuenta suspendida

Cuando se suspende una cuenta de administrador AWS, la cuenta pierde el permiso para ver el gráfico de comportamiento en Detective. Detective deja de introducir datos en el gráfico de comportamiento.

Cuando se suspende la cuenta de un miembro AWS, el Detective deja de ingerir los datos de esa cuenta.

Transcurridos 90 días, la cuenta se termina o se reactiva. Cuando se reactiva una cuenta de administrador, se restauran los permisos de Detective de la cuenta. Detective reanuda la ingesta de datos de la cuenta. Cuando se reactiva una cuenta de miembro, Detective reanuda la ingesta de datos de la cuenta.

AWS cuenta cerrada

Cuando se cierra una AWS cuenta, el Detective responde al cierre de la siguiente manera.

- Si se trata de una cuenta de administrador, Detective elimina el gráfico de comportamiento.
- Si se trata de una cuenta de miembro, Detective elimina la cuenta del gráfico de comportamiento.

AWS conserva los datos de la política de la cuenta durante 90 días a partir de la fecha de entrada en vigor del cierre de la cuenta del administrador. Al final del período de 90 días, elimina AWS permanentemente todos los datos de la política de la cuenta.

- Si desea conservar los resultados por más de 90 días, puede archivar las políticas. También puedes usar una acción personalizada con una EventBridge regla para almacenar los resultados en un bucket de S3.
- Mientras se AWS conserven los datos de la política, al volver a abrir la cuenta cerrada, se la AWS reasignará como administradora del servicio y se recuperarán los datos de la política de servicio de la cuenta.
- Para obtener más información, consulte Cierre de una cuenta.

> **Important**
>
> Para los clientes de las regiones: AWS GovCloud (US)
>
> - Antes de cerrar la cuenta, realice una copia de seguridad y, luego, elimine los recursos de la cuenta. Ya no tendrá acceso a ellos después de cerrar la cuenta.

Uso de scripts de Detective Python para administrar cuentas

Amazon Detective proporciona un conjunto de scripts de Python de código abierto en el GitHub repositorio amazon-detective-multiaccount-scripts. Los scripts requieren Python 3.

Puede utilizar estos scripts para llevar a cabo las siguientes tareas:

- Habilitar Detective para una cuenta de administrador en varias regiones.

  Al habilitar Detective, puede asignar valores de etiqueta al gráfico de comportamiento.
- Agregar cuentas de miembros a gráficos de comportamiento de la cuenta de administrador en varias regiones.
- Enviar correos electrónicos de invitación a cuentas de miembros. También puede configurar la solicitud para que no envíe correos electrónicos de invitación.
- Eliminar cuentas de miembros de gráficos de comportamiento de la cuenta de administrador en varias regiones.
- Deshabilitar Detective para una cuenta de administrador en varias regiones. Cuando una cuenta de administrador deshabilita Detective, el gráfico de comportamiento de la cuenta de administrador se deshabilita en todas las regiones.

Descripción general del script `enableDetective.py`

El script `enableDetective.py` hace lo siguiente:

1. Habilita Detective para una cuenta de administrador en cada región especificada, siempre que la cuenta de administrador no tuviera habilitado Detective en una región.

   Al utilizar el script para habilitar Detective, puede asignar valores de etiqueta al gráfico de comportamiento.

2. También puede enviar invitaciones desde la cuenta de administrador a las cuentas de miembros especificadas para cada gráfico de comportamiento.

   Los mensajes de correo electrónico de invitación utilizan el formato de contenido predeterminado para mensajes, que no se puede personalizar.

   También puede configurar la solicitud para que no envíe correos electrónicos de invitación.
3. Acepta automáticamente las invitaciones enviadas a cuentas de miembros.

   Como el script acepta automáticamente las invitaciones, las cuentas de miembros pueden ignorar los mensajes.

   Se recomienda comunicar directamente a las cuentas de miembros que las invitaciones se aceptan automáticamente.

Descripción general del script **`disableDetective.py`**

El script `disableDetective.py` elimina las cuentas de miembros especificadas de los gráficos de comportamiento de la cuenta de administrador en las regiones especificadas.

También permite deshabilitar Detective para la cuenta de administrador en las regiones especificadas.

Permisos necesarios para los scripts

Los scripts requieren un AWS rol preexistente en la cuenta de administrador y en todas las cuentas de los miembros que añada o elimine.

> **Note**
>
> El nombre del rol debe ser el mismo en todas las cuentas.

IAMLas mejores prácticas recomendadas por la política son utilizar los roles con el mínimo alcance. Para ejecutar el flujo de trabajo del script —crear un gráfico, crear miembros y agregar miembros al gráfico , los permisos necesarios son los siguientes:

- detective: CreateGraph
- detective: CreateMembers

- detective: DeleteGraph
- detective: DeleteMembers
- detective: ListGraphs
- detective: ListMembers
- detective: AcceptInvitation

Relación de confianza del rol

La relación de confianza del rol debe permitir que la instancia o las credenciales locales asuman el rol.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::<ACCOUNTID>:user/<USERNAME>"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Si no dispone de un rol común que incluya el permiso necesario, deberá crear un rol que incluya, como mínimo, los permisos necesarios en cada cuenta de miembro. También debe crear este rol en la cuenta de administrador.

Al crear el rol, asegúrese de hacer lo siguiente:

- Utilice el mismo nombre de rol en cada cuenta.
- Añada los permisos necesarios arriba (recomendado) o seleccione la política AmazonDetectiveFullAccessgestionada.
- Agregue el bloque de relaciones de confianza del rol, tal como se indica más arriba.

Para automatizar este proceso, puede utilizar la `EnableDetective.yaml` AWS CloudFormation plantilla. Como la plantilla solo crear recursos globales, se puede ejecutar en cualquier región.

Configuración del entorno de ejecución para scripts de Python

Puede ejecutar los scripts desde una EC2 instancia o desde una máquina local.

Lanzar y configurar una EC2 instancia

Una opción para ejecutar los scripts es ejecutarlos desde una EC2 instancia.

Para lanzar y configurar una EC2 instancia

1. Lanza una EC2 instancia en tu cuenta de administrador. Para obtener más información sobre cómo lanzar una EC2 instancia, consulte Introducción a las instancias de Amazon EC2 Linux en la Guía del EC2 usuario de Amazon.
2. Adjunta a la instancia un IAM rol que tenga permisos que permitan a la instancia llamar desde `AssumeRole` la cuenta de administrador.

   Si usaste la `EnableDetective.yaml` AWS CloudFormation plantilla, se `EnableDetective` creó un rol de instancia con un perfil denominado.

   De lo contrario, para obtener información sobre la creación de un rol de instancia, consulta la entrada del blog Cómo reemplazar o adjuntar fácilmente un IAM rol a una EC2 instancia existente mediante la EC2 consola.
3. Instale el software necesario:
   - APT: `sudo apt-get -y install python3-pip python3 git`
   - RPM: `sudo yum -y install python3-pip python3 git`
   - Boto (versión mínima: 1.15): `sudo pip install boto3`
4. Clona el repositorio en la EC2 instancia.

   ```
   git clone https://github.com/aws-samples/amazon-detective-multiaccount-scripts.git
   ```

Configuración de una máquina local para ejecutar los scripts

También puede ejecutar los scripts desde una máquina local.

Configuración de una máquina local para ejecutar los scripts

1. Compruebe que haya configurado en la máquina local las credenciales de la cuenta de administrador que tiene permiso para llamar a `AssumeRole`.
2. Instale el software necesario:
   - Python 3
   - Boto (versión mínima: 1.15)
   - GitHub scripts

Plataforma	Instrucciones de configuración
Windows	1. Instale Python 3 (https://www.python.org/downloads/windows/). 2. Abra un símbolo del sistema. 3. Ejecute `pip install boto3` para instalar Boto. 4. Descargue el código fuente del script desde (). GitHub https://github.com/aws-samples/amazon-detective-multiaccount-scripts
Mac	1. Instale Python 3 (https://www.python.org/downloads/mac-osx/). 2. Abra un símbolo del sistema. 3. Ejecute `pip install boto3` para instalar Boto. 4. Descargue el código fuente del script desde () GitHub . https://github.com/aws-samples/amazon-detective-multiaccount-scripts
Linux	1. Para instalar Python 3, ejecute uno de los siguientes comandos: • `sudo apt-get -y install install python3-pip python3 git` • `sudo yum install git python` 2. Ejecute `sudo pip install boto3` para instalar Boto.

Plataforma	Instrucciones de configuración
	3. Clona el código fuente del script desde https://github.com/aws-samples/amazon-detective-multiaccount-scripts.

Creación de una lista en formato `.csv` con las cuentas de miembros para agregar o eliminar

Para identificar las cuentas de miembros que quiera agregar a gráficos de comportamiento o eliminar de estos, es necesario proporcionar un archivo `.csv` que contenga una lista con las cuentas.

Se agrega una cuenta por línea. Cada entrada de la cuenta de un miembro contiene el ID de la AWS cuenta y la dirección de correo electrónico del usuario raíz de la cuenta.

Vea el siguiente ejemplo:

```
111122223333,srodriguez@example.com
444455556666,rroe@example.com
```

Ejecución de **`enableDetective.py`**

Puede ejecutar el `enableDetective.py` script desde una EC2 instancia o desde su máquina local.

Para ejecutar **`enableDetective.py`**

1. Copia el `.csv` archivo en el `amazon-detective-multiaccount-scripts` directorio de tu EC2 instancia o máquina local.
2. Cambie al directorio de `amazon-detective-multiaccount-scripts`.
3. Ejecute el script `enableDetective.py`.

   ```
   enableDetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --tags tagValueList --enabled_regions regionList  --
   disable_email
   ```

Al ejecutar el script, sustituya los siguientes valores:

administratorAccountID

El ID de AWS cuenta de la cuenta de administrador.

roleName

El nombre del AWS rol que se va a asumir en la cuenta de administrador y en la cuenta de cada miembro.

inputFileName

El nombre del archivo `.csv` que contiene la lista con las cuentas de miembros que se van a agregar a los gráficos de comportamiento de la cuenta de administrador.

tagValueList

(Opcional) Una lista de valores de etiqueta separados por comas que se asignan a un nuevo gráfico de comportamiento.

El formato de los valores de etiqueta es *key*=*value*. Por ejemplo:

```
--tags Department=Finance,Geo=Americas
```

regionList

(Opcional) Una lista de valores separados por comas con las regiones en las que se agregarán cuentas de miembros al gráfico de comportamiento de la cuenta de administrador. Por ejemplo:

```
--enabled_regions us-east-1,us-east-2,us-west-2
```

Es posible que la cuenta de administrador no haya habilitado Detective en una región. En ese caso, el script habilita Detective y crea un nuevo gráfico de comportamiento para la cuenta de administrador.

Si no proporciona una lista de regiones, el script funciona en todas las regiones compatibles con Detective.

`--disable_email`

(Opcional) Si se incluye, Detective no envía correos electrónicos de invitación a cuentas de miembros.

Ejecución de **`disableDetective.py`**

Puede ejecutar el `disableDetective.py` script desde una EC2 instancia o desde su máquina local.

Para ejecutar **`disableDetective.py`**

1. Copie el archivo `.csv` en el directorio `amazon-detective-multiaccount-scripts`.
2. Si desea utilizar el archivo `.csv` para eliminar las cuentas de miembros indicadas en una lista especificada de regiones de los gráficos de comportamiento de la cuenta de administrador, ejecute el script `disableDetective.py` de la siguiente forma:

   ```
   disabledetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --disabled_regions regionList
   ```

3. Para deshabilitar Detective en la cuenta de administrador para todas las regiones, ejecute el script `disableDetective.py` con la marca `--delete-master`.

   ```
   disabledetective.py --master_account administratorAccountID --assume_role roleName
    --input_file inputFileName --disabled_regions regionList --delete_master
   ```

Al ejecutar el script, sustituya los siguientes valores:

`administratorAccountID`

El ID de AWS cuenta de la cuenta de administrador.

`roleName`

El nombre del AWS rol que se va a asumir en la cuenta de administrador y en la cuenta de cada miembro.

`inputFileName`

El nombre del archivo `.csv` que contiene la lista con las cuentas de miembros que se van a eliminar de los gráficos de comportamiento de la cuenta de administrador.

Debe proporcionar un archivo `.csv` aunque vaya a deshabilitar Detective.

regionList

(Opcional) Una lista de regiones separadas por comas en la que se puede realizar una de las siguientes acciones:

- Eliminar cuentas de miembros de gráficos de comportamiento de la cuenta de administrador
- Si la marca `--delete-master` está incluida, deshabilitar Detective

Por ejemplo:

```
--disabled_regions us-east-1,us-east-2,us-west-2
```

Si no proporciona una lista de regiones, el script funciona en todas las regiones compatibles con Detective.

Integración de Amazon Detective con Amazon Security Lake

Amazon Security Lake es un servicio de lago de datos de seguridad totalmente gestionado. Puede usar Security Lake para centralizar automáticamente los datos de seguridad de los AWS entornos, los proveedores de SaaS, las fuentes locales, las fuentes en la nube y las fuentes de terceros en un lago de datos diseñado específicamente que se almacena en su cuenta. AWS Security Lake le ayuda a analizar los datos de seguridad para que pueda comprender mejor su postura de seguridad en toda la organización. Con Security Lake, también puede mejorar la protección de sus cargas de trabajo, aplicaciones y datos.

Amazon Detective se integra con Amazon Security Lake, lo que permite consultar y recuperar datos de registros sin procesar almacenados por Security Lake.

Con esta integración puede recopilar registros y eventos de los siguientes orígenes que Security Lake admite de forma nativa. Detective admite hasta la versión 2 de origen (OCSF 1.1.0).

- AWS CloudTrail eventos de gestión, versión 1.0 y posteriores
- Registros de flujo de Amazon Virtual Private Cloud (Amazon VPC) versión 1.0 y versiones posteriores
- Registro de auditoría de Amazon Elastic Kubernetes Service (Amazon EKS) versión 2.0.
  — Para utilizar los registros de auditoría de Amazon EKS como fuente, debe añadirlos `ram:ListResources` a los permisos de IAM. Para obtener más información, consulte Añadir los permisos de IAM necesarios a su cuenta.

Para obtener más información sobre cómo Security Lake convierte automáticamente los registros y eventos que provienen de AWS servicios compatibles de forma nativa en el esquema OCSF, consulte la Guía del usuario de Amazon Security Lake.

Tras integrar Detective con Security Lake, Detective comienza a extraer registros sin procesar de Security Lake relacionados con los eventos de AWS CloudTrail administración y los registros de flujo de Amazon VPC. Para obtener más información, consulte Consultar registros sin procesar.

Habilitación de la integración de Detective con Security Lake

Para integrar Detective con Security Lake, debe completar los siguientes pasos.

1. Antes de empezar

Utilice una cuenta de administración de Organizations para designar un administrador delegado de Security Lake para su organización. Asegúrese de que Security Lake esté activado y compruebe que Security Lake recopila registros y eventos de los eventos de AWS CloudTrail administración y de los registros de flujo de Amazon Virtual Private Cloud (Amazon VPC).

De acuerdo con la arquitectura de referencia de seguridad, el Detective recomienda usar una cuenta de Log Archive y aplazar el uso de una cuenta de herramientas de seguridad para la implementación de Security Lake.

2. Crear un suscriptor de Security Lake

   Para consumir registros y eventos de Amazon Security Lake, usted debe ser suscriptor de Security Lake. Siga estos pasos para conceder acceso de consulta a un administrador de cuentas de Detective.

3. Añadir los permisos AWS Identity and Access Management (IAM) necesarios a su identidad de IAM.
   - Añada estos permisos para crear la integración de Detective con Security Lake:
     - Adjunte estos permisos de AWS Identity and Access Management (IAM) a su identidad de IAM. Para obtener más información, consulta la sección Añadir los permisos de IAM necesarios a tu cuenta.
     - Añada esta política de IAM al principal de IAM que piensa utilizar para transferir la AWS CloudFormation función de servicio. Para obtener más información, consulte la sección Añadir permisos a su cuenta principal de IAM.
   - Si ya ha integrado Detective con Security Lake, para utilizar la integración, adjunte estos permisos (IAM) a su identidad de IAM. Para obtener más información, consulte la sección Añadir los permisos de IAM necesarios a su cuenta.
4. Aceptar la invitación del ARN de Resource Share y habilitar la integración

Utilice la AWS CloudFormation plantilla para configurar los parámetros necesarios para crear y administrar el acceso a las consultas para los suscriptores de Security Lake. Para ver los pasos detallados para crear una pila, consulte Crear una pila con la AWS CloudFormation plantilla. Cuando termine de crear la pila, habilite la integración.

Para ver una demostración de cómo integrar Amazon Detective con Amazon Security Lake mediante la consola Detective, vea el siguiente vídeo: Integración de Amazon Detective con Amazon Security Lake: Cómo configurar -->

Antes de empezar a integrar Detective con Security Lake

En este tema se describen los pasos preliminares, como delegar un administrador de Security Lake para su organización, habilitar Security Lake para su cuenta de administrador de Detective y verificar que Security Lake recopila registros y eventos.

Security Lake se integra AWS Organizations para administrar la recopilación de registros en varias cuentas de una organización. Para usar Security Lake para una organización, su cuenta AWS Organizations de administración debe designar primero a un administrador delegado de Security Lake para su organización. A continuación, el administrador delegado de Security Lake debe habilitar Security Lake y habilitar la recopilación de registros y eventos para cuentas de miembros de la organización.

Antes de integrar Security Lake con Detective, asegúrese de que Security Lake esté activado para la cuenta de administrador de Detective. Primero debe configurar los ajustes de su lago de datos y configurar la recopilación de registros habilitando Security Lake mediante la consola de Security Lake. Para ver los pasos detallados sobre cómo habilitar Security Lake, consulte Introducción en la Guía del usuario de Amazon Security Lake.

Compruebe también que Security Lake esté recopilando registros y eventos de los eventos de AWS CloudTrail administración y de los registros de flujo de Amazon Virtual Private Cloud (Amazon VPC). Para obtener más información sobre la recopilación de registros en Security Lake, consulte Recopilación de datos de AWS los servicios en la Guía del usuario de Amazon Security Lake.

Paso 1: Crear un suscriptor de Security Lake en Detective

En este tema se explica cómo usar la consola de Detective para crear un suscriptor de Security Lake.

Para consumir registros y eventos de Amazon Security Lake, usted debe ser suscriptor de Security Lake. Los suscriptores pueden consultar y acceder a los datos que recopila Security Lake. Un suscriptor con acceso a consultas puede consultar AWS Lake Formation tablas directamente en un bucket de Amazon Simple Storage Service (Amazon S3) mediante servicios como Amazon Athena. Para convertirse en suscriptor, el administrador de Security Lake debe proporcionarle acceso de suscriptor que le permita realizar consultas en el lago de datos. Para obtener información sobre cómo lo hace el administrador, consulte Crear un suscriptor con acceso de consulta en la Guía del usuario de Amazon Security Lake.

Siga estos pasos para crear un suscriptor de Security Lake y conceder acceso de consulta a una cuenta de administrador de Detective.

Para crear un suscriptor de Detective en Security Lake

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Integraciones.
3. En el panel de suscriptores de Security Lake, anote los valores de ID de cuenta e ID externo.

   Pídale al administrador de Security Lake que las use IDs para:

   - Para crear un suscriptor de Detective en Security Lake.
   - Para configurar el suscriptor para que tenga acceso de consulta.
   - Para asegurarse de que se crea el suscriptor de consulta de Security Lake con permisos de Lake Formation, seleccione Lake Formation como Método de acceso a los datos en la consola de Security Lake.

   Cuando el administrador de Security Lake crea un suscriptor para usted, Security Lake genera un ARN del recurso compartido de Amazon para usted. Pida al administrador que le envíe este ARN.
4. Introduzca el ARN del recurso compartido proporcionado por el administrador de Security Lake en el panel Suscriptor de Security Lake.
5. Tras recibir el ARN del recurso compartido del administrador de Security Lake, introdúzcalo en el cuadro ARN del recurso compartido del panel Suscriptor de Security Lake.

Paso 2: Añadir los permisos de IAM necesarios a su cuenta en Detective

En este tema se explican los detalles de la política de permisos AWS Identity and Access Management (de IAM) que debe añadir a su identidad de IAM.

Para habilitar la integración de Detective con Security Lake, debe adjuntar la siguiente política de permisos AWS Identity and Access Management (IAM) a su identidad de IAM.

Asocie las siguientes políticas insertadas al rol. Sustituya `athena-results-bucket` por el nombre de su bucket de Amazon S3 si quiere utilizar su propio bucket de Amazon S3 para almacenar los resultados de consultas de Athena. Si desea que Detective genere automáticamente un

bucket de Amazon S3 para almacenar el resultado de la consulta de Athena, elimine todos los `S3ObjectPermissions` de la política de IAM.

Si no dispone de los permisos necesarios para adjuntar esta política a su identidad de IAM, póngase en contacto con su administrador. AWS Si tiene los permisos necesarios pero se produce un problema, consulte Solucionar problemas con los mensajes de error de acceso denegado en la Guía del usuario de IAM.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets"
      ],
      "Resource": "*"
    },
    {
      "Sid": "S3ObjectPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetObject",
        "s3:PutObject"
      ],
      "Resource": [
        "arn:aws:s3:::<athena-results-bucket>",
        "arn:aws:s3:::<athena-results-bucket>/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "glue:GetDatabases",
        "glue:GetPartitions",
        "glue:GetTable",
        "glue:GetTables"
      ],
      "Resource": [
        "arn:aws:glue:*:<ACCOUNT ID>:database/amazon_security_lake*",
        "arn:aws:glue:*:<ACCOUNT ID>:table/amazon_security_lake*/
amazon_security_lake*",
```

```
        "arn:aws:glue:*:<ACCOUNT ID>:catalog"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "athena:BatchGetQueryExecution",
        "athena:GetQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryRuntimeStatistics",
        "athena:GetWorkGroup",
        "athena:ListQueryExecutions",
        "athena:StartQueryExecution",
        "athena:StopQueryExecution",
        "lakeformation:GetDataAccess",
        "ram:ListResources"
      ],
      "Resource": "*"
    },
    {
       "Effect": "Allow",
        "Action": [
          "ssm:GetParametersByPath"
        ],
        "Resource": [
          "arn:aws:ssm:*:<ACCOUNT ID>:parameter/Detective/SLI"
        ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:GetTemplateSummary",
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
```

```
          "organizations:ServicePrincipal": [
            "securitylake.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Paso 3: Aceptar la invitación del ARN de Resource Share

En este tema se explican los pasos para aceptar la invitación del ARN de Resource Share mediante una AWS CloudFormation plantilla, que es un paso obligatorio antes de habilitar la integración de Detective con Security Lake.

Para acceder a registros de datos sin procesar de Security Lake debe aceptar una invitación del recurso compartido de la cuenta de Security Lake que creó el administrador de Security Lake. También necesita permisos de AWS Lake Formation para configurar uso compartido de tablas entre cuentas. Además, debe crear un bucket de Amazon Simple Storage Service (Amazon S3) que pueda recibir registros de consultas sin procesar.

En el siguiente paso, utilizarás una AWS CloudFormation plantilla para crear una pila para: aceptar la invitación del ARN de Resource Share, crear Rastreador de AWS Glue los recursos necesarios y conceder permisos de AWS Lake Formation administrador.

Para aceptar la invitación del ARN de Resource Share y habilitar la integración

1. Cree una CloudFormation pila nueva con la CloudFormation plantilla. Para obtener más información, consulta Crear una pila con la plantilla de AWS CloudFormation.
2. Cuando termine de crear la pila, seleccione Activar la integración para activar la integración de Detective con Security Lake.

Crear una pila con la plantilla de AWS CloudFormation

Detective proporciona una AWS CloudFormation plantilla que puede utilizar para configurar los parámetros necesarios para crear y administrar el acceso a las consultas para los suscriptores de Security Lake.

Paso 1: Crear un rol AWS CloudFormation de servicio

Debe crear un rol AWS CloudFormation de servicio para crear una pila con la AWS CloudFormation plantilla. Si no tiene los permisos necesarios para crear un rol de servicio, póngase en contacto con el administrador de la cuenta de administrador de Detective. Para obtener más información sobre el rol de servicio de AWS CloudFormation , consulte Rol de servicio de AWS CloudFormation.

1. Inicie sesión en la consola de IAM AWS Management Console y ábrala en https://console.aws.amazon.com/iam/.
2. En el panel de navegación de la consola de IAM, seleccione Roles y, a continuación, elija Crear rol.
3. En Select trusted entity (Seleccionar entidad de confianza), elija AWS service (Servicio de).
4. Elija AWS CloudFormation. A continuación, elija Siguiente.
5. Escriba un nombre para el rol. Por ejemplo, `CFN-DetectiveSecurityLakeIntegration`.
6. Asocie las siguientes políticas insertadas al rol. `<Account ID>`Sustitúyalo por tu ID AWS de cuenta.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "CloudFormationPermission",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateChangeSet"
            ],
            "Resource": [
                "arn:aws:cloudformation:*:aws:transform/*"
            ]
        },
        {
            "Sid": "IamPermissions",
            "Effect": "Allow",
            "Action": [
                "iam:CreateRole",
                "iam:DeleteRole",
                "iam:AttachRolePolicy",
                "iam:DetachRolePolicy",
                "iam:UpdateAssumeRolePolicy",
```

```
                "iam:PutRolePolicy",
                "iam:DeleteRolePolicy",
                "iam:CreatePolicy",
                "iam:DeletePolicy",
                "iam:PassRole",
                "iam:GetRole",
                "iam:GetRolePolicy"
            ],
            "Resource": [
                "arn:aws:iam::<ACCOUNT ID>:role/*",
                "arn:aws:iam::<ACCOUNT ID>:policy/*"
            ]
        },
        {
            "Sid": "S3Permissions",
            "Effect": "Allow",
            "Action": [
                "s3:CreateBucket",
                "s3:DeleteBucket*",
                "s3:PutBucket*",
                "s3:GetBucket*",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:GetEncryptionConfiguration"
            ],
            "Resource": [
                "arn:aws:s3:::*"
            ]
        },
        {
            "Sid": "LambdaPermissions",
            "Effect": "Allow",
            "Action": [
                "lambda:CreateFunction",
                "lambda:DeleteFunction",
                "lambda:GetFunction",
                "lambda:TagResource",
                "lambda:InvokeFunction"
            ],
            "Resource": [
                "arn:aws:lambda:*:<ACCOUNT ID>:function:*"
            ]
        },
        {
```

```
            "Sid": "CloudwatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:CreateLogGroup",
                "logs:DeleteLogGroup",
                "logs:DescribeLogGroups"
            ],
            "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
        },
        {
            "Sid": "KmsPermission",
            "Effect": "Allow",
            "Action": [
                "kms:Decrypt"
            ],
            "Resource": "arn:aws:kms:*:<ACCOUNT ID>:key/*"
        }
    ]
}
```

Paso 2: Añadir permisos a su cuenta principal de IAM.

Necesitará los siguientes permisos para crear una pila con el rol de CloudFormation servicio que creó en el paso anterior. Añada la siguiente política de IAM a la entidad principal de IAM que piensa utilizar para transferir la función de CloudFormation servicio. Asumirá esta entidad principal de IAM para crear la pila. Si no tiene los permisos necesarios para agregar la política de IAM, póngase en contacto con el administrador de la cuenta de administrador de Detective.

> **Note**
>
> En la siguiente política, la `CFN-DetectiveSecurityLakeIntegration` utilizada en esta política hace referencia al rol que creó en el paso de rol de servicio de `Creating an AWS CloudFormation` anterior. Cámbielo por el nombre del rol que introdujo en el paso anterior si es diferente.

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

```
             "Sid": "PassRole",
             "Effect": "Allow",
             "Action":
             [
                "iam:GetRole",
                "iam:PassRole"
             ],
             "Resource": "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
        },
        {
            "Sid": "RestrictCloudFormationAccess",
            "Effect": "Allow",
            "Action": [
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:UpdateStack"
            ],
            "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*",
            "Condition": {
                "StringEquals": {
                    "cloudformation:RoleArn": [
                        "arn:aws:iam::<ACCOUNT ID>:role/CFN-
DetectiveSecurityLakeIntegration"
                    ]
                }
            }
        },
        {
            "Sid": "CloudformationDescribeStack",
            "Effect": "Allow",
            "Action": [
                "cloudformation:DescribeStacks",
                "cloudformation:DescribeStackEvents",
                "cloudformation:GetStackPolicy"
            ],
            "Resource": "arn:aws:cloudformation:*:<ACCOUNT ID>:stack/*"
        },
        {
            "Sid": "CloudformationListStacks",
            "Effect": "Allow",
            "Action": [
                "cloudformation:ListStacks"
            ],
```

```
            "Resource": "*"
        },
        {
            "Sid": "CloudWatchPermissions",
            "Effect": "Allow",
            "Action": [
                "logs:GetLogEvents"
            ],
            "Resource": "arn:aws:logs:*:<ACCOUNT ID>:log-group:*"
        }
    ]
}
```

Paso 3: Especificar valores personalizados en la consola AWS CloudFormation

1. Ve a la AWS CloudFormation consola de Detective.
2. (Opcional) Introduzca un Nombre de pila. El nombre de pila se rellena automáticamente. Puede cambiar el nombre de pila por uno que no entre en conflicto con los nombres de pila existentes.
3. Introduzca los siguientes Parámetros.

   - AthenaResultsBucket— Si no introduce valores, esta plantilla genera un bucket de Amazon S3. Si desea utilizar su propio bucket, introduzca un nombre de bucket para almacenar los resultados de consultas de Athena. Si utiliza su propio bucket, asegúrese de que el bucket esté en la misma región que el ARN de Resource Share. Si utiliza su propio bucket, asegúrese de que los `LakeFormationPrincipals` que elige tienen permisos para escribir y leer objetos desde el bucket. Para obtener más información sobre los permisos de bucket, consulte Resultados de la consulta y consultas recientes en la Guía del usuario de Amazon Athena.
   - DTRegion— Este campo viene rellenado previamente. No cambie los valores de este campo.
   - LakeFormationPrincipals— Introduzca el ARN de los directores de IAM (por ejemplo, el ARN del rol de IAM) a los que quiere conceder acceso para utilizar la integración de Security Lake, separados por comas. Estos podrían ser sus analistas de seguridad e ingenieros de seguridad que utilizan Detective.

     Solo puede utilizar las entidades principales de IAM a las que anteriormente asoció permisos de IAM en el paso [`Step 2: Add the required IAM permissions to your account`].
   - ResourceShareARN: este campo viene rellenado previamente. No cambie los valores de este campo.

4. Permisos

   Rol de IAM: seleccione el rol que creó en el paso `Creating an AWS CloudFormation Service Role`. Si lo desea, puede dejarlo en blanco si su rol de IAM actual tiene todos los permisos necesarios en el paso `Creating an AWS CloudFormation Service Role`.

5. Revise y marque todas las casillas Acepto y, a continuación, haga clic en el botón Crear pila. Para obtener más información, consulte los siguientes recursos de IAM que se crearán.

```
* ResourceShareAcceptorCustomResourceFunction
    - ResourceShareAcceptorLambdaRole
    - ResourceShareAcceptorLogsAccessPolicy
* SsmParametersCustomResourceFunction
    - SsmParametersLambdaRole
    - SsmParametersLogsAccessPolicy
* GlueDatabaseCustomResourceFunction
    - GlueDatabaseLambdaRole
    - GlueDatabaseLogsAccessPolicy
* GlueTablesCustomResourceFunction
    - GlueTablesLambdaRole
    - GlueTablesLogsAccessPolicy
```

Paso 4: Añadir la política de bucket de Amazon S3 a los principios de IAM en **`LakeFormationPrincipals`**

(Opcional) Si deja que esta plantilla genere un `AthenaResultsBucket` para usted, deberá adjuntar la siguiente política a las entidades principales de IAM en `LakeFormationPrincipals`.

```
{
  "Sid": "S3ObjectPermissions",
  "Effect": "Allow",
  "Action": [
    "s3:GetObject",
    "s3:PutObject"
  ],
  "Resource": [
    "arn:aws:s3:::<athena-results-bucket>",
    "arn:aws:s3:::<athena-results-bucket>/*"
  ]
}
```

`athena-results-bucket`Sustitúyala por el nombre`AthenaResultsBucket`. Se `AthenaResultsBucket` puede encontrar en la AWS CloudFormation consola:

1. Abre la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.
2. Haga clic en la pila.
3. Haga clic en la pestaña Recursos.
4. Busque el ID lógico `AthenaResultsBucket` y copie su ID físico.

Cambiar la configuración de integración de Detective

Si desea cambiar alguno de los parámetros que utilizó para integrar Detective con Security Lake, puede editarlo y, a continuación, volver a habilitar la integración. Puede editar la AWS CloudFormation plantilla para volver a habilitar esta integración en los siguientes escenarios:

- Para actualizar la suscripción de Security Lake, puede crear un nuevo suscriptor o el administrador de Security Lake puede actualizar el origen de datos de la suscripción existente.
- Para especificar un bucket de Amazon S3 diferente para almacenar los registros de consultas sin procesar.
- Para especificar diferentes entidades principales de Lake Formation.

Cuando vuelva a habilitar la integración de Detective con Security Lake, podrá editar el ARN del recurso compartido y ver los Permisos de IAM. Para editar los permisos de IAM puede ir a la consola de IAM desde Detective. También puede editar los valores que ingresó anteriormente en la AWS CloudFormation plantilla. Debe eliminar la CloudFormation pila existente y volver a crearla para volver a habilitar la integración.

Rehabilitación de la integración de Detective con Security Lake

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Integraciones.
3. Puede editar la integración siguiendo uno de estos pasos:
   - En el panel Security Lake, seleccione Editar.
   - En el panel Security Lake, seleccione Ver. En la página de vista, elija Editar.
4. Introduzca un nuevo ARN del recurso compartido para acceder a los orígenes de datos de una región.

5. Consulte los permisos de IAM actuales y vaya a la consola de IAM si desea editar los permisos de IAM.
6. Edite los valores de la CloudFormation plantilla.

   1. Elimine la pila existente antes de crear una nueva. Si no elimina la pila existente e intenta crear una nueva pila en la misma región, la solicitud producirá error. Para obtener más información, consulta Eliminar una CloudFormation pila.

   1. Crea una CloudFormation pila nueva. Para obtener más información, consulta Crear una pila con la plantilla de AWS CloudFormation.
7. Seleccione Habilitar integración.

AWS Regiones compatibles para la integración de Detective con Security Lake

Puede integrar Detective con Security Lake en las siguientes AWS regiones.

Nombre de la región	Región	Punto de conexión	Protocolo;
Este de EE. UU. (Ohio)	us-east-2	securitylake.us-east-2.amazonaws.com	HTTPS
Este de EE. UU. (Norte de Virginia)	us-east-1	securitylake.us-east-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Norte de California)	us-west-1	securitylake.us-west-1.amazonaws.com	HTTPS
Oeste de EE. UU. (Oregón)	us-west-2	securitylake.us-west-2.amazonaws.com	HTTPS
Asia-Pacífico (Bombay)	ap-south-1	securitylake.ap-south-1.amazonaws.com	HTTPS
Asia-Pacífico (Seúl)	ap-northeast-2	securitylake.ap-northeast-2.amazonaws.com	HTTPS

Nombre de la región	Región	Punto de conexión	Protocolo;
Asia-Pacífico (Singapur)	ap-southeast-1	securitylake.ap-southeast-1.amazonaws.com	HTTPS
Asia-Pacífico (Sídney)	ap-southeast-2	securitylake.ap-southeast-2.amazonaws.com	HTTPS
Asia-Pacífico (Tokio)	ap-northeast-1	securitylake.ap-northeast-1.amazonaws.com	HTTPS
Canadá (centro)	ca-central-1	securitylake.ca-central-1.amazonaws.com	HTTPS
Europa (Fráncfort)	eu-central-1	securitylake.eu-central-1.amazonaws.com	HTTPS
Europa (Irlanda)	eu-west-1	securitylake.eu-west-1.amazonaws.com	HTTPS
Europa (Londres)	eu-west-2	securitylake.eu-west-2.amazonaws.com	HTTPS
Europa (París)	eu-west-3	securitylake.eu-west-3.amazonaws.com	HTTPS
Europa (Estocolmo)	eu-north-1	securitylake.eu-north-1.amazonaws.com	HTTPS
América del Sur (São Paulo)	sa-east-1	securitylake.sa-east-1.amazonaws.com	HTTPS

Consulta de registros sin procesar en Detective

Tras integrar Detective con Security Lake, Detective comienza a extraer registros sin procesar de Security Lake relacionados con los eventos de AWS CloudTrail administración y los registros de flujo de Amazon Virtual Private Cloud (Amazon VPC).

> **Note**
>
> No hay recargos adicionales por consultar registros sin procesar en Detective. Los cargos por uso de otros AWS servicios, incluido Amazon Athena, se seguirán aplicando a las tarifas publicadas.

AWS CloudTrail Los eventos de gestión están disponibles para los siguientes perfiles:

- AWS cuenta
- AWS usuario
- AWS rol
- AWS sesión de rol
- EC2 Instancia de Amazon
- Bucket de Amazon S3
- Dirección IP
- Clúster de Kubernetes
- Pod de Kubernets
- Asunto de Kubernet
- rol de IAM
- Sesión de rol de IAM
- Usuario de IAM

FLow Los registros de Amazon VPC están disponibles para los siguientes perfiles:

- EC2 Instancia de Amazon
- Pod de Kubernetes

Para ver una demostración de cómo integrar Amazon Detective con Amazon Security Lake mediante la consola Detective, vea el siguiente vídeo: Integración de Amazon Detective con Amazon Security Lake: Cómo utilizarla -->

Consulta de los registros sin procesar de una cuenta de AWS

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Roles y, a continuación, busque una `AWS account`.
3. En la sección Volumen total de llamadas a la API, seleccione Mostrar los detalles del rango de tiempo.
4. Desde aquí puede empezar a Consultar registros sin procesar.

En la tabla Vista previa del registro sin procesar puede ver los registros y los eventos recuperados consultando datos de Security Lake. Para obtener más información sobre los registros de eventos sin procesar, puede ver los datos que se muestran en Amazon Athena.

Raw log preview: CloudTrail

View raw event logs that were retrieved by querying data from Security Lake. For more details about the raw event logs, you can view the data displayed in Athena.

Raw log preview (500+)

1 2 3 4 5 6 7 ... 50

date_time	requestor_arn	account_id	region	source_ip	service	api_
2023-12-22 09:58:38.000 UTC			us-east-1		s3.amazonaws.com	GetE
2023-12-22 09:59:49.000 UTC			us-east-1		sts.amazonaws.com	Assu
2023-12-22 10:00:13.000 UTC			us-east-1		ec2.amazonaws.com	Desc
2023-12-22 10:00:13.000 UTC			us-east-1		sts.amazonaws.com	Assu
2023-12-22 10:00:13.000 UTC			us-east-1		iam.amazonaws.com	GetI
2023-12-22 10:00:13.000 UTC			us-east-1		sts.amazonaws.com	Assu
2023-12-22 10:00:13.000 UTC			us-east-1		sts.amazonaws.com	GetC
2023-12-22 10:00:13.000 UTC			us-east-1		autoscaling.amazonaws.com	Desc
2023-12-22 10:00:14.000 UTC			us-east-1		ec2.amazonaws.com	Desc
2023-12-22 10:00:14.000 UTC			us-east-1		ec2.amazonaws.com	Desc

Close | Cancel query request | See results in Athena | Download results

En la tabla Registros de consulta sin procesar, puede Cancelar solicitud de consulta, Ver resultados en Amazon Athena y Descargar resultados como archivo de valores separados por comas (.csv).

Si ve registros en Detective, pero la consulta no devuelve resultados, podría deberse a los siguientes motivos.

- Es posible que los registros sin procesar pasen a estar disponibles en Detective antes de mostrarse en tablas de registros de Security Lake. Inténtelo de nuevo más tarde.
- Es posible que falten registros en Security Lake. Si esperó durante un período prolongado, significa que faltan registros en Security Lake. Póngase en contacto con el administrador de Security Lake para solucionar el problema.

Ejemplos

- Consultando registros sin procesar para un rol AWS
- Consulta de registros sin procesar para un clúster de Amazon EKS
- Consulta de registros sin procesar para una instancia de Amazon EC2

Consultando registros sin procesar para un rol AWS

Si quieres entender la actividad de un AWS rol en una nueva geolocalización, puedes hacerlo en la consola de Detectives.

Para consultar los registros sin procesar de un rol de AWS

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En la sección Geolocalizaciones recientemente observadas de la página Resumen del Detective, anote la AWS función.
3. En el panel de navegación, elija Buscar y, a continuación, busque el `AWS role`.
4. Para el AWS rol, amplíe el recurso para mostrar las llamadas a la API específicas que ese recurso emitió desde esa dirección IP.
5. Seleccione el icono de lupa situado junto a la llamada a la API que desea investigar para abrir la tabla Vista previa del registro sin procesar.

Consulta de registros sin procesar para un clúster de Amazon EKS

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En la sección Clústeres de contenedores con el mayor número de pods creados de la página Resumen del Detective, navegue hasta un clúster de Amazon EKS.
3. En la página de detalles del clúster de Amazon EKS, seleccione la pestaña de actividad de la API de Kubernets.

4. En la sección Actividad general de la API de Kubernets relacionada con este clúster de Amazon EKS, selecciona Mostrar detalles para el tiempo de alcance.
5. Desde aquí puede empezar a Consultar registros sin procesar.

Consulta de registros sin procesar para una instancia de Amazon EC2

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Buscar y, a continuación, busque una `Amazon EC2 instance`.
3. En la sección Volumen total del flujo de la VPC, seleccione el icono de lupa situado junto a la llamada a la API que desea investigar para abrir la tabla Vista previa de registros sin procesar.
4. Desde aquí puede empezar a Consultar registros sin procesar.

En la tabla Vista previa del registro sin procesar puede ver los registros y los eventos recuperados consultando datos de Security Lake. Para obtener más información sobre los registros de eventos sin procesar, puede ver los datos que se muestran en Amazon Athena.

En la tabla Registros de consulta sin procesar, puede Cancelar solicitud de consulta, Ver resultados en Amazon Athena y Descargar resultados como archivo de valores separados por comas (.csv).

Desactivación de la integración de Detective con Security Lake

Si deshabilita la integración de Detective con Security Lake ya no podrá consultar los datos de registros y eventos de Security Lake.

Para deshabilitar la integración de Detective con Security Lake

1. Abre la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, elija Integraciones.
3. Elimine la pila existente. Para obtener más información, consulta Eliminar una CloudFormation pila.
4. En el panel Deshabilitar la integración de Security Lake, seleccione Deshabilitar.

Eliminar una CloudFormation pila

Si no elimina la pila existente, no se podrá crear una nueva pila en la misma región. Puede eliminar una CloudFormation pila mediante la CloudFormation consola o mediante la AWS CLI.

Para eliminar la AWS CloudFormation pila (consola)

1. Abre la AWS CloudFormation consola en https://console.aws.amazon.com/cloudformation.
2. En la página Stacks de la CloudFormation consola, selecciona la pila que quieres eliminar. La pila se debe estar ejecutando en este momento.
3. En el panel de detalles de la pila, seleccione Eliminar.
4. Seleccione Eliminar pila cuando se le indique.

> **Note**
>
> La operación de eliminación de la pila no se puede detener una vez que comienza. La pila avanza al estado `DELETE_IN_PROGRESS`.

Una vez que se haya completado la eliminación de la pila, la pila estará en el estado `DELETE_COMPLETE`.

Solución de errores de eliminación de pilas

Si aparece un error de permiso en el mensaje `Failed to delete stack` después de hacer clic en el `Delete` botón, significa que tu rol de IAM no tiene CloudFormation permiso para eliminar una pila. Póngase en contacto con el administrador de su cuenta para eliminar la pila.

Para eliminar la CloudFormation pila (AWS CLI)

Introduzca el siguiente comando en la interfaz AWS CLI:

```
aws cloudformation delete-stack --stack-name your-stack-name --role-arn
      arn:aws:iam::<ACCOUNT ID>:role/CFN-DetectiveSecurityLakeIntegration
```

`CFN-DetectiveSecurityLakeIntegration` es el rol de servicio que creó en el paso `Creating an AWS CloudFormation Service Role`.

Previsión y supervisión de los costes de los Detectives

Para ayudarlo a hacer el seguimiento de su actividad en Detective, la página Uso muestra la cantidad de ingesta de datos y el costo previsto.

- En el caso de las cuentas de administrador, la página Uso muestra el volumen de datos y el costo previsto en todo el gráfico de comportamiento.
- En el caso de las cuentas de miembro, la página Uso muestra el volumen de datos y el costo previsto de la cuenta en los gráficos de comportamiento a los que contribuyen.

Detective también admite el AWS CloudTrail registro.

Contenido

- Acerca de la prueba gratuita para gráficos de comportamiento
- Supervisión del uso de una cuenta de administrador de Detective
- Supervisión del uso de una cuenta de miembro de Detective
- Cómo calcula Amazon Detective el costo previsto

Acerca de la prueba gratuita para gráficos de comportamiento

Amazon Detective ofrece una prueba gratuita de 30 días para cada cuenta de cada región. La prueba gratuita de una cuenta comienza la primera vez que se lleva a cabo una de las siguientes acciones.

- Una cuenta habilita Detective manualmente y se convierte en la cuenta de administrador de un gráfico de comportamiento.
- Se designa una cuenta como cuenta de administrador de Detective para una organización en AWS Organizations y es la primera vez que se habilita Detective en dicha cuenta.
- Si Detective ya estaba habilitado en la cuenta de administrador antes de la designación, no se inicia una nueva prueba gratuita de 30 días en la cuenta.
- Una cuenta acepta una invitación para que se asigne como cuenta de miembro en un gráfico de comportamiento y se habilita como cuenta de miembro.
- La cuenta de administrador de Detective habilita una cuenta de la organización como cuenta de miembro.

A partir de ese momento, la prueba gratuita dura 30 días. No se facturará por el procesamiento de datos de la cuenta durante ese periodo. Cuando finaliza el periodo de prueba, Detective empieza a cobrar a la cuenta por los datos que aporta a los gráficos de comportamiento. Para obtener más información sobre cómo puede llevar un seguimiento de la actividad de Detective, supervisar el uso y ver el costo previsto, consulte Previsión y supervisión de los costes de los Detectives. Para obtener más información acerca de los precios, consulte Precios de Detective.

Se utiliza el mismo periodo de 30 días para todos los gráficos de comportamiento de una región. Supongamos que, por ejemplo, una cuenta se habilita como cuenta de miembro en un gráfico de comportamiento. Esta acción provoca el inicio de un periodo de prueba gratuita de 30 días. Una vez transcurridos 10 días de prueba, la cuenta se habilita en un segundo gráfico de comportamiento en la misma región. Para este segundo gráfico de comportamiento, la cuenta dispondrá de 20 días de datos gratuitos.

La versión de prueba gratuita ofrece múltiples beneficios:

- Las cuentas de administrador pueden descubrir las funcionalidades y características de Detective para comprobar su valor.
- Las cuentas de administrador y de miembros pueden supervisar el volumen de datos y el coste estimado antes de que Detective empiece a cobrar por ellos. Consulte the section called “Uso y costo de la cuenta de administrador” y the section called “Seguimiento del uso de cuentas de miembro”.

Versión de prueba gratuita para orígenes de datos opcionales

Detective también ofrece una prueba gratuita durante 30 días para orígenes de datos opcionales. Esta versión de prueba gratuita es independiente de la prueba gratuita que se ofrece para los orígenes de datos principales de Detective cuando Detective se habilita por primera vez.

> **Note**
>
> Si un cliente deshabilita un paquete de origen de datos opcional en el plazo de 7 días después de habilitarlo, Detective puede reiniciar una sola vez y de forma automática la versión de prueba gratuita para ese paquete de origen de datos si se habilita de nuevo.

Para habilitar o deshabilitar un origen de datos opcional, consulte Tipos de orígenes de datos opcionales en Detective.

Supervisión del uso de una cuenta de administrador de Detective

Amazon Detective factura a cada cuenta los datos utilizados en cada gráfico de comportamiento al que pertenece la cuenta. Detective cobra una tarifa plana por niveles por GB para todos los datos, con independencia de su origen.

Para las cuentas de administrador, la página Uso de la consola de Detective le permite ver el volumen de datos ingeridos Por origen de datos o Por cuenta en los 30 días anteriores. Las cuentas de administrador también ven un costo previsto para un periodo típico de 30 días, para su cuenta y para todo el gráfico de comportamiento.

Para ver la información de uso de Detective

1. Inicie sesión en AWS Management Console. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, en Configuración, elija Uso.
3. Elija una pestaña para optar por ver el uso Por origen de datos o Por cuenta.

Volumen de ingesta de datos de cada cuenta

El volumen de ingesta por cuenta de miembro muestra las cuentas activas en el gráfico de comportamiento. No incluye las cuentas de miembro eliminadas.

Para cada cuenta, la lista de ingesta de volumen proporciona la siguiente información.

- El identificador de la AWS cuenta y la dirección de correo electrónico del usuario raíz.
- La fecha en la que la cuenta comenzó a contribuir con datos al gráfico de comportamiento.

  Para la cuenta de administrador, esta es la fecha en la que la cuenta habilitó Detective.

  En el caso de las cuentas de miembro, esta es la fecha en la que se habilitó una cuenta como cuenta de miembro tras aceptar la invitación.
- El volumen de ingesta de datos de la cuenta durante los 30 días anteriores. El total incluye todos los tipos de origen.
- Si la cuenta se encuentra actualmente dentro del periodo de prueba gratuito. En el caso de las cuentas que se encuentran dentro del periodo de prueba gratuito, la lista muestra el número de días restantes.

Si ninguna de las cuentas está dentro del periodo de prueba gratuito, no se mostrará la columna de estado de la prueba gratuita.

Costos previstos del gráfico de comportamiento

Costo previsto de esta cuenta muestra el costo previsto de 30 días de datos para la cuenta de administrador. El costo previsto se basa en el volumen promedio diario de la cuenta de administrador.

> **Important**
>
> Esta cantidad es solo un costo previsto. Proyecta el costo total de datos de la cuenta de administrador durante un periodo típico de 30 días. Se basa en el uso de los 30 días anteriores. Consulte the section called “Cómo calcula Detective el costo previsto”.

Costo previsto del gráfico de comportamiento

Costo previsto de todas las cuentas muestra un costo total previsto de 30 días de datos para todo el gráfico de comportamiento. El costo previsto se basa en el volumen promedio diario de cada cuenta.

> **Important**
>
> Esta cantidad es solo un costo previsto. Proyecta el costo total de los datos del gráfico de comportamiento para un periodo típico de 30 días. Se basa en el uso de los 30 días anteriores. El costo previsto no incluye las cuentas de miembro que se hayan eliminado del gráfico de comportamiento. Consulte the section called “Cómo calcula Detective el costo previsto”.

Volumen de ingesta de datos por paquetes de origen

Seleccione Por paquete de origen para ver el volumen de ingesta de datos, enumerado por los distintos paquetes de origen habilitados en su gráfico de comportamiento.

Todas las cuentas pueden ver estos datos para sus propias cuentas. Una cuenta de administrador puede ver paneles adicionales que enumeran el uso por paquete de origen de cada miembro. No incluye las cuentas de miembro eliminadas.

Detective básico

Los paneles principales de Detective muestran el volumen de datos ingeridos de las fuentes principales de Detective (CloudTrail registros, registros de VPC flujo y GuardDuty hallazgos) durante los últimos 30 días.

Registros de auditoría de EKS

EKSLos paneles de registros de auditoría muestran el volumen de datos ingeridos de las fuentes de registros de EKS auditoría durante los últimos 30 días. Los paneles de este paquete fuente solo están disponibles si los registros de EKS auditoría están habilitados para el gráfico de comportamiento.

Supervisión del uso de una cuenta de miembro de Detective

Amazon Detective factura a cada cuenta los datos utilizados en cada gráfico de comportamiento al que pertenece la cuenta. Detective cobra una tarifa plana por niveles por GB para todos los datos, con independencia de su origen.

En el caso de las cuentas de miembro, la página Uso muestra el volumen de datos y el costo previsto a 30 días solo para dicha cuenta.

Para ver la información de uso de Detective

1. Inicie sesión en AWS Management Console. A continuación, abra la consola de Detectives en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, en Configuración, elija Uso.

Volumen de ingesta de cada gráfico de comportamiento

Volumen de ingesta de esta cuenta muestra los gráficos de comportamiento a los que contribuye la cuenta de miembro. No incluye las pertenencias a las que ha renunciado ni las pertenencias que la cuenta de administrador ha eliminado.

La lista incluye la siguiente información acerca de cada gráfico de comportamiento:

- El número de cuenta de la cuenta de administrador
- El volumen de ingesta de datos de la cuenta de miembro durante los 30 días anteriores. El total incluye todos los tipos de origen.

- La fecha en la que se habilitó la cuenta de miembro para el gráfico de comportamiento.

Costo previsto en todos los gráficos de comportamiento

Costo previsto de esta cuenta muestra un costo previsto para 30 días de datos para la cuenta de miembro en todos los gráficos de comportamiento a los que contribuye. El costo previsto se basa en el volumen promedio diario de la cuenta de miembro.

> **Important**
>
> Esta cantidad es solo un costo previsto. Proyecta el costo total de datos de la cuenta de administrador durante un periodo típico de 30 días. Se basa en el uso de los 30 días anteriores. Consulte the section called “Cómo calcula Detective el costo previsto”.

Cómo calcula Amazon Detective el costo previsto

Para calcular los valores de costo previsto que se muestran en la página Uso, Detective hace lo siguiente:

1. Para obtener el costo previsto de una cuenta individual en un gráfico de comportamiento, Detective hace lo siguiente:
   a. Calcula el volumen promedio por día. Añade el volumen de datos de todos los días activos y, a continuación, lo divide entre el número de días que la cuenta ha estado activa.

      Si la cuenta se habilitó hace más de 30 días, el número de días es 30. Si la cuenta se habilitó hace menos de 30 días, el número de días es el transcurrido desde la fecha de aceptación.

      Por ejemplo, si la cuenta se habilitó hace 12 días, Detective suma el volumen de ingesta de esos 12 días y, a continuación, lo divide entre 12.

   b. Multiplica por 30 el promedio diario de la cuenta. Este es el uso previsto de la cuenta para 30 días.

   c. Usa su modelo de precios para calcular el costo previsto a 30 días para el uso previsto en 30 días.
2. Para obtener el costo previsto total de un gráfico de comportamiento, Detective hace lo siguiente:
   a. Combina el uso previsto para 30 días de todas las cuentas del gráfico de comportamiento.

   b. Usa su modelo de precios para calcular el costo previsto a 30 días para el uso previsto total de 30 días.
3. Para obtener el costo previsto total de una cuenta de miembro en todos los gráficos de comportamiento, Detective hace lo siguiente:
   a. Combina el uso previsto para 30 días de todos los gráficos de comportamiento.
   b. Usa su modelo de precios para calcular el costo previsto a 30 días para el uso previsto total de 30 días.
4. Si utiliza una VPC de Amazon compartida, Detective calcula el costo previsto en función de la actividad de monitorización. Le recomendamos que revise el costo proyectado de sus investigaciones específicas para su entorno.
   a. Si una cuenta miembro de Detective tiene una VPC de Amazon compartida y hay otras cuentas ajenas a Detective que utilizan la VPC compartida, Detective supervisará todo el tráfico de esa VPC. El uso y el costo aumentarán y Detective proporcionará una visualización de todo el flujo de tráfico de la VPC.
   b. Si tiene una instancia de EC2 dentro de una VPC de Amazon compartida y el propietario compartido no es miembro de Detective, Detective no monitorizará tráfico de la VPC y, por tanto, el uso y el costo disminuirán. Si desea ver el flujo de tráfico dentro de la VPC, debe agregar al propietario de la VPC de Amazon como miembro de su gráfico de Detective.

Seguridad en Amazon Detective

La seguridad en la nube AWS es la máxima prioridad. Como AWS cliente, usted se beneficia de una arquitectura de centro de datos y red diseñada para cumplir con los requisitos de las organizaciones más sensibles a la seguridad.

La seguridad es una responsabilidad compartida entre usted 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 AWS los servicios en la AWS nube. AWS también le proporciona servicios que puede utilizar de forma segura.

  Auditores independientes prueban y verifican periódicamente la eficacia de nuestra seguridad en el marco de los programas de conformidad de AWS.

  Para obtener más información acerca de los programas de conformidad que se aplican a Amazon Detective, consulte Servicios de AWS en el ámbito del programa de conformidad.
- Seguridad en la nube: su responsabilidad viene determinada por el AWS servicio que utilice. Usted también es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y los reglamentos aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Detective. En los siguientes temas, se le mostrará cómo configurar Detective para satisfacer sus objetivos de seguridad y conformidad. También aprenderá a usar otros AWS servicios que lo ayudan a monitorear y proteger sus recursos de Detective.

Contenido

- Protección de datos en Amazon Detective
- Identity and Access Management para Amazon Detective
- Validación de conformidad para Amazon Detective
- Resiliencia de Amazon Detective
- Seguridad de la infraestructura en Amazon Detective
- Mejores prácticas de seguridad para Detectives

Protección de datos en Amazon Detective

La AWS modelo de responsabilidad compartida se aplica a la protección de datos en Amazon Detective. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global en la que se ejecutan todos los Nube de AWS. Usted es responsable de mantener el control sobre el contenido que está alojado en esta infraestructura. También es responsable de las tareas de configuración y administración de la seguridad del Servicios de AWS que utilizas. Para obtener más información sobre la privacidad de los datos, consulte la sección Privacidad de datos FAQ. Para obtener información sobre la protección de datos en Europa, consulte la AWS Modelo de responsabilidad compartida y GDPR entrada de blog sobre el AWS Blog de seguridad.

Para fines de protección de datos, le recomendamos que proteja Cuenta de AWS credenciales y configure los usuarios 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 multifactorial (MFA) con cada cuenta.
- UtiliceSSL/TLSpara comunicarse con AWS recursos. Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Configure API y registre la actividad del usuario con AWS CloudTrail. Para obtener información sobre el uso de CloudTrail senderos para capturar AWS actividades, consulte Trabajar con CloudTrail senderos en la AWS CloudTrail Guía del usuario.
- Uso AWS soluciones de cifrado, junto con todos los controles de seguridad predeterminados 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 entre FIPS 140 y 3 módulos criptográficos validados para acceder AWS mediante una interfaz de línea de comandos o un API FIPS terminal. Para obtener más información sobre los FIPS puntos finales disponibles, consulte la Norma Federal de Procesamiento de Información (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 cuando trabajas con un Detective u otro Servicios de AWS usando la consolaAPI, AWS CLI, o AWS SDKs. 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, le recomendamos encarecidamente que no incluya información sobre las credenciales URL para validar su solicitud a ese servidor.

Detective cifra todos los datos que procesa y los almacena en reposo y en tránsito.

Contenido

- Administración de claves para Amazon Detective

Administración de claves para Amazon Detective

Dado que Detective no almacena ningún dato de identificación personal del cliente, utiliza Claves administradas por AWS.

Este tipo de clave KMS se puede utilizar en varias cuentas. Consulte la descripción de las claves AWS propias en la Guía para AWS Key Management Service desarrolladores.

Este tipo de clave KMS rota automáticamente cada año (aproximadamente cada 365 días). Consulte la descripción de la rotación de claves en la Guía para AWS Key Management Service desarrolladores.

Identity and Access Management para Amazon Detective

AWS Identity and Access Management (IAM) es una Servicio de AWS que ayuda al administrador a controlar de forma segura el acceso a AWS los recursos. IAMlos administradores controlan quién puede autenticarse (iniciar sesión) y quién está autorizado (tiene permisos) para usar los recursos de Detective. IAMes una Servicio de AWS que puede utilizar sin coste adicional.

Contenido

- Público
- Autenticación con identidades
- Administración de acceso mediante políticas
- Cómo funciona Amazon Detective con IAM
- Ejemplos de políticas de basadas en identidades de Amazon Detective
- AWS políticas gestionadas para Amazon Detective
- Usar roles vinculados a servicios para Detective

- Solución de problemas de identidad y acceso de Amazon Detective

Público

La forma de usar AWS Identity and Access Management (IAM) varía según el trabajo que realices en Detective.

Usuario del servicio: si utiliza el servicio de Detective para realizar su trabajo, el administrador le proporciona las credenciales y los permisos que necesita. A medida que utilice más características de Detective para realizar su trabajo, es posible que necesite permisos adicionales. Entender cómo se administra el acceso puede ayudarle a solicitar los permisos correctos al administrador. Si no puede acceder a una característica en Detective, consulte Solución de problemas de identidad y acceso de Amazon Detective.

Administrador del servicio: si está a cargo de los recursos de Detective en su empresa, probablemente tenga acceso completo a Detective. Su trabajo consiste en determinar a qué características y recursos de Detective deben acceder los usuarios del servicio. A continuación, debe enviar solicitudes a su IAM administrador para cambiar los permisos de los usuarios del servicio. Revise la información de esta página para comprender los conceptos básicos deIAM. Para obtener más información sobre cómo su empresa puede utilizar IAM Detective, consulteCómo funciona Amazon Detective con IAM.

IAMadministrador: si es IAM administrador, es posible que desee obtener información sobre cómo escribir políticas para administrar el acceso a Detective. Para ver ejemplos de políticas basadas en la identidad de los Detectives que puede utilizarIAM, consulte. Ejemplos de políticas de basadas en identidades de Amazon Detective

Autenticación con identidades

La autenticación es la forma de iniciar sesión AWS con sus credenciales de identidad. Debe estar autenticado (con quien haya iniciado sesión AWS) como IAM usuario o asumiendo un IAM rol. Usuario raíz de la cuenta de AWS

Puede iniciar sesión AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad. AWS IAM Identity Center Los usuarios (IAMIdentity Center), 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, el administrador configuró previamente la federación de identidades mediante roles. IAM Cuando accede AWS mediante la federación, asume indirectamente un rol.

Según el tipo de usuario que sea, puede iniciar sesión en el portal AWS Management Console o en el de AWS acceso. Para obtener más información sobre cómo iniciar sesión AWS, consulte Cómo iniciar sesión Cuenta de AWS en su Guía del AWS Sign-In usuario.

Si accede AWS mediante programación, AWS incluye un kit de desarrollo de software (SDK) y una interfaz de línea de comandos (CLI) para firmar criptográficamente sus solicitudes con sus credenciales. Si no utilizas AWS herramientas, debes firmar las solicitudes tú mismo. Para obtener más información sobre cómo usar el método recomendado para firmar las solicitudes usted mismo, consulte la versión 4 de la AWS firma para ver API las solicitudes en la Guía del IAM usuario.

Independientemente del método de autenticación que use, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, le AWS recomienda que utilice la autenticación multifactorial (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactorial en la Guía del AWS IAM Identity Center usuario y Autenticación AWS multifactorial IAM en la Guía del IAM usuario.

Cuenta de AWS usuario root

Al crear una Cuenta de AWS, comienza con una identidad de inicio de sesión que tiene acceso completo a todos Servicios de AWS los recursos de la cuenta. Esta identidad se denomina usuario Cuenta de AWS raíz y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizaste 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 tareas que requieren que inicie sesión como usuario root, consulte Tareas que requieren credenciales de usuario root en la Guía del IAM usuario.

Usuarios y grupos de IAM

Un IAMusuario es una identidad propia Cuenta de AWS que tiene permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos utilizar credenciales temporales en lugar de crear IAM usuarios con credenciales de larga duración, como contraseñas y claves de acceso. Sin embargo, si tiene casos de uso específicos que requieren credenciales a largo plazo con IAM los usuarios, le recomendamos que rote las claves de acceso. Para obtener más información, consulte Rotar las claves de acceso con regularidad para los casos de uso que requieran credenciales de larga duración en la Guía del IAM usuario.

Un IAMgrupo es una identidad que especifica un conjunto de IAM usuarios. No puede iniciar sesión como grupo. Puede usar los grupos para especificar permisos para varios usuarios a la vez. Los

grupos facilitan la administración de los permisos para grandes conjuntos de usuarios. Por ejemplo, puede asignar un nombre a un grupo IAMAdminsy concederle permisos para administrar IAM los recursos.

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 IAM usuarios en la Guía del IAM usuario.

IAMFunciones

Un IAMrol es una identidad dentro de ti Cuenta de AWS que tiene permisos específicos. Es similar a un IAM usuario, pero no está asociado a una persona específica. Para asumir temporalmente un IAM rol en la AWS Management Console, puede cambiar de un IAM rol de usuario a uno (consola). Puede asumir un rol llamando a una AWS API operación AWS CLI o o utilizando una operación personalizadaURL. Para obtener más información sobre los métodos de uso de roles, consulte Métodos para asumir un rol en la Guía del IAM usuario.

IAMlos roles con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, puede 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 sobre los roles para la federación, consulte Crear un rol para un proveedor de identidades externo (federación) en la Guía del IAM usuario. Si usa IAM Identity Center, configura un conjunto de permisos. Para controlar a qué pueden acceder sus identidades después de autenticarse, IAM Identity Center correlaciona el conjunto de permisos con un rol en. IAM Para obtener información acerca de los conjuntos de permisos, consulta Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center .
- Permisos IAM de usuario temporales: un IAM usuario o rol puede asumir un IAM rol para asumir temporalmente diferentes permisos para una tarea específica.
- Acceso multicuenta: puedes usar un IAM rol para permitir que alguien (un responsable de confianza) de una cuenta diferente acceda a los recursos de tu cuenta. Los roles son la forma principal de conceder acceso entre cuentas. Sin embargo, con algunos Servicios de AWS, puedes adjuntar una política directamente a un recurso (en lugar de usar un rol como proxy). Para conocer la diferencia entre las funciones y las políticas basadas en recursos para el acceso multicuenta, consulta el tema sobre el acceso a los recursos entre cuentas IAM en la Guía del IAM usuario.

- Acceso entre servicios: algunos Servicios de AWS utilizan funciones en otros. Servicios de AWS Por ejemplo, cuando realizas una llamada en un servicio, es habitual 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 al servicio.
  - Sesiones de acceso directo (FAS): cuando utilizas un IAM usuario o un rol para realizar acciones en AWS ellas, se te considera director. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FASutiliza los permisos del principal que llama a an Servicio de AWS, junto con los que solicitan, Servicio de AWS para realizar solicitudes a los servicios descendentes. FASlas solicitudes solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información detallada sobre la política a la hora de realizar FAS solicitudes, consulte Reenviar las sesiones de acceso.
  - Función de servicio: una función de servicio es una IAMfunción que un servicio asume para realizar acciones en su nombre. Un IAM administrador puede crear, modificar y eliminar un rol de servicio desde dentroIAM. Para obtener más información, consulte Crear un rol para delegar permisos a un Servicio de AWS en la Guía del IAM usuario.
  - Función vinculada a un servicio: una función vinculada a un servicio es un tipo de función de servicio que está vinculada a un. Servicio de AWS El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados al servicio aparecen en usted Cuenta de AWS y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.
- Aplicaciones que se ejecutan en Amazon EC2: puedes usar un IAM rol para administrar las credenciales temporales de las aplicaciones que se ejecutan en una EC2 instancia y que realizan AWS CLI o AWS API solicitan. Esto es preferible a almacenar las claves de acceso dentro de la EC2 instancia. Para asignar un AWS rol a una EC2 instancia y ponerlo a disposición de todas sus aplicaciones, debe crear un perfil de instancia adjunto a la instancia. Un perfil de instancia contiene el rol y permite que los programas que se ejecutan en la EC2 instancia obtengan credenciales temporales. Para obtener más información, consulta Usar un IAM rol para conceder permisos a las aplicaciones que se ejecutan en EC2 instancias de Amazon en la Guía del IAM usuario.

Administración de acceso mediante políticas

El acceso se controla AWS creando políticas y adjuntándolas a AWS identidades o recursos. Una política es un objeto AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando un director (usuario, usuario raíz o sesión de rol) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan AWS como JSON documentos. Para obtener más información sobre la estructura y el contenido de los documentos de JSON políticas, consulte Descripción general de JSON las políticas en la Guía del IAM usuario.

Los administradores pueden usar AWS JSON las políticas 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. Para conceder a los usuarios permiso para realizar acciones en los recursos que necesitan, un IAM administrador puede crear IAM políticas. A continuación, el administrador puede añadir las IAM políticas a las funciones y los usuarios pueden asumir las funciones.

IAMlas políticas definen los permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con esa política puede obtener información sobre el rol de AWS Management Console AWS CLI, el o el AWS API.

Políticas basadas en identidad

Las políticas basadas en la identidad son documentos de política de JSON permisos que se pueden adjuntar a una identidad, como un IAM usuario, 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 la identidad, consulte Definir IAM permisos personalizados con políticas administradas por el cliente en la Guía del usuario. 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 administradas son políticas independientes que puede adjuntar a varios usuarios, grupos y funciones de su empresa. Cuenta de AWS Las políticas administradas incluyen políticas AWS administradas y políticas administradas por el cliente. Para saber cómo elegir entre una política gestionada o una política integrada, consulte Elegir entre políticas gestionadas y políticas integradas en la Guía del IAM usuario.

Políticas basadas en recursos

Las políticas basadas en recursos son documentos de JSON política que se adjuntan a un recurso. Algunos ejemplos de políticas basadas en recursos son las políticas de confianza de IAM roles 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. Los principales pueden 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 puede usar políticas AWS administradas desde una política IAM basada en recursos.

Listas de control de acceso () ACLs

Las listas de control de acceso (ACLs) controlan qué directores (miembros de la cuenta, usuarios o roles) tienen permisos para acceder a un recurso. ACLsson similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de JSON políticas.

Amazon S3 AWS WAF y Amazon VPC son ejemplos de servicios compatiblesACLs. Para obtener más informaciónACLs, consulte la descripción general de la lista de control de acceso (ACL) en la Guía para desarrolladores de Amazon Simple Storage Service.

Otros tipos de políticas

AWS admite tipos de políticas adicionales y menos comunes. 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 función avanzada en la que se establecen los permisos máximos que una política basada en la identidad puede conceder a una IAM entidad (IAMusuario o rol). 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, consulte los límites de los permisos para IAM las entidades en la Guía del IAMusuario.

- Políticas de control de servicios (SCPs): SCPs son JSON políticas que especifican los permisos máximos para una organización o unidad organizativa (OU) AWS Organizations. AWS Organizations es un servicio para agrupar y administrar de forma centralizada varios de los Cuentas de AWS que son propiedad de su empresa. Si habilitas todas las funciones de una organización, puedes aplicar políticas de control de servicios (SCPs) a una o a todas tus cuentas. SCPLimita los permisos de las entidades en las cuentas de los miembros, incluidas las de cada una Usuario raíz de la cuenta de AWS. Para obtener más información sobre OrganizationsSCPs, consulte las políticas de control de servicios en la Guía del AWS Organizations usuario.
- Políticas de control de recursos (RCPs): RCPs son JSON políticas que puedes usar para establecer los permisos máximos disponibles para los recursos de tus cuentas sin actualizar las IAM políticas asociadas a cada recurso que poseas. Esto RCP limita los permisos de los recursos en las cuentas de los miembros y puede afectar a los permisos efectivos de las identidades Usuario raíz de la cuenta de AWS, incluidos los permisos, independientemente de si pertenecen a su organización. Para obtener más información sobre Organizations e RCPs incluir una lista de Servicios de AWS ese apoyoRCPs, consulte Políticas de control de recursos (RCPs) en la Guía del AWS Organizations usuario.
- 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 obtener más información, consulte las políticas de sesión en la Guía del IAM usuario.

Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para saber cómo se AWS determina si se debe permitir una solicitud cuando se trata de varios tipos de políticas, consulte la lógica de evaluación de políticas en la Guía del IAM usuario.

Cómo funciona Amazon Detective con IAM

De forma predeterminada, los usuarios y roles no tienen permiso para crear ni modificar los recursos de Amazon Detective. Tampoco pueden realizar tareas con AWS Management Console AWS CLI, o AWS API. Un administrador de Detectives debe tener AWS Identity and Access Management (IAM) políticas que concedan permiso a IAM los usuarios y roles para realizar API operaciones específicas

en los recursos específicos que necesitan. El administrador debe asociar esas políticas a la entidad principal que necesite esos permisos.

Detective utiliza políticas IAM basadas en la identidad para conceder permisos a los siguientes tipos de usuarios y acciones:

- Cuentas de administrador: la cuenta de administrador es el propietario de un determinado gráfico de comportamiento, que utiliza los datos de su cuenta. Las cuentas de administrador pueden invitar a cuentas de miembros para que aporten datos al gráfico de comportamiento. La cuenta de administrador también puede usar el gráfico de comportamiento para clasificar e investigar los hallazgos y los recursos asociados a esas cuentas.

  Puede configurar políticas para que todos los usuarios, además de las cuentas de administrador, puedan llevar a cabo distintas tareas. Por ejemplo, un usuario de una cuenta de administrador puede tener permisos únicamente para administrar cuentas de miembros. Es posible que otro usuario solo tenga permisos para usar el gráfico de comportamiento con fines de investigación.
- Cuentas de miembros: una cuenta de miembro es una cuenta a la que se le ha invitado a aportar datos a un gráfico de comportamiento. Para ello, la cuenta de miembro debe responder a una invitación. Después de aceptarla, la cuenta de miembro puede eliminar su cuenta del gráfico de comportamiento.

Para obtener una visión general de cómo Servicios de AWS trabajan Detective y otrosIAM, consulte Creación de políticas en la JSON pestaña de la Guía del IAM usuario.

Políticas basadas en identidades de Detective

Con las políticas IAM basadas en la identidad, puede especificar las acciones y los recursos permitidos o denegados, así como las condiciones en las que se permiten o deniegan las acciones. Detective admite acciones, claves de condición y recursos específicos.

Para obtener más información sobre todos los elementos que se utilizan en una JSON política, consulte la Referencia sobre los elementos IAM JSON de la política en la Guía del IAMusuario.

Acciones

Los administradores pueden usar AWS JSON políticas para especificar quién tiene acceso a qué. Es decir, qué entidad principal puedes realizar acciones en qué recursos y en qué condiciones.

El `Action` elemento de una JSON política describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de política suelen tener el mismo nombre que

la AWS API operación asociada. Hay algunas excepciones, como las acciones que solo permiten permisos y que no tienen una operación coincidente. API 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.

Las instrucciones de la política deben incluir un elemento `Action` o `NotAction`. El elemento `Action` enumera las acciones permitidas por la política, mientras que el elemento `NotAction` enumera las no permitidas.

Las acciones definidas para Detective le indican las tareas que puede llevar a cabo con Detective. Las acciones de políticas en Detective tienen el siguiente prefijo: `detective:`.

Por ejemplo, para conceder permiso para usar la `CreateMembers` API operación para invitar a las cuentas de los miembros a un gráfico de comportamiento, debes incluir la `detective:CreateMembers` acción en su política.

Para especificar varias acciones en una única instrucción, sepárelas con comas. Por ejemplo, en el caso de una cuenta de miembro, la política incluye el conjunto de acciones relacionadas con la administración de invitaciones:

```
"Action": [
      "detective:ListInvitations",
      "detective:AcceptInvitation",
      "detective:RejectInvitation",
      "detective:DisassociateMembership
]
```

También puede utilizar comodines (*) para especificar varias acciones. Por ejemplo, para gestionar los datos utilizados en un gráfico de rendimiento, las cuentas de administrador de Detective deben poder llevar a cabo las siguientes tareas:

- Consultar la lista de cuentas de miembros (`ListMembers`)
- Obtener información sobre determinadas cuentas de miembros (`GetMembers`)
- Invitar cuentas de miembros al gráfico de comportamiento (`CreateMembers`)
- Eliminar miembros del gráfico de comportamiento (`DeleteMembers`)

En lugar de enumerar estas acciones por separado, puede otorgar acceso a todas las acciones que terminan con la palabra `Members`. La política necesaria para ello incluiría la siguiente acción:

```
"Action": "detective:*Members"
```

Para ver una lista de las acciones de Detective, consulte Acciones definidas por Amazon Detective en la Referencia de autorizaciones de servicio.

Recursos

Los administradores pueden usar AWS JSON políticas 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` JSON de política especifica el objeto o los objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso mediante su 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 obtener más información sobre el formato deARNs, consulte Amazon Resource Names (ARNs) y AWS Service Namespaces.

En el caso de Detective, el único tipo de recurso disponible es el gráfico de comportamiento. El recurso gráfico de comportamiento de Detective tiene lo siguienteARN:

```
arn:aws:detective:${Region}:${AccountId}:graph:${GraphId}
```

En este ejemplo, el gráfico de comportamiento tiene los siguientes valores:

- La región del gráfico de comportamiento es `us-east-1`.
- El ID de la cuenta de administrador es `111122223333`.

- El ID del gráfico de comportamiento es `027c7c4610ea4aacaf0b883093cab899`.

Para identificar este gráfico de comportamiento en una `Resource` declaración, usaría lo siguienteARN:

```
"Resource": "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
```

Se utilizan comas para separar los distintos recursos de una instrucción `Resource`.

```
"Resource": [
      "resource1",
      "resource2"
]
```

Por ejemplo, se puede invitar a la misma AWS cuenta a ser una cuenta de miembro en más de un gráfico de comportamiento. En este caso, en la política de dicha cuenta de miembro, la instrucción `Resource` indica los gráficos de comportamiento a los que se ha invitado la cuenta.

```
"Resource": [
      "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
      "arn:aws:detective:us-east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
]
```

Algunas acciones de Detective, como crear un gráfico de comportamiento y enumerar gráficos de comportamiento o sus correspondientes invitaciones, no se llevan a cabo para un gráfico de comportamiento en concreto. En el caso de estas acciones, la instrucción `Resource` debe incluir el carácter comodín (*).

```
"Resource": "*"
```

En el caso de las acciones de la cuenta de administrador, Detective verifica siempre que el usuario que ha realizado la solicitud pertenece a la cuenta de administrador del gráfico de comportamiento correspondiente. En el caso de las acciones de cuentas de miembros, Detective verifica siempre que el usuario que ha realizado la solicitud pertenece a la cuenta de miembro. Incluso si una IAM política concede acceso a un gráfico de comportamiento, si el usuario no pertenece a la cuenta correcta, no podrá realizar la acción.

Para todas las acciones que se realizan en un gráfico de comportamiento específico, la IAM política debe incluir el gráficoARN. El gráfico se ARN puede añadir más adelante. Por ejemplo, cuando una cuenta activa Detective por primera vez, la IAM política inicial proporciona acceso a todas las acciones de Detective mediante el comodín del gráficoARN. De esta forma, el usuario puede empezar a administrar de inmediato las cuentas de miembros y llevar a cabo investigaciones con el gráfico de comportamiento. Una vez creado el gráfico de comportamiento, puede actualizar la política para añadir el gráficoARN.

Claves de condición

Los administradores pueden usar AWS JSON políticas 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 mediante una `OR` operación lógica. 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, puede conceder a un IAM usuario permiso para acceder a un recurso solo si está etiquetado con su nombre de IAM usuario. Para obtener más información, consulte los elementos IAM de la política: variables y etiquetas en la Guía del IAM usuario.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del IAMusuario.

Detective no define su propio conjunto de claves de condición, aunque sí admite el uso de claves de condición globales. Para ver todas las claves de condición AWS globales, consulte las claves de contexto de condición AWS globales en la Guía del IAM usuario.

Para obtener información sobre las acciones y los recursos que le permiten utilizar una clave de condición, consulte Acciones definidas por Amazon Detective.

Ejemplos

Para ver ejemplos de políticas basadas en identidades de Detective, consulte Ejemplos de políticas de basadas en identidades de Amazon Detective.

Políticas de Detective basadas en recursos (no compatibles)

Detective no admite políticas basadas en recursos.

Autorización basada en etiquetas de gráficos de comportamiento de Detective

Se pueden asignar valores de etiqueta a cada gráfico de comportamiento. Puede utilizar estos valores de etiqueta en instrucciones de condición para administrar el acceso al gráfico de comportamiento.

La instrucción de condición de un valor de etiqueta utiliza el siguiente formato.

```
{"StringEquals"{"aws:ResourceTag/<tagName>": "<tagValue>"}}
```

En el siguiente ejemplo, el código se utiliza para permitir o denegar una acción cuando el valor de la etiqueta `Department` es `Finance`.

```
{"StringEquals"{"aws:ResourceTag/Department": "Finance"}}
```

Para ver ejemplos de políticas que utilizan valores de etiqueta de recursos, consulte the section called “Cuenta de administrador: restricción del acceso en función de valores de etiqueta”.

IAMFunciones de Detective

Un IAMrol es una entidad de tu AWS cuenta que tiene permisos específicos.

Uso de credenciales temporales con Detective

Puedes usar credenciales temporales para iniciar sesión con la federación, asumir un IAM rol o asumir un rol multicuenta. Para obtener credenciales de seguridad temporales, puede llamar a AWS STS API operaciones como AssumeRoleo GetFederationToken.

Detective admite el uso de credenciales temporales.

Roles vinculados a servicios

Las funciones vinculadas al servicio permiten a AWS los servicios acceder a los recursos de otros servicios para completar una acción en su nombre. Los roles vinculados al servicio aparecen en tu IAM cuenta y son propiedad del servicio. Un IAM administrador puede ver los permisos de los roles vinculados al servicio, pero no editarlos.

Para obtener más información acerca de cómo crear o administrar roles vinculados a servicios de Detective, consulte the section called “Usar roles vinculados a servicios”.

Roles de servicio (no compatibles)

Esta característica permite que un servicio asuma un rol de servicio en su nombre. Este rol permite que el servicio obtenga acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles de servicio aparecen en tu IAM cuenta y son propiedad de la cuenta. Esto significa que un IAM administrador puede cambiar los permisos de este rol. Sin embargo, hacerlo podría deteriorar la funcionalidad del servicio.

Detective no admite roles de servicio.

Ejemplos de políticas de basadas en identidades de Amazon Detective

De forma predeterminada, IAM los usuarios y los roles no tienen permiso para crear o modificar los recursos de Detective. Tampoco pueden realizar tareas con AWS Management Console AWS CLI, o AWS API.

IAMEl administrador debe crear IAM políticas que concedan a los usuarios y roles permisos para realizar API operaciones específicas en los recursos específicos que necesitan. A continuación, el administrador adjunta esas políticas a los IAM usuarios o grupos que requieren esos permisos.

Para obtener información sobre cómo crear una política IAM basada en la identidad con estos documentos de JSON política de ejemplo, consulte Creación de políticas en la JSON pestaña de la Guía del IAM usuario.

Temas

- Prácticas recomendadas sobre las políticas
- Uso de la consola de Detective
- Cómo permitir a los usuarios que vean sus propios permisos

- Cuenta de administrador: administración de cuentas de miembros en un gráfico de comportamiento
- Cuenta de administrador: uso de un gráfico de comportamiento con fines de investigación
- Cuenta de miembro: administración de las invitaciones y suscripciones a gráficos de comportamiento
- Cuenta de administrador: restricción del acceso en función de valores de etiqueta

Prácticas recomendadas sobre las políticas

Las políticas basadas en identidades determinan si alguien puede crear o eliminar los recursos de Detective de la cuenta, o bien 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 AWS administradas y avance hacia los permisos con privilegios mínimos: para empezar a conceder permisos a sus usuarios y cargas de trabajo, utilice las políticas AWS administradas que otorgan permisos para muchos casos de uso comunes. Están disponibles en su. Cuenta de AWS Le recomendamos que reduzca aún más los permisos definiendo políticas administradas por el AWS cliente que sean específicas para sus casos de uso. Para obtener más información, consulte las políticas AWS gestionadas o las políticas AWS gestionadas para las funciones laborales en la Guía del IAM usuario.
- Aplique permisos con privilegios mínimos: cuando establezca permisos con IAM políticas, 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. Para obtener más información sobre cómo IAM aplicar permisos, consulte Políticas y permisos IAM en la IAM Guía del usuario.
- Utilice las condiciones en IAM las políticas para restringir aún más el acceso: puede añadir una condición a sus políticas para limitar el acceso a las acciones y los recursos. Por ejemplo, puede escribir una condición de política para especificar que todas las solicitudes deben enviarse medianteSSL. También puedes usar condiciones para conceder el acceso a las acciones del servicio si se utilizan a través de una acción específica Servicio de AWS, por ejemplo AWS CloudFormation. Para obtener más información, consulte los elementos IAM JSON de la política: Condición en la Guía del IAM usuario.
- Utilice IAM Access Analyzer para validar sus IAM políticas y garantizar permisos seguros y funcionales: IAM Access Analyzer valida las políticas nuevas y existentes para que se ajusten

al lenguaje de las políticas (JSON) y IAM a las IAM mejores prácticas. IAMAccess Analyzer proporciona más de 100 comprobaciones de políticas y recomendaciones prácticas para ayudarle a crear políticas seguras y funcionales. Para obtener más información, consulte Validar políticas con IAM Access Analyzer en la Guía del IAM usuario.

- Requerir autenticación multifactorial (MFA): si se encuentra en una situación en la que se requieren IAM usuarios o un usuario raíz Cuenta de AWS, actívela MFA para aumentar la seguridad. Para solicitarlo MFA cuando se convoque a API las operaciones, añada MFA condiciones a sus políticas. Para obtener más información, consulte APIAcceso seguro con MFA en la Guía del IAM usuario.

Para obtener más información sobre las prácticas recomendadasIAM, consulte las prácticas recomendadas de seguridad IAM en la Guía del IAM usuario.

Uso de la consola de Detective

Para utilizar la consola de Amazon Detective, el usuario o el rol deben tener acceso a las acciones relevantes, que coincidan con las acciones correspondientes deAPI.

Para habilitar Detective y trabajar con una cuenta de administrador en un gráfico de comportamiento, el usuario o el rol deben tener permiso para realizar la acción `CreateGraph`.

Para llevar a cabo acciones de la cuenta de administrador con la consola de Detective, el usuario o el rol deben tener permiso para realizar la acción `ListGraphs`. Esta acción concede permiso para obtener los gráficos de comportamiento en los que la cuenta tiene funciones de administrador. También debe tener permiso para realizar acciones específicas de la cuenta de administrador.

Las acciones más básicas de la cuenta de administrador son visualizar una lista de las cuentas de miembros de un gráfico de comportamiento y utilizar el gráfico de comportamiento con fines de investigación.

- Para ver una lista con las cuentas de miembros de un gráfico de comportamiento, la entidad principal debe tener permiso para realizar la acción `ListMembers`.
- Para investigar un gráfico de comportamiento, la entidad principal debe tener permiso para realizar la acción `SearchGraph`.

Para llevar a cabo acciones de una cuenta de miembro con la consola de Detective, el usuario o el rol deben tener permiso para realizar la acción `ListInvitations`. Esta acción concede permiso

para ver las invitaciones a gráficos de rendimiento. También pueden obtener permiso para realizar ciertas acciones de cuentas de miembro.

Cómo permitir a los usuarios que vean sus propios permisos

En este ejemplo se muestra cómo se puede crear una política que permita a IAM los usuarios ver las políticas integradas y administradas asociadas a su identidad de usuario. Esta política incluye permisos para completar esta acción en la consola o mediante programación mediante la tecla o. AWS CLI AWS API

```
{
    "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": "*"
        }
    ]
}
```

Cuenta de administrador: administración de cuentas de miembros en un gráfico de comportamiento

Este ejemplo de política está dirigido a los usuarios de cuentas de administrador que tan solo son responsables de administrar las cuentas de miembros incluidas en un gráfico de rendimiento. Asimismo, la política permite al usuario ver información sobre el uso y desactivar Detective. La política no concede permiso para utilizar el gráfico de comportamiento con fines de investigación.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":
["detective:ListMembers","detective:CreateMembers","detective:DeleteMembers","detective:DeleteG
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
  },
  {
    "Effect":"Allow",
    "Action":["detective:CreateGraph","detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Cuenta de administrador: uso de un gráfico de comportamiento con fines de investigación

Este ejemplo de política está dirigido a los usuarios de cuentas de administrador que utilizan el gráfico de comportamiento únicamente con fines de investigación. No pueden ver ni editar la lista con las cuentas de miembros del gráfico de rendimiento.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
    "Action":["detective:SearchGraph"],
    "Resource":"arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899"
   },
   {
```

```
    "Effect":"Allow",
    "Action":["detective:ListGraphs"],
    "Resource":"*"
  }
 ]
}
```

Cuenta de miembro: administración de las invitaciones y suscripciones a gráficos de comportamiento

Este ejemplo de política está dirigido a los usuarios que pertenecen a una cuenta de miembro. En este ejemplo, la cuenta de miembro está incluida en dos gráficos de comportamiento. La política concede permiso para responder a las invitaciones y eliminar la cuenta de miembro del gráfico de comportamiento.

```
{"Version":"2012-10-17",
  "Statement":[
   {
    "Effect":"Allow",
   "Action":
["detective:AcceptInvitation","detective:RejectInvitation","detective:DisassociateMembership"],
   "Resource":[
       "arn:aws:detective:us-
east-1:111122223333:graph:027c7c4610ea4aacaf0b883093cab899",
       "arn:aws:detective:us-
east-1:444455556666:graph:056d2a9521xi2bbluw1d164680eby416"
    ]
  },
  {
    "Effect":"Allow",
    "Action":["detective:ListInvitations"],
    "Resource":"*"
  }
 ]
}
```

Cuenta de administrador: restricción del acceso en función de valores de etiqueta

La siguiente política permite al usuario utilizar un gráfico de comportamiento con fines de investigación si la etiqueta `SecurityDomain` del gráfico de comportamiento coincide con la etiqueta `SecurityDomain` del usuario.

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Allow",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals"{
                "aws:ResourceTag/SecurityDomain": "aws:PrincipalTag/SecurityDomain"
            }
        }
    },
    {
        "Effect":"Allow",
        "Action":["detective:ListGraphs"],
        "Resource":"*"
    } ]
}
```

La siguiente política evita que los usuarios puedan utilizar un gráfico de comportamiento con fines de investigación si el valor de la etiqueta `SecurityDomain` del gráfico de comportamiento es `Finance`.

```
{
    "Version":"2012-10-17",
    "Statement":[ {
        "Effect":"Deny",
        "Action":["detective:SearchGraph"],
        "Resource":"arn:aws:detective:*:*:graph:*",
        "Condition": {
            "StringEquals": {"aws:ResourceTag/SecurityDomain": "Finance"}
        }
    } ]
}
```

AWS políticas gestionadas para Amazon Detective

Una política AWS administrada es una política independiente creada y administrada por AWS. AWS Las políticas administradas están diseñadas para proporcionar permisos para muchos casos de uso comunes, de modo que pueda empezar a asignar permisos a usuarios, grupos y funciones.

Ten en cuenta que es posible que las políticas AWS administradas no otorguen permisos con privilegios mínimos para tus casos de uso específicos, ya que están disponibles para que los usen todos los AWS clientes. Se recomienda definir políticas administradas por el cliente específicas para sus casos de uso a fin de reducir aún más los permisos.

No puedes cambiar los permisos definidos en AWS las políticas administradas. Si AWS actualiza los permisos definidos en una política AWS administrada, la actualización afecta a todas las identidades principales (usuarios, grupos y roles) a las que está asociada la política. AWS es más probable que actualice una política AWS administrada cuando Servicio de AWS se lance una nueva o cuando estén disponibles nuevas operaciones de API para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

AWS política gestionada: AmazonDetectiveFullAccess

Puede adjuntar la política `AmazonDetectiveFullAccess` a sus identidades de IAM.

Esta política otorga permisos administrativos que brindan a una entidad principal acceso completo a todas las acciones de Amazon Detective. También puede adjuntar esta política a una entidad principal antes de que esta habilite Detective en su cuenta. También debe adjuntarse al rol que se utiliza para ejecutar los scripts de Detective Python para crear y administrar un gráfico de comportamiento.

Las entidades principales con estos permisos pueden administrar cuentas de miembro, agregar etiquetas a su gráfico de comportamiento y usar Detective con fines de investigación. También pueden archivar GuardDuty los hallazgos. La política proporciona los permisos que la consola de Detective necesita para mostrar los nombres de las cuentas en las que se encuentran AWS Organizations.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `detective`: permite a las entidades principales obtener acceso completo a todas las acciones de Detective.
- `organizations`: permite a las entidades principales recuperar de AWS Organizations información sobre las cuentas de una organización. Si una cuenta pertenece a una organización,

estos permisos permiten que la consola de Detective muestre los nombres de las cuentas además de los números de cuenta.

- `guardduty`— Permite a los directores obtener y archivar GuardDuty los hallazgos desde Detective.
- `securityhub`: permite a las entidades principales obtener resultados de Security Hub desde Detective.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "detective:*",
                "organizations:DescribeOrganization",
                "organizations:ListAccounts"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:ArchiveFindings"
            ],
            "Resource": "arn:aws:guardduty:*:*:detector/*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "guardduty:GetFindings",
                "guardduty:ListDetectors"

            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                 "securityHub:GetFindings"
            ],
```

```
            "Resource": "*"
        }
    ]
}
```

AWS política gestionada: AmazonDetectiveMemberAccess

También puede adjuntar la política `AmazonDetectiveMemberAccess` a sus entidades de IAM.

Esta política proporciona acceso de miembro a Amazon Detective y acceso limitado a la consola.

Con esta política, puede:

- Ver las invitaciones de pertenencia a gráficos de Detective y aceptar o rechazar dichas invitaciones.
- Ver cómo su actividad en Detective contribuye al costo de uso del servicio en la página Uso.
- Renunciar a su pertenencia a un gráfico.

Esta política otorga permisos de solo lectura que brindan acceso limitado a la consola de Detective.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `detective`: permite a los miembros acceder a Detective.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:AcceptInvitation",
        "detective:BatchGetMembershipDatasources",
        "detective:DisassociateMembership",
```

```
        "detective:GetFreeTrialEligibility",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListInvitations",
        "detective:RejectInvitation"
      ],
      "Resource": "*"
    }
  ]
}
```

Política administrada de AWS : AmazonDetectiveInvestigatorAccess

Puede adjuntar la política `AmazonDetectiveInvestigatorAccess` a sus entidades de IAM.

Esta política proporciona acceso de investigador al servicio de Detective y acceso limitado a las dependencias de la interfaz de usuario de la consola de Detective. Esta política concede permisos para habilitar las investigaciones de Detective en Detective para usuarios y roles de IAM. Puede investigar para identificar los indicadores de riesgo, por ejemplo, resultados, utilizando un informe de investigación que proporciona análisis e información sobre indicadores de seguridad. El informe se clasifica por gravedad, que se determina mediante el análisis de comportamiento y machine learning de Detective. Puede utilizar el informe para priorizar la corrección de los recursos.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `detective`: proporciona a las entidades principales acceso de investigador a las acciones de Detective para habilitar investigaciones de Detective y resumen de grupo de resultados.
- `guardduty`— Permite a los directores obtener y archivar GuardDuty los hallazgos desde Detective.
- `securityhub`: permite a las entidades principales obtener resultados de Security Hub desde Detective.
- `organizations`— Permite a los directores recuperar información sobre las cuentas de una organización desde. AWS Organizations Si una cuenta pertenece a una organización, estos

permisos permiten que la consola de Detective muestre los nombres de las cuentas además de los números de cuenta.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "DetectivePermissions",
      "Effect": "Allow",
      "Action": [
        "detective:BatchGetGraphMemberDatasources",
        "detective:BatchGetMembershipDatasources",
        "detective:DescribeOrganizationConfiguration",
        "detective:GetFreeTrialEligibility",
        "detective:GetGraphIngestState",
        "detective:GetMembers",
        "detective:GetPricingInformation",
        "detective:GetUsageInformation",
        "detective:ListDatasourcePackages",
        "detective:ListGraphs",
        "detective:ListHighDegreeEntities",
        "detective:ListInvitations",
        "detective:ListMembers",
        "detective:ListOrganizationAdminAccount",
        "detective:ListTagsForResource",
        "detective:SearchGraph",
        "detective:StartInvestigation",
        "detective:GetInvestigation",
        "detective:ListInvestigations",
        "detective:UpdateInvestigationState",
        "detective:ListIndicators",
        "detective:InvokeAssistant"
      ],
      "Resource": "*"
    },
    {
      "Sid": "OrganizationsPermissions",
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
```

```
      "Resource": "*"
    },
    {
      "Sid": "GuardDutyPermissions",
      "Effect": "Allow",
      "Action": [
        "guardduty:ArchiveFindings",
        "guardduty:GetFindings",
        "guardduty:ListDetectors"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SecurityHubPermissions",
      "Effect": "Allow",
      "Action": [
        "securityHub:GetFindings"
      ],
      "Resource": "*"
    }
  ]
}
```

AWS política gestionada: AmazonDetectiveOrganizationsAccess

Puede adjuntar la política `AmazonDetectiveOrganizationsAccess` a sus entidades de IAM.

Esta política concede permiso para habilitar y administrar Amazon Detective dentro de una organización. Puede habilitar Detective en toda la organización y determinar la cuenta de administrador delegada para Detective.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `detective`: permite a las entidades principales acceder a las acciones de Detective.
- `iam`: especifica que se cree un rol vinculado a un servicio cuando el Detective llama a `EnableOrganizationAdminAccount`.
- `organizations`— Permite a los directores recuperar información sobre las cuentas de una organización desde AWS Organizations. Si una cuenta pertenece a una organización, estos

permisos permiten que la consola de Detective muestre los nombres de las cuentas además de los números de cuenta. Permite la integración de un AWS servicio, permite registrar y anular el registro de la cuenta de miembro especificada como administrador delegado y permite a los directores recuperar cuentas de administrador delegado en otros servicios de seguridad como Amazon Detective, Amazon, Amazon GuardDuty Macie y. AWS Security Hub

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "detective:DisableOrganizationAdminAccount",
        "detective:EnableOrganizationAdminAccount",
        "detective:ListOrganizationAdminAccount"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateServiceLinkedRole"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "iam:AWSServiceName": "detective.amazonaws.com"
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:EnableAWSServiceAccess",
        "organizations:RegisterDelegatedAdministrator",
        "organizations:DeregisterDelegatedAdministrator"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
```

```
            "detective.amazonaws.com"
          ]
        }
      }
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:DescribeAccount",
        "organizations:DescribeOrganization",
        "organizations:ListAccounts"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "organizations:ListDelegatedAdministrators"
      ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
          "organizations:ServicePrincipal": [
            "detective.amazonaws.com",
            "guardduty.amazonaws.com",
            "macie.amazonaws.com",
            "securityhub.amazonaws.com"
          ]
        }
      }
    }
  ]
}
```

Política administrada de AWS : AmazonDetectiveServiceLinkedRole

No puede adjuntar la política `AmazonDetectiveServiceLinkedRole` a sus entidades de IAM. Esta política está adjunta a un rol vinculado a un servicio que permite a Detective realizar acciones en su nombre. Para obtener más información, consulte the section called “Usar roles vinculados a servicios”.

Esta política concede permisos administrativos que autorizan al rol vinculado al servicio acceder a información sobre las cuentas de una organización.

Detalles de los permisos

Esta política incluye los permisos siguientes:

- `organizations`: recupera la información sobre las cuentas de una organización.

```
{
  "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
              "organizations:DescribeAccount",
              "organizations:ListAccounts"
            ],
            "Resource": "*"
        }
    ]
}
```

Actualizaciones de Detectives de las políticas AWS gestionadas

Vea los detalles sobre las actualizaciones de las políticas AWS administradas para Detective desde que este servicio comenzó a rastrear estos cambios. Para obtener alertas automáticas sobre los cambios realizados en esta página, suscríbase a la fuente RSS en la Página del historial de revisión de .

Cambio	Descripción	Fecha
AmazonDetectiveInvestigatorAccess: actualizaciones de políticas existentes	Se agregaron a la política de `AmazonDetectiveInvestigatorAccess` acciones de resumen de grupos de investigaciones y resultados de Detective.	26 de noviembre de 2023

Cambio	Descripción	Fecha
	Estas acciones permiten iniciar, recuperar y actualizar las investigaciones de Detective y obtener un resumen de grupo de resultados desde Detective.	
AmazonDetectiveFullAccess y AmazonDetectiveInvestigatorAccess: actualizaciones de las políticas existentes	Detective agregó las acciones `GetFindings` de Security Hub a las políticas `AmazonDetectiveFullAccess` y `AmazonDetectiveInvestigatorAccess`. Estas acciones permiten obtener los resultados de Security Hub desde Detective.	16 de mayo de 2023
AmazonDetectiveOrganizationsAccess: política nueva	Detective agregó la política `AmazonDetectiveOrganizationsAccess`. Esta política otorga permiso para habilitar y administrar Detective dentro de una organización.	2 de marzo de 2023
AmazonDetectiveMemberAccess: política nueva	Detective agregó la política `AmazonDetectiveMemberAccess`. Esta política proporciona acceso de miembro a Detective y acceso limitado a las dependencias de la interfaz de usuario de la consola.	17 de enero de 2023

Cambio	Descripción	Fecha
AmazonDetectiveFullAccess: actualizaciones de una política existente	El Detective agregó GuardDuty `GetFindings` acciones a la `AmazonDetectiveFullAccess` política. Estas acciones permiten obtener GuardDuty hallazgos desde el interior de Detective.	17 de enero de 2023
AmazonDetectiveInvestigatorAccess: política nueva	Detective agregó la política `AmazonDetectiveInvestigatorAccess` . Esta política permite a la entidad principal realizar investigaciones en Detective.	17 de enero de 2023
AmazonDetectiveServiceLinkedRole: política nueva	Detective agregó una nueva política para su rol vinculado al servicio. La política permite al rol vinculado al servicio recuperar información sobre las cuentas de una organización.	16 de diciembre de 2021
Detective comenzó a hacer el seguimiento de los cambios	Detective comenzó a rastrear los cambios en sus políticas AWS gestionadas.	10 de mayo de 2021

Usar roles vinculados a servicios para Detective

Amazon Detective utiliza funciones AWS Identity and Access Management vinculadas al servicio (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Detective. Los roles vinculados al servicio están predefinidos por el Detective e incluyen todos los permisos que el servicio requiere para llamar a otros AWS servicios en su nombre.

Un rol vinculado a un servicio simplifica la configuración de Detective al evitar que se tengan que agregar manualmente los permisos necesarios. Detective define los permisos de sus roles vinculados al servicio y, salvo que se defina de otro modo, solo Detective puede asumir sus roles. Los permisos definidos incluyen las políticas de confianza y de permisos, y que la política de permisos no se pueda adjuntar a ninguna otra entidad de IAM.

Solo es posible eliminar un rol vinculado a un servicio después de eliminar sus recursos relacionados. Esto protege sus recursos de Detective, ya que evita que se puedan eliminar accidentalmente permisos de acceso a los recursos.

Para obtener información sobre otros servicios que admiten roles vinculados a servicios, consulte Servicios de AWS que funcionan con IAM y busque los servicios que muestran Sí en la columna Rol vinculado a servicio. Seleccione una opción Sí con un enlace para ver la documentación acerca del rol vinculado al servicio en cuestión.

Permisos de rol vinculado a servicio de Detective

El Detective usa el rol vinculado al servicio denominado AWSServiceRoleForDetective: permite que el Detective acceda a la AWS Organizations información en su nombre.

El rol AWSServiceRoleForDetective vinculado al servicio confía en los siguientes servicios para asumir el rol:

- `detective.amazonaws.com`

El rol AWSServiceRoleForDetective vinculado al servicio usa la política administrada. `AmazonDetectiveServiceLinkedRolePolicy`

Para obtener más información sobre las actualizaciones de la `AmazonDetectiveServiceLinkedRolePolicy` política, consulta Amazon Detective actualiza las políticas AWS gestionadas. Para recibir alertas automáticas sobre los cambios en esta política, suscríbase a la fuente RSS de la página del historial de documentos del Detective.

Debe configurar permisos para permitir a una entidad de IAM (como un usuario, grupo o rol) crear, editar o eliminar un rol vinculado a servicios. Para obtener más información, consulte Permisos de roles vinculados a servicios en la Guía del usuario de IAM.

Crear un rol vinculado a servicio para Detective

No necesita crear manualmente un rol vinculado a un servicio. Cuando designa la cuenta de administrador de Detective para una organización en la AWS Management Console AWS CLI, la o la AWS API, Detective crea el rol vinculado al servicio para usted.

Si elimina este rol vinculado a servicios y necesita crearlo de nuevo, puede utilizar el mismo proceso para volver a crear el rol en su cuenta. Al designar la cuenta de administrador de Detective de una organización, Detective crea el rol vinculado al servicio en su nombre una vez más.

Editar un rol vinculado a servicio para Detective

Detective no le permite editar el rol AWSServiceRoleForDetective vinculado al servicio. Después de crear un rol vinculado al servicio, no podrá cambiar el nombre del rol, ya que varias entidades podrían hacer referencia al rol. Sin embargo, sí puede editar la descripción del rol con IAM. Para obtener más información, consulte Editar un rol vinculado a servicios en la Guía del usuario de IAM.

Eliminar un rol vinculado a un servicio para Detective

Si ya no necesita usar una característica o servicio que requieran un rol vinculado a un servicio, le recomendamos que elimine dicho rol. Así no tendrá una entidad no utilizada que no se monitorice ni mantenga de forma activa. Sin embargo, debe limpiar los recursos de su rol vinculado al servicio antes de eliminarlo manualmente.

> **Note**
>
> Si el servicio Detective está utilizando el rol mientras usted intenta eliminar los recursos, la eliminación podría fallar. Si esto sucede, espere unos minutos y reintente la operación.

Para eliminar los recursos de Detective utilizados por el AWSServiceRoleForDetective

1. Elimine la cuenta de administrador de Detective. Consulte the section called “Designación de la cuenta de administrador de Detective”.
2. Repita el proceso en cada región en la que haya designado la cuenta de administrador de Detective.

Para eliminar manualmente el rol vinculado al servicio con IAM

Utilice la consola de IAM AWS CLI, la o la AWS API para eliminar la función vinculada al AWSServiceRoleForDetective servicio. Para obtener más información, consulte Eliminar un rol vinculado a un servicio en la Guía del usuario de IAM.

Regiones admitidas para los roles vinculados a servicios de Detective

Detective admite el uso de roles vinculados a servicios en todas las regiones en las que el servicio está disponible. Para obtener más información, consulte Regiones y puntos de conexión de AWS.

Solución de problemas de identidad y acceso de Amazon Detective

Utilice la siguiente información para ayudarle a diagnosticar y solucionar problemas comunes que pueden surgir al trabajar con Detective yIAM. Si encuentra problemas de acceso denegado o dificultades similares al trabajar con AWS Identity and Access Management(IAM), consulte los IAM temas de solución de problemas de la Guía del IAM usuario.

No tengo autorización para realizar una acción en Detective

Si AWS Management Console le indica que no está autorizado a realizar una acción, debe ponerse en contacto con el administrador para obtener ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

El siguiente ejemplo de error se produce cuando el `mateojackson` IAM usuario intenta usar la consola para aceptar una invitación para convertirse en miembro de la cuenta de un gráfico de comportamiento, pero no tiene `detective:AcceptInvitation` permisos.

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to
 perform: detective:AcceptInvitation on resource: arn:aws:detective:us-
east-1:444455556666:graph:567856785678
```

En este caso, Mateo pide a su administrador que actualice sus políticas de forma que pueda obtener acceso al recurso `arn:aws:detective:us-east-1:444455556666:graph:567856785678` mediante la acción `detective:AcceptInvitation`.

No estoy autorizado a realizar iam: PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Detective.

Algunas Servicios de AWS permiten transferir una función existente a ese servicio en lugar de crear una nueva función de servicio o una función vinculada a un servicio. Para ello, debe tener permisos para transferir el rol al servicio.

El siguiente ejemplo de error se produce cuando un IAM usuario llamado `marymajor` intenta usar la consola para realizar una acción en Detective. 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 AWS administrador. El gestionador es la persona que le proporcionó las credenciales de inicio de sesión.

Quiero permitir que personas ajenas a mi AWS cuenta accedan a mis recursos de Detective

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 admiten políticas basadas en recursos o listas de control de acceso (ACLs), puedes usar esas políticas para permitir que las personas accedan a tus recursos.

Para obtener más información, consulte lo siguiente:

- Para obtener información acerca de si Detective admite estas características, consulte Cómo funciona Amazon Detective con IAM.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a través de los Cuentas de AWS que eres propietario, consulta Cómo proporcionar acceso a un IAM usuario en otro de tu Cuenta de AWS propiedad en la Guía del IAMusuario.
- Para obtener información sobre cómo proporcionar acceso a tus recursos a terceros Cuentas de AWS, consulta Cómo permitir el acceso a recursos que Cuentas de AWS son propiedad de terceros en la Guía del IAM usuario.
- Para obtener información sobre cómo proporcionar acceso mediante la federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del IAM usuario.

- Para saber la diferencia entre el uso de roles y políticas basadas en recursos para el acceso entre cuentas, consulte el acceso a recursos entre cuentas IAM en la Guía del usuario. IAM

Validación de conformidad para Amazon Detective

Amazon Detective forma parte del programa AWS de garantía. Para obtener más información, consulte Health Information Trust Alliance Common Security Framework (HITRUST) CSF .

Para obtener una lista de AWS los servicios incluidos en el ámbito de los programas de cumplimiento específicos, consulte AWSServicios incluidos en el ámbito de aplicación por programa de conformidad y . Para obtener información general, consulte Programas de AWS cumplimiento > Programas AWS .

Puede descargar informes de auditoría de terceros utilizando AWS Artifact. Para obtener más información, consulte Descarga de informes en AWS Artifact .

AWS proporciona los siguientes recursos para ayudar a garantizar el cumplimiento:

- Guías de inicio rápido sobre sobre seguridad y cumplimiento: las guías sobre seguridad y cumplimiento abordan las consideraciones arquitectónicas y proporcionan los pasos para implementar entornos básicos centrados en la seguridad y el cumplimiento AWS.
- Evaluación de los recursos con las reglas de la guía para AWS Config desarrolladores: el AWS Config servicio evalúa en qué medida las configuraciones de sus recursos cumplen con las prácticas internas, las directrices del sector y las normas.
- AWS Security Hub— Este AWS servicio proporciona una visión integral del estado de su seguridad AWS que le ayuda a comprobar su conformidad con los estándares y las mejores prácticas del sector de la seguridad.

Resiliencia de Amazon Detective

La infraestructura AWS global se basa en AWS regiones y zonas de disponibilidad. AWS Las regiones proporcionan varias zonas de disponibilidad aisladas y separadas físicamente, que están conectadas mediante redes de baja latencia, alto rendimiento y alta redundancia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que realizan una conmutación por error automática entre las zonas sin interrupciones. 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 AWS las regiones y las zonas de disponibilidad, consulte Infraestructura global.AWS

Además de la infraestructura AWS global, Detective utiliza la resiliencia integrada en Amazon DynamoDB y Amazon Simple Storage Service (Amazon S3). Para obtener más información, consulte Resiliencia y recuperación ante desastres en Amazon DynamoDB y Resiliencia en Amazon Simple Storage Service.

La arquitectura de Detective también es resistente a los fallos de una única zona de disponibilidad. Esta resiliencia está integrada en Detective y no requiere ninguna configuración.

Seguridad de la infraestructura en Amazon Detective

Como servicio gestionado, Amazon Detective; está protegido por la seguridad de la red AWS global. Para obtener información sobre los servicios AWS de seguridad y cómo se AWS protege la infraestructura, consulte Seguridad AWS en la nube. Para diseñar su AWS entorno utilizando las mejores prácticas de seguridad de la infraestructura, consulte Protección de infraestructuras en un marco de buena AWS arquitectura basado en el pilar de la seguridad.

Utiliza las API llamadas AWS publicadas para acceder a Detective; a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Necesitamos TLS 1.2 y recomendamos TLS 1.3.
- Cifre suites con perfecto secreto (PFS), como (Ephemeral Diffie-Hellman) o DHE ECDHE (Elliptic Curve Ephemeral Diffie-Hellman). La mayoría de los sistemas modernos como Java 7 y posteriores son compatibles con estos modos.

Además, las solicitudes deben firmarse con un identificador de clave de acceso y una clave de acceso secreta que esté asociada a un director. IAM También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

Mejores prácticas de seguridad para Detectives

Detective proporciona un número de características de seguridad que debe tener en cuenta a la hora de desarrollar e implementar sus propias políticas de seguridad. Las siguientes prácticas recomendadas son directrices generales y no constituyen una solución de seguridad completa. Puesto que es posible que estas prácticas recomendadas no sean adecuadas o suficientes para el entorno, considérelas como consideraciones útiles en lugar de como normas.

En el caso de Detective, las prácticas recomendadas de seguridad están relacionadas con la administración de cuentas en un gráfico de comportamiento.

Mejores prácticas para las cuentas de administrador de Detectives

Cuando añada cuentas de miembros a su gráfico de comportamiento de Detective, invite únicamente a las cuentas que usted supervise.

Limite el acceso al gráfico de comportamiento. Los usuarios con la AmazonDetectiveFullAccesspolítica pueden conceder acceso a todas las acciones de los Detectives. Las entidades principales con estos permisos pueden administrar cuentas de miembro, agregar etiquetas a su gráfico de comportamiento y usar Detective con fines de investigación. Cuando un usuario obtiene acceso a un gráfico de comportamiento, puede ver todos los resultados de las cuentas de miembros. En estos resultados puede mostrarse información de seguridad confidencial.

Prácticas recomendadas para cuentas de miembros

Si recibe una invitación a un gráfico de comportamiento, asegúrese de validar el origen de la invitación.

Compruebe el AWS identificador de la cuenta de administrador que envió la invitación. Verifique que conoce a quién pertenece la cuenta y si la cuenta que ha enviado la invitación tiene un interés legítimo para supervisar sus datos de seguridad.

Registrar API llamadas de Amazon Detective con AWS CloudTrail

Detective está integrado con AWS CloudTrail un servicio que proporciona un registro de las acciones realizadas por un usuario, un rol o un AWS servicio de Detective. CloudTrail captura todas las API llamadas de Detective como eventos. Las llamadas capturadas incluyen llamadas desde la consola de Detectives y llamadas en código a las API operaciones de Detective.

- Si crea una ruta, puede habilitar la entrega continua de CloudTrail eventos a un bucket de Amazon S3, incluidos los eventos para Detective.
- Si no configura una ruta, podrá ver los eventos más recientes en la CloudTrail consola, en el historial de eventos.

Con la información recopilada por CloudTrail, puedes determinar lo siguiente:

- La solicitud que se realizó a Detective
- La dirección IP desde la que se realizó la solicitud
- Quién realizó la solicitud
- Cuando se realizó
- Detalles adicionales sobre la solicitud

Para obtener más información CloudTrail, consulte la Guía AWS CloudTrail del usuario.

Información de Detectives en CloudTrail

CloudTrail está habilitada en tu AWS cuenta al crearla. Cuando se produce una actividad en Detective, esa actividad se registra en un CloudTrail evento, junto con otros eventos de AWS servicio, en el historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS . Para obtener más información, consulte Visualización de eventos con el historial de CloudTrail eventos.

Para tener un registro continuo de los eventos de tu AWS cuenta, incluidos los eventos de Detective, crea un registro. Un rastro permite CloudTrail entregar archivos de registro a un bucket de Amazon S3.

De manera predeterminada, cuando se crea un registro de seguimiento en la consola, el registro de seguimiento se aplica a todas las regiones de AWS . La ruta registra los eventos de todas las regiones de la AWS partición y envía los archivos de registro al bucket de Amazon S3 que especifique. También puede configurar otros AWS servicios para analizar más a fondo los datos de eventos recopilados en los CloudTrail registros y actuar en función de ellos.

Para más información, consulte los siguientes temas:

- Introducción a la creación de registros de seguimiento
- CloudTrail Servicios e integraciones compatibles
- Configuración de Amazon SNS Notifications para CloudTrail
- Recibir archivos de CloudTrail registro de varias regiones y recibir archivos de CloudTrail registro de varias cuentas

CloudTrail registra todas las operaciones de los Detectives, que están documentadas en la APIReferencia de Detectives.

Por ejemplo, las llamadas a las `CreateMembers` `DeleteMembers` operaciones y las operaciones generan entradas en los archivos de CloudTrail registro. `AcceptInvitation`

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario lo ayuda a determinar lo siguiente:

- Si la solicitud se realizó con credenciales de usuario root o AWS Identity and Access Management (IAM)
- Si la solicitud se realizó con credenciales de seguridad temporales de un rol o un usuario federado
- Si la solicitud la realizó otro AWS servicio

Para obtener más información, consulte el CloudTrail userIdentityElemento.

Comprensión de las entradas del archivo de registro de Detective

Un rastro es una configuración que permite la entrega de eventos como archivos de registro a un bucket de Amazon S3 que usted especifique. CloudTrail Los archivos de registro contienen una o más entradas de registro.

Un evento representa una única solicitud desde cualquier origen. Los eventos incluyen información sobre la acción solicitada, la fecha y la hora de la acción, los parámetros de la solicitud, etc. CloudTrail Los archivos de registro no son un registro ordenado de las API llamadas públicas, por lo que las entradas no aparecen en ningún orden específico.

El siguiente ejemplo muestra una entrada de CloudTrail registro que demuestra la `AcceptInvitation` acción.


```
      {
            "EventId": "f2545ee3-170f-4340-8af4-a983c669ce37",
            "Username": "JaneRoe",
            "EventTime": 1571956406.0,
            "CloudTrailEvent": "{\"eventVersion\":\"1.05\",\"userIdentity\":
{\"type\":\"AssumedRole\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS:JaneRoe\",\"arn
\":\"arn:aws:sts::111122223333:assumed-role/1A4R5SKSPGG9V/JaneRoe\",\"accountId
\":\"111122223333\",\"accessKeyId\":\"AKIAIOSFODNN7EXAMPLE\",\"sessionContext\":
{\"attributes\":{\"mfaAuthenticated\":\"false\",\"creationDate\":\"2019-10-24T21:54:56Z
\"},\"sessionIssuer\":{\"type\":\"Role\",\"principalId\":\"AROAJZARKEP6WKJ5JHSUS
\",\"arn\":\"arn:aws:iam::111122223333:role/1A4R5SKSPGG9V\",\"accountId\":
\"111122223333\",\"userName\":\"JaneRoe\"}}},\"eventTime\":\"2019-10-24T22:33:26Z
\",\"eventSource\":\"detective.amazonaws.com\",\"eventName\":\"AcceptInvitation
\",\"awsRegion\":\"us-east-2\",\"sourceIPAddress\":\"192.0.2.123\",\"userAgent
\":\"aws /3 aws-sdk-java/1.11.648 Linux/4.14.133-97.112.amzn2.x86_64 OpenJDK_64-
Bit_Server_VM/25.201-b09 java/1.8.0_201 vendor/Oracle_Corporation exec-env/
AWS_Lambda_java8\",\"errorCode\":\"ValidationException\",\"requestParameters\":
{\"masterAccount\":\"111111111111\"},\"responseElements\":{\"message\":\"Invalid
 request body\"},\"requestID\":\"8437ff99-5ec4-4b1a-8353-173be984301f\",\"eventID\":
\"f2545ee3-170f-4340-8af4-a983c669ce37\",\"readOnly\":false,\"eventType\":\"AwsApiCall
\",\"recipientAccountId\":\"111122223333\"}",
            "EventName": "AcceptInvitation",
            "EventSource": "detective.amazonaws.com",
            "Resources": []
        },
```

Regiones y cuotas de Amazon Detective

Tenga en cuenta las siguientes cuotas cuando utilice Amazon Detective.

Regiones y puntos de conexión de Detectives

Para ver la lista de Regiones de AWS lugares donde Detective está disponible, consulte Puntos finales del servicio de Detective.

Cuotas de Detective

Detective cuenta con las siguientes cuotas, que no se pueden configurar.

Recurso	Cuota	Comentarios
Número de cuentas de miembros	1200	El número de cuentas de miembros que una cuenta de administrador puede agregar a un gráfico de comportamiento.
Volumen de datos del gráfico de comportamiento: advertencia de volumen	9 TB al día	Si el volumen de datos de un gráfico de comportamiento supera los 9 TB al día, Detective muestra una advertencia para avisar de que el gráfico de comportamiento se acerca al volumen máximo permitido.
Volumen de datos del gráfico de comportamiento: no se permiten nuevas cuentas	10 TB al día	Si el volumen de datos de un gráfico de comportamiento supera los 10 TB al día, no puede agregar nuevas cuentas de miembros al gráfico de comportamiento.
Volumen de datos del gráfico de comportamiento: detiene la ingesta de datos en el gráfico de comportamiento	15 TB al día	Si el volumen de datos de un gráfico de comportamiento supera los 15 TB al día, Detective deja de introducir datos en el gráfico de comportamiento.

Recurso	Cuota	Comentarios
		El límite de 15 TB al día refleja tanto el volumen de datos habitual como los picos de volumen de datos. Para volver a habilitar la ingesta de datos, debe ponerse en contacto con Soporte.

Internet Explorer 11 no compatible

No puede utilizar Detective con Internet Explorer 11.

Administrar etiquetas de un gráfico de comportamiento

Una etiqueta es una etiqueta opcional que puede definir y asignar a AWS los recursos, incluidos ciertos tipos de recursos de Detective. Las etiquetas pueden ayudarle a identificar, clasificar y administrar recursos de distintas formas, como por finalidad, propietario, entorno u otros criterios. Por ejemplo, puede usar etiquetas para aplicar políticas, asignar costos, distinguir entre las versiones de los recursos o identificar los recursos que respaldan determinados requisitos de conformidad o flujos de trabajo.

Puede asignar etiquetas a su gráfico de comportamiento. A continuación, puede utilizar los valores de las etiquetas en IAM las políticas para gestionar el acceso a las funciones de los gráficos de comportamiento en Detective. Consulte the section called “Autorización basada en etiquetas de gráficos de comportamiento de Detective”.

También puede usar las etiquetas como herramienta de informes de costos. Por ejemplo, para hacer un seguimiento de los costes asociados a la seguridad, puedes asignar la misma etiqueta a tu gráfico de comportamiento de Detective, a tu recurso AWS Security Hub central y a los GuardDuty detectores de Amazon. Luego AWS Cost Explorer, puede buscar esa etiqueta para ver una vista consolidada de los costos de esos recursos.

Visualización de las etiquetas de un gráfico de comportamiento

Puede administrar las etiquetas de su gráfico de comportamiento desde la página General.

Console

Para ver la lista de etiquetas asignadas al gráfico de comportamiento

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, en Configuración, seleccione General.

Detective API, AWS CLI

Puede usar el Detective API o el AWS Command Line Interface para obtener la lista de etiquetas para su gráfico de comportamiento.

Para obtener la lista de etiquetas de un gráfico de comportamiento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `ListTagsForResource`operación. Debe proporcionar el gráfico ARN de su comportamiento.
- AWS CLI:: en la línea de comandos, ejecute el comando `list-tags-for-resource`.

```
aws detective list-tags-for-resource --resource-arn <behavior graph ARN>
```

Ejemplo

```
aws detective list-tags-for-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Añadir etiquetas a un gráfico de comportamiento

Console

Desde la lista de etiquetas de la página General, puede añadir valores de etiquetas al gráfico de comportamiento.

Para añadir una etiqueta al gráfico de comportamiento

1. Elija Añadir nueva etiqueta.
2. En Clave, escriba el nombre de la etiqueta.
3. En Valor, escriba el valor de la etiqueta.

Detective API, AWS CLI

Puede utilizar el Detective API o el AWS CLI para añadir valores de etiqueta a su gráfico de comportamiento.

Para añadir etiquetas a un gráfico de comportamiento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `TagResource`operación. Usted proporciona el gráfico de comportamiento ARN y los valores de las etiquetas que desea añadir.
- AWS CLI: en la línea de comandos, ejecute el comando `tag-resource`.

```
aws-detective tag-resource --aws detective tag-resource --resource-arn <behavior
 graph ARN> --tags '{"TagName":"TagValue"}'
```

Ejemplo

```
aws detective tag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tags '{"Department":"Finance"}'
```

Eliminar etiquetas de un gráfico de comportamiento

Console

Para eliminar una etiqueta de la lista de la página General, elija la opción Eliminar para esa etiqueta.

Detective API, AWS CLI

Puede utilizar el Detective API o el AWS CLI para eliminar los valores de las etiquetas de su gráfico de comportamiento.

Para eliminar etiquetas de un gráfico de comportamiento (DetectiveAPI, AWS CLI)

- DetectiveAPI: Utilice la `UntagResource`operación. Usted proporciona el gráfico ARN de comportamiento y los nombres de las etiquetas que se van a eliminar.
- AWS CLI: en la línea de comandos, ejecute el comando `untag-resource`.

```
aws detective untag-resource --resource-arn <behavior graph ARN> --tag-keys
 "TagName"
```

Ejemplo

```
aws detective untag-resource --resource-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234 --tag-keys "Department"
```

Deshabilitación de Amazon Detective

La cuenta de administrador de un gráfico de rendimiento puede deshabilitar Amazon Detective desde la consola de Detective, la API de Detective o AWS Command Line Interface. Al deshabilitar Detective, se eliminan el gráfico de rendimiento y los datos de Detective asociados a este.

Cuando se elimina un gráfico de comportamiento, no se puede restaurar.

Contenido

- Deshabilitación de Detective (consola)
- Desactivar Detective (API de Detective), AWS CLI
- Desactivación de Detective en todas las regiones (secuencia de comandos de Python activada GitHub)

Deshabilitación de Detective (consola)

Puede deshabilitar Amazon Detective desde la AWS Management Console.

Para deshabilitar Amazon Detective (consola)

1. Abra la consola de Amazon Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación de Detective, vaya a Configuración y elija General.
3. En la página General, en Desactivar Amazon Detective, selecciona Desactivar Amazon Detective.
4. Cuando se le pida confirmación, escriba **`disable`**.
5. Selecciona Desactivar Amazon Detective.

Desactivar Detective (API de Detective), AWS CLI

Puede deshabilitar Amazon Detective desde la API de Detective o la AWS Command Line Interface. Para obtener el ARN del gráfico de comportamiento que se utilizará en la solicitud, utilice la operación `ListGraphs`.

Para deshabilitar Detective (API de Detective AWS CLI),

- API de Detective: utilice la operación `DeleteGraph`. Debe proporcionar el ARN del gráfico.

- AWS CLI: en la línea de comandos, ejecute el comando `delete-graph`.

```
aws detective delete-graph --graph-arn <graph ARN>
```

Ejemplo:

```
aws detective delete-graph --graph-arn arn:aws:detective:us-
east-1:111122223333:graph:123412341234
```

Desactivación de Detective en todas las regiones (secuencia de comandos de Python activada GitHub)

Detective proporciona un script de código abierto GitHub que le permite deshabilitar Detective para una cuenta de administrador en una lista específica de regiones.

Para obtener información sobre cómo configurar y utilizar los GitHub scripts, consultethe section called “Secuencias de comandos Python de Amazon Detective”.

Historial de revisión de la Guía del usuario de Detective

En la siguiente tabla se describen los cambios importantes que se han realizado en la documentación desde la versión más reciente de Detective. Para recibir notificaciones sobre los cambios en esta documentación, puede suscribirse a una fuente RSS.

- Última actualización de la documentación: 20 de febrero de 2025

Cambio	Descripción	Fecha
Se agregó soporte para los hallazgos de secuencias de GuardDuty ataques de Amazon	Detective agregó soporte para encontrar los tipos asociados con la detección GuardDuty extendida de amenazas. GuardDutydetecta una secuencia de ataque cuando una secuencia específica de múltiples acciones, como las actividades de la API y la detección de GuardDuty hallazgos, se alinea con una actividad potencialmente sospechosa. Para obtener información sobre la detección extendida de amenazas y los tipos de búsqueda de secuencias de ataques, consulte Detección extendida de amenazas en la Guía del GuardDuty usuario de Amazon.	20 de febrero de 2025
Se agregó soporte para la búsqueda de Amazon GuardDuty IAM	Detective ha añadido compatibilidad con un nuevo tipo de GuardDuty búsqueda que le avisa cuando se utilizan	4 de febrero de 2025

	credenciales de usuario restringidas, creadas para los que aparecen Cuentas de AWS en su entorno, para realizar solicitudes Servicios de AWS. Para obtener más información, consulte Policy:IAMUser/ShortTermRootCredentialUsageen la Guía del GuardDuty usuario de Amazon.	
Nueva característica	Se agregó un diseño de línea de tiempo a la visualización del grupo Detective Finding. Se introdujo la funcionalidad del botón de reproducción y el filtrado de los hallazgos basado en la gravedad. Estas mejoras pueden ayudarlo a comprender mejor la progresión de los eventos, priorizar los problemas críticos y llevar a cabo investigaciones de seguridad más eficientes.	27 de diciembre de 2024

Se agregó soporte para los GuardDuty hallazgos de Amazon	Detective agregó soporte para los siguientes tres tipos de GuardDuty búsqueda que le notifican cuando se ejecutan comandos sospechosos en una carga de trabajo de contenedor o EC2 instancia de Amazon dentro de su AWS entorno: • Discovery:Runtime/SuspiciousCommand • Persistence:Runtime/SuspiciousCommand • PrivilegeEscalation:Runtime/SuspiciousCommand	6 de noviembre de 2024
Se agregó soporte para los GuardDuty hallazgos de Amazon	Detective ahora admite los siguientes tipos de búsqueda GuardDuty de Runtime Monitoring. • `Execution:Runtime/SuspiciousShell` • `PriviliegeEscalation:Runtime/ElevationToRoot`	27 de agosto de 2024

Se agregó soporte para los GuardDuty hallazgos de Amazon	Detective ahora ofrece soporte para la protección contra GuardDuty malware para S3. Esto le ayuda a escanear los objetos recién cargados a los buckets de Amazon S3 para detectar posibles cargas sospechosas y malware, y tomar medidas para aislarlos antes de que se incorporen a los procesos posteriores.	9 de julio de 2024
Funcionalidad actualizada	Detective agregó un nuevo diseño radial al panel de visualización del grupo de búsqueda para proporcionar una visualización mejorada y facilitar la interpretación de los datos.	26 de junio de 2024
Nuevas versiones fuente de Security Lake	Además de la versión de origen 1 (OCSF 1.0.0-rc.2), Detective ahora ingiere datos de la versión de origen 2 (OCSF 1.1.0) para las fuentes de Security Lake compatibles con Detective.	15 de mayo de 2024
Nueva fuente de registro de Security Lake	Puede utilizar la integración de Detective con Security Lake para recopilar registros y eventos de los registros de auditoría de Amazon EKS.	15 de mayo de 2024

Actualización de la documentación	El contenido de la Guía de administración de Amazon Detective ahora está consolidado en la Guía del usuario de Amazon Detective. El soporte estándar de Amazon Detective Administration Guide finalizará el 8 de mayo de 2024.	15 de abril de 2024
Se agregó soporte para los GuardDuty hallazgos de Amazon	Detective ahora admite los siguientes tipos de búsqueda GuardDuty de Runtime Monitoring. • `Execution:Runtime/MaliciousFileExecuted` • `Execution:Runtime/SuspiciousTool` • `DefenseEvasion:Runtime/PtraceAntiDebugging` • `Execution:Runtime/SuspiciousCommand` • `DefenseEvasion:Runtime/SuspiciousCommand`	5 de abril de 2024
Se ha eliminado el requisito de GuardDuty ser miembro de Amazon	Ya no es necesario que seas GuardDuty cliente para activar Amazon Detective. Se ha eliminado el requisito de tener GuardDuty activado Detective en tu cuenta durante 48 horas antes de activar Detective.	2 de febrero de 2024

Se agregó soporte para los GuardDuty hallazgos de Amazon	Detective amplía el soporte para los tipos de búsqueda de GuardDuty EC2 Runtime Monitoring a ECS y EC2 recursos.	30 de enero de 2024
Funcionalidad actualizada	Ahora puedes llevar a cabo una investigación de Detectives desde la página de Investigaciones para encontrar un recurso específico que desees investigar. Detective recomienda recursos en función de su actividad en resultados y grupos de resultados. Detective Investigations le permite investigar a los usuarios de IAM y las funciones de IAM con indicadores de compromiso, lo que puede ayudarle a determinar si un recurso está implicado en un incidente de seguridad.	16 de enero de 2024

Funcionalidad actualizada	Ahora puede ejecutar una investigación de Detective desde la página Investigaciones sobre un recurso recomendado. Detective recomienda recursos en función de su actividad en resultados y grupos de resultados. Detective Investigations le permite investigar a los usuarios y las funciones de IAM con indicadores de compromiso, lo que puede ayudarle a determinar si un recurso está implicado en un incidente de seguridad.	26 de diciembre de 2023
Cambios en la forma en que el Detective lee el flujo de tráfico compartido VPCs	Si utiliza una VPC de Amazon compartida, es posible que vea cambios en el tráfico monitorizado por Detective. Le recomendamos que revise los cambios en Detalles de actividad de Volumen total de llamadas a la API para comprender los posibles efectos en su cobertura y que revise Cómo calcula Amazon Detective el costo previsto para comprender cómo pueden afectar a sus costos de servicio.	20 de diciembre de 2023

Disponibilidad regional	Se han añadido las regiones de Europa (Estocolmo), Europa (París) y Canadá (Central) a la lista AWS de regiones en las que está disponible la integración de Detective con Security Lake.	8 de diciembre de 2023
Nueva característica	Las investigaciones de Detective ayudan a investiga r usuarios y roles de IAM con indicadores de riesgo, que pueden servir para determina r si un recurso está implicado en un incidente de seguridad.	26 de noviembre de 2023
Nueva característica	De forma predeterminada, Detective genera automátic amente resúmenes de grupos de resultados para grupos de resultados con tecnología de inteligencia artificial generativ a (IA generativa). El resumen de grupo de resultados analiza rápidamente las relaciones entre resultados y recursos afectados y, a continuación, resume las posibles amenazas en lenguaje natural.	26 de noviembre de 2023

Nueva característica	La integración de Detective con Security Lake permite consultar y recuperar datos de registros sin procesar almacenados por Security Lake. Con esta integración, puede recopilar registros y eventos de eventos de CloudTrail administración y registros de flujo de Amazon Virtual Private Cloud (Amazon VPC).	26 de noviembre de 2023
Información sobre políticas administradas agregada al capítulo de seguridad	Se agregaron a la política de `AmazonDetectiveInvestigatorAccess` acciones de resumen de grupos de investigaciones y resultados de Detective.	26 de noviembre de 2023
Ver la descripción general de un resultado	Si un resultado está relacionado con una actividad más amplia, Detective le invita a Ir al grupo de resultados.	18 de septiembre de 2023
Puntos de conexión y cuotas de Amazon Detective	Detective ya está disponible en la región de Israel (Tel Aviv).	25 de agosto de 2023
Visualización mejorada de grupos de resultados	La visualización de grupos de resultados de Detective ahora incluye grupos de resultados con resultados agregados, lo que agiliza el análisis de pruebas, entidades y resultados relacionados.	8 de agosto de 2023

Grupos de resultados mejorados	Los grupos de resultados ahora incluyen los resultado s de vulnerabilidades de Amazon Inspector.	13 de junio de 2023
Se agregó compatibilidad con Amazon GuardDuty Lambda Protection	Detective ahora ofrece soporte para GuardDuty Lambda Protection.	26 de mayo de 2023
Se agregaron hallazgos de AWS seguridad como un nuevo paquete de fuente de datos opcional.	Detective ahora proporcio na los hallazgos AWS de seguridad como un paquete de fuente de datos opcional. Este paquete de origen de datos opcional permite a Detective ingerir datos de Security Hub y agregarlos a un gráfico de comportamiento.	16 de mayo de 2023
Se agregó compatibilidad con los tipos de búsqueda de Amazon GuardDuty EKS Runtime Monitoring	Detective ahora admite los tipos de búsqueda de GuardDuty EKS Runtime Monitoring.	3 de mayo de 2023
Se agregó compatibilidad con los tipos de búsqueda GuardDuty de Amazon RDS Protection	Detective ahora admite los tipos de búsqueda GuardDuty de RDS Protection.	20 de abril de 2023

Se agregó soporte para tipos de GuardDuty búsqueda adicionales de Amazon	Detective ahora proporcio na perfiles para los siguiente s tipos de GuardDuty hallazgos adicionales: `DefenseEvasion: EC2UnusualDNSResol ver` `DefenseEvasion: EvasionEC2UnusualD oHActivity` `DefenseEv asion: DefenseEv asionEC2UnusualDoT Activity`	12 de abril de 2023
Se agregaron nuevos paneles a la consola de Detective para ayudar a los usuarios a seleccionar la política administrada de AWS adecuada a su caso de uso específico.	Detective ofrece políticas administradas para que pueda elegir de forma segura los permisos que necesita.	3 de abril de 2023
Ver el tráfico de flujo de VPC para los clústeres de EKS	Se ha añadido una nueva sección para el tráfico de flujo de Amazon Virtual Private Cloud (Amazon VPC) con clústeres de Amazon Elastic Kubernetes Service (Amazon EKS).	2 de marzo de 2023
El grupo de resultados ahora incluye una representación visual dinámica del gráfico de comportamiento de Detective	El grupo de resultados de Detective ahora incluye una representación visual dinámica del gráfico de comportamiento de Detective para enfatizar la relación entre las entidades y los resultados dentro del grupo de resultados.	28 de febrero de 2023

Exporte datos desde la página Resumen y la página de resultados de búsqueda de Detective. Los datos se exportan en formato CSV (valores separados por comas).	Detective ahora le ofrece la opción de exportar datos a su navegador desde la consola de Detective.	7 de febrero de 2023
Se ha añadido un volumen total de flujo de la VPC para las cargas de trabajo de EKS y Amazon EKS	Detective ahora añade resúmenes visuales y análisis sobre los registros de flujo de Amazon Virtual Private Cloud (VPC) de las cargas de trabajo de Amazon Elastic Kubernetes Service (Amazon EKS).	19 de enero de 2023
Información sobre políticas administradas agregada al capítulo de seguridad	El Detective ahora apoya las acciones de GuardDuty obtención de hallazgos a través de la AmazonDetectiveFullAccess política. El capítulo de seguridad ahora proporciona detalles sobre las siguientes nuevas políticas gestionadas para Detective : AmazonDetectiveMemberAccess y AmazonDetectiveInvestigatorAccess.	17 de enero de 2023
Retención de datos agregada	Con Detective, puede acceder a un historial de datos de eventos que se remonta a un año.	20 de diciembre de 2022

Se ha añadido la opción de ajustar el rango temporal en la página de resumen.	Detective ahora ofrece la opción de ajustar el rango temporal para ver la actividad de cualquier periodo de 24 horas comprendido en los 365 días anteriores.	5 de octubre de 2022
Buscar un resultado o entidad	Detective ahora ofrece una búsqueda que no distingue entre mayúsculas y minúscula s.	3 de octubre de 2022
Se ha añadido la capacidad de establecer la marca de rango temporal	Detective ahora proporcio na una forma de configurar la preferencia de formato de la marca de rango temporal. Esta preferencia se aplicará a todas las marcas temporales en Detective.	3 de octubre de 2022
Términos relacionados con los grupos de resultados agregados	Ahora, Detective admite grupos de resultados que conectan los resultados relacionados entre sí en una única pantalla para que pueda investigar posibles actividad es malintencionadas en su entorno. Desde el perfil de un grupo de resultados, puede acceder a los perfiles de entidades y a descripciones generales de los resultados relacionados con este grupo.	3 de agosto de 2022

Se han añadido nuevos perfiles asociados a registros de auditoría de Amazon EKS	Detective ahora proporciona perfiles que le permiten investigar la actividad asociada a las siguientes entidades relacionadas con contenedores: clústeres de Amazon EKS, imágenes de contenedor, pods de Kubernetes y sujetos de Kubernetes.	26 de julio de 2022
Nuevo origen de datos opcional agregado	Ahora, Detective admite registros de auditoría de EKS como un paquete de origen de datos opcional. Una cuenta de administrador puede habilitar este nuevo origen de datos para un gráfico de comportamiento. Los gráficos que se creen a partir de esta fecha tendrán este origen de datos habilitado de forma predeterminada. Los administradores pueden deshabilitar este origen de datos manualmente en cualquier momento.	26 de julio de 2022

Nuevo rol vinculado a servicios y nueva política administrada para Detective	Detective ahora cuenta con un rol vinculado a servicios, `AWSServiceRoleForDetective` . Este rol vinculado a servicios se utiliza para acceder a datos de Organizations en nombre del usuario. El rol utiliza una nueva política administrada, `AmazonDetectiveServiceLinkedRolePolicy` .	16 de diciembre de 2021
Se agregó la integración con AWS Organizations	Detective ahora está integrado con Organizations. La cuenta de administración de la organización designa una cuenta de administrador de Detective para la organización. La cuenta de administración de Detective puede ver todas las cuentas de la organización y habilitarlas como cuentas de miembros en el gráfico de comportamiento de la organización.	16 de diciembre de 2021

Se han sustituido los perfiles de resultado por la descripción general de los resultados	Los perfiles de resultado contenían visualizaciones que analizaban la actividad del recurso implicado. La nueva descripción general de los hallazgos contiene los detalles de búsqueda GuardDuty obtenidos y una lista de las entidades involucradas. Desde la descripción general del resultado, puede pasar a los perfiles de las entidades relacionadas.	20 de septiembre de 2021
Se ha eliminado el límite de los tipos de GuardDuty búsqueda admitidos	Detective ya no se limita a un conjunto seleccionado de tipos de GuardDuty hallazgos . Detective recopila automátic amente los detalles de resultados de todos los tipos de resultados, y proporcio na acceso a los perfiles de entidad de las entidades relacionadas.	20 de septiembre de 2021
Enlace a los detalles del resultado desde el panel de perfil del resultado asociado	En el perfil de una entidad, al elegir un resultado de la lista de resultados asociada, los detalles del resultado se muestran en el panel de la derecha. El rango temporal se establece en la franja horaria del resultado.	20 de septiembre de 2021

Se han añadido buckets de S3 a los tipos de entidades disponibles en Detective	Detective ahora proporciona perfiles de buckets de S3. Los perfiles de bucket de S3 proporcionan detalles sobre las entidades principales que interactuaron con el bucket de S3 y las operaciones de API que realizaron en el bucket de S3.	20 de septiembre de 2021
Nueva opción para generar Detective URLs en Splunk	El proyecto Splunk Trumpet te permite enviar AWS contenido a Splunk. El proyecto ahora le permite añadir un Detective URLs para navegar a los perfiles en busca de GuardDuty hallazgos .	8 de septiembre de 2021
Se reemplazó AKIDs en los detalles de la actividad para las cuentas y los roles	En los perfiles de las cuentas, los detalles de actividad del volumen general de llamadas a la API ahora muestran los usuarios o las funciones en lugar de los identificadores de las claves de acceso (AKIDs). En los perfiles de rol, los detalles de actividad del volumen total de llamadas a la API ahora muestran las sesiones de rol en lugar de AKIDs. En el caso de la actividad que se produjo antes de este cambio, el llamante aparece como Recurso desconocido.	14 de julio de 2021

Se ha añadido el servicio de llamadas a la información sobre las llamadas a la API	En la consola de Detective , la información sobre las llamadas a la API ahora incluye el servicio que emitió la llamada. Se ha añadido una columna Servicio a las listas sobre el Volumen total de llamadas a la API, las Llamadas a la API observadas recientemente y las Llamadas a la API con aumento de volumen. En cuanto a los detalles de actividad relaciona dos con el Volumen total de llamadas a la API y las Geolocalizaciones recién observadas, los métodos de API se agrupan según los servicios que los emitieron . En el caso de la actividad que se produjo antes de este cambio, los métodos de API se agrupan como Servicio desconocido.	14 de julio de 2021
Nueva pestaña Interacción de recursos para usuarios, roles y sesiones de rol	La pestaña Interacción de recursos para usuarios, roles y sesiones de rol contiene información sobre la actividad de asunción de roles que implicó a esas entidades. Para las sesiones de rol, esta es una pestaña nueva. Para los usuarios y roles, esta es una pestaña existente con contenido nuevo.	29 de junio de 2021

Valores actualizados para las cuotas de volumen de datos en los gráficos de comportamiento	Se han incrementado las cuotas de volumen de datos para gráficos de comportamiento. Con un volumen de 3,24 TB al día, Detective emite una advertencia. Con un volumen de 3,6 TB al día, no se pueden agregar nuevas cuentas. Con un volumen de 4,5 TB al día, Detective deja de introducir datos en el gráfico de comportamiento.	10 de junio de 2021
Valores de etiqueta agregados a las opciones de script de Python	Al utilizar el script de Python `enableDetective.py` para habilitar Detective, puede asignar valores de etiqueta al gráfico de comportamiento.	19 de mayo de 2021

Habilitación automática agregada para las cuentas de miembros que superan la comprobación de volumen de datos	Cuando las cuentas de miembros aceptan una invitación, su estado es Aceptado (No habilitado) hasta que Detective verifica que los datos de las cuentas no provocarán que el volumen de datos del gráfico de comportamiento supere la cuota. Si el volumen de datos no es un problema, Detective cambia automáticamente el estado a Aceptado (Habilita do). Tenga en cuenta que las cuentas de miembros cuyo estado sea Aceptado (No habilitado) en este momento no se habilitarán automátic amente.	12 de mayo de 2021
Información sobre políticas administradas agregada al capítulo de seguridad	Se ha agregado una nueva sección al capítulo de seguridad para proporcionar información sobre las políticas administradas para Detective . En este momento, Detective admite solo una política administrada, `AmazonDet ectiveFullAccess` .	10 de mayo de 2021

Valores de volumen de datos modificados en la lista de cuentas de miembros	En la página de administración de cuentas, la lista de cuentas de miembros ahora muestra el volumen de datos diario de cada cuenta de miembro. Anteriormente, la lista mostraba el volumen como un porcentaje del volumen total permitido.	29 de abril de 2021
Opciones revisadas para administrar cuentas de miembros	Se ha reemplazado el menú Administrar cuentas por el menú Acciones. Se han combinado las opciones para agregar cuentas de una en una y a partir de un archivo .csv. Se ha trasladado la opción Habilitar cuentas de Administrar cuentas a una opción independiente al lado de Acciones.	5 de abril de 2021
Adición de etiquetas de gráficos de comportamiento y de la autorización basada en etiquetas	Al habilitar Detective, puede agregar etiquetas al gráfico de comportamiento. Puede administrar las etiquetas de un gráfico de comportamiento desde la página General. Detective también admite la autorización basada en valores de etiqueta.	31 de marzo de 2021

Se agregó soporte para tipos de GuardDuty búsqueda adicionales de Amazon	Detective ahora proporciona perfiles para los siguientes tipos de GuardDuty búsqueda adicionales: `CredentialAccess:IAMUser/AnomalousBehavior` `DefenseEvasion:IAMUser/AnomalousBehavior` ,`Discovery:IAMUser/AnomalousBehavior` ,`Exfiltration:IAMUser/AnomalousBehavior` ,`Impact:IAMUser/AnomalousBehavior` ,`InitialAccess:IAMUser/AnomalousBehavior` ,`Persistence:IAMUser/AnomalousBehavior` , `PrivilegeEscalation:IAMUser/AnomalousBehavior`	29 de marzo de 2021
Se agregaron diferencias para AWS GovCloud (US) las regiones	Detective ya está disponible en las AWS GovCloud (US) regiones. En AWS GovCloud (EE. UU., Este) y AWS GovCloud (EE. UU., Oeste), Detective no envía correos electrónicos de invitación a las cuentas de los miembros. Detective tampoco elimina automáticamente las cuentas de miembros que se desactivan en AWS.	24 de marzo de 2021

Pestañas agregadas para filtrar la lista de cuentas de miembros en función de su estado	Ahora, la lista de cuentas de miembros cuenta con pestañas que le permiten filtrar la lista en función del estado de la cuenta de miembro. Puede ver todas las cuentas de miembros, las cuentas con el estado Aceptado (Habilitado) o las cuentas con otros estados que no sean Aceptado (Habilitado).	16 de marzo de 2021
Se agregó soporte para tipos de GuardDuty búsqueda adicionales de Amazon	Detective ahora proporcio na perfiles para los siguiente s tipos de GuardDuty búsqueda adicional es:`Backdoor:EC2/C&CActivity.B` ,`Impact:EC2/PortSweep` , `Impact:EC2/WinRMBruteForce` , y `PrivilegeEscalation:IAMUser/AdministrativePermissions`	4 de marzo de 2021
Opción agregada al script de Python para suprimir los correos electrónicos de invitación	El script `enableDetective.py` de Detective ahora cuenta con una opción `--disable_email` . Cuando se incluye esta opción, Detective no envía correos electrónicos de invitación a cuentas de miembros.	26 de febrero de 2021

Cambio del término “cuenta maestra” a “cuenta de administrador”	Se ha cambiado el término "cuenta maestra" por "cuenta de administrador". El término también se cambia en la consola de Detective y la API.	25 de febrero de 2021
Se cambió “cuenta maestra” a “cuenta de administrador”	Se ha cambiado el término "cuenta maestra" por "cuenta de administrador". El término también se cambia en la consola de Detective y la API.	25 de febrero de 2021
Se han añadido detalles de actividad al panel de perfil Volumen total de flujo de VPC hacia y desde la dirección IP del resultado	El panel de perfil Volumen total de flujo de VPC hacia y desde la dirección IP del resultado ahora permite ver los detalles de la actividad. Los detalles de la actividad solo están disponibles si el resultado está asociado a una única dirección IP. Los detalles de la actividad muestran el volumen de cada combinación de puertos, protocolos y dirección.	25 de febrero de 2021
Opción agregada a la API para no enviar correos electróni cos de invitación a cuentas de miembros	Al utilizar la API de Detective para agregar cuentas de miembros, las cuentas de administrador pueden elegir no enviar correos electróni cos de invitación a cuentas de miembros.	25 de febrero de 2021

Nuevos detalles de actividad para el panel de perfil Volumen total de llamadas a la API en los perfiles de dirección IP	Ahora puede ver los detalles de la actividad de las direccion es IP desde el panel de perfil Volumen total de llamadas a la API. Los detalles de la actividad muestran el número de llamadas correctas y fallidas de cada recurso que emitió la llamada desde la dirección IP.	23 de febrero de 2021
Nuevo panel de perfil Volumen total del flujo de la VPC en los perfiles de direcciones IP	El perfil de dirección IP ahora contiene el panel de perfil Volumen total del flujo de la VPC. El panel de perfil muestra el volumen del tráfico de flujo de VPC hacia y desde la dirección IP. Puede mostrar los detalles de la actividad para mostrar el volumen de cada EC2 instancia con la que se comunicó la dirección IP.	21 de enero de 2021
Se ha añadido la página Resumen de Detective	La página Resumen de Detectives contiene visualiza ciones para guiar a los analistas hacia las entidades de interés en función de la geolocalización, el número de llamadas a la API y el volumen de tráfico de Amazon EC2 .	21 de enero de 2021

Se actualizó la opción para pasar de Amazon GuardDuty a Detective	En GuardDuty, la opción Investigar en Detective se mueve del menú Acciones al panel de detalles de búsqueda. Muestra una lista de entidades relacionadas. Si se admite el tipo de resultado , la lista también incluye el resultado. A continuación, puede optar por navegar a un perfil de entidad o a un perfil de resultado.	15 de enero de 2021
Se ha añadido la opción de establecer la franja horaria de los detalles de actividad en el rango temporal predeterm inado	En los detalles de actividad de Volumen total de llamadas a la API y Volumen total del flujo de la VPC, puede configurar la franja horaria para los detalles de la actividad como el rango temporal predeterminado del perfil.	15 de enero de 2021
Se ha añadido el tratamien to de intervalos de tiempo de gran volumen para las entidades	Se ha añadido un nuevo aviso para indicar cuándo una entidad tiene uno o más intervalos de tiempo de gran volumen. Una nueva página Entidades de gran volumen muestra todos los intervalo s de gran volumen del rango temporal actual.	18 de diciembre de 2020
Cuota de cuentas de miembros aumentada a 1200	Las cuentas maestras ahora pueden invitar a hasta 1200 cuentas de miembros a un gráfico de comportamiento. La cuota anterior era de 1000.	11 de diciembre de 2020

Valores agregados para las cuotas de volumen de datos en los gráficos de comportamiento	Se ha actualizado la información sobre las cuotas de volumen de datos en los gráficos de comportamiento para agregar valores de cuota específicos.	11 de diciembre de 2020
Se ha añadido una selección de intervalo de tiempo para los detalles de actividad en el panel de perfil Volumen total de llamadas a la API	En el panel Volumen total del flujo de API, ahora puede ver los detalles de la actividad para cualquier intervalo de tiempo seleccionado. Inicialmente, el panel muestra una opción para mostrar los detalles de la actividad durante el rango temporal.	29 de septiembre de 2020
Se ha añadido la selección de intervalo para los detalles de actividad en el panel de perfil Volumen total del flujo de la VPC	En el panel Volumen total del flujo de la VPC, puede ver los detalles de la actividad de un único intervalo de tiempo en el gráfico. Para ver los detalles del intervalo de tiempo, elija el intervalo de tiempo.	25 de septiembre de 2020
Nuevas entidades de sesión de rol y usuario federado	Detective ahora le permite explorar e investigar la autenticación federada. Puede ver qué recursos han asumido cada rol y cuándo se produjeron esas autenticaciones.	17 de septiembre de 2020

Actualizaciones en la administración del rango temporal	Se ha eliminado la opción de bloquear o desbloquear el rango temporal. Siempre está bloqueado. En un perfil de resultado, se muestra una advertencia si el rango temporal es distinto de la franja horaria del resultado.	4 de septiembre de 2020
El encabezado del perfil permanece visible mientras se desplaza por un perfil	En los perfiles, el tipo, el identificador y el rango temporal permanecen visibles mientras se desplaza por los paneles de perfil de una pestaña. Cuando las pestañas no están visibles, puede usar la lista desplegable de pestañas de las rutas de navegación para ir a otra pestaña.	4 de septiembre de 2020
La búsqueda siempre muestra resultados de búsqueda	Al realizar una búsqueda, ahora se muestran los resultados en la página Búsqueda. A partir de los resultados, puede pasar a un perfil de resultado o de entidad.	27 de agosto de 2020
Se ha añadido a los criterios de búsqueda permitidos	Se han ampliado los criterios de búsqueda permitidos. Puede buscar AWS usuarios y AWS roles por nombre. Puede usar el ARN para buscar hallazgos, AWS funciones, AWS usuarios e EC2 instancias.	27 de agosto de 2020

Enlaces a otras consolas desde los paneles de perfil	En el EC2 panel de perfil de detalles de la EC2 instancia, el identificador de la instancia está vinculado a la EC2 consola de Amazon. En los paneles de perfil Detalles del usuario y Detalles del rol, el nombre del usuario y el nombre del rol están vinculado s a la consola de IAM.	14 de agosto de 2020
Detalles de actividad de los datos de flujo de VPC	El panel de perfil Volumen total del flujo de la VPC ahora proporciona acceso a los detalles de actividad. Los detalles de la actividad muestran el flujo de tráfico entre las direcciones IP y una EC2 instancia durante un período de tiempo seleccion ado.	23 de julio de 2020
Uso y costo previsto visibles para cuentas de miembros	Las cuentas de miembros ahora pueden ver su propia información sobre el uso. En el caso de las cuentas de miembros, en la página Uso se muestran la cantidad de datos ingeridos en cada gráfico de comportamiento al que aportan datos. Asimismo, las cuentas de miembros pueden consultar su costo previsto en un periodo de 30 días.	26 de mayo de 2020

Prueba gratuita disponible por cuenta, en vez de por gráfico de comportamiento	Ahora, cada cuenta de Amazon Detective recibe una prueba gratuita independiente en cada región. La prueba gratuita comienza cuando se habilita Detective en la cuenta o la primera vez que la cuenta se habilita como cuenta de miembro.	26 de mayo de 2020
Nuevos scripts de Python de código abierto en GitHub	El nuevo amazon-detective-multiaccount-scriptsrepositorio GitHub proporciona scripts de Python de código abierto que puede usar para administrar gráficos de comportamiento en todas las regiones. Entre otras cosas, le permiten habilitar Detective, agregar cuentas de miembros, eliminar cuentas de miembros y deshabilitar Detective.	21 de enero de 2020
Presentación de Amazon Detective	Detective utiliza machine learning y visualizaciones diseñadas específicamente para ayudarle a analizar e investigar los problemas de seguridad en sus cargas de trabajo de Amazon Web Services (AWS).	2 de diciembre de 2019

Las traducciones son generadas a través de traducción automática. En caso de conflicto entre la traducción y la version original de inglés, prevalecerá la version en inglés.