aws

Guía de administración

# Amazon Detective

# Amazon Detective: Guía de administración

# Table of Contents

# ¿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 periodo de tiempo seleccionado. Detective relaciona estos cambios con los resultados de GuardDuty. Para obtener más información sobre los datos de origen en Detective, consulte Datos de origen usados en un gráfico de comportamiento.

# ¿Cómo funciona Detective?

Detective extrae automáticamente los eventos de tiempo, así como los intentos de inicio de sesión, las llamadas a la API y el tráfico de red de los registros de flujo de AWS CloudTrail y Amazon VPC. También ingiere los resultados 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 las acciones discrepantes, como los intentos de inicio de sesión fallidos o las llamadas sospechosas a la API. También puede ver cómo estas acciones afectan a los recursos; por ejemplo, a las cuentas de AWS e instancias de Amazon EC2. 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 resultados pueden ayudar a responder a preguntas como "¿Es esta

una llamada a la API inusual para este rol?". 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 cuentas de AWS. 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 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 los recursos de AWS y los resultados de GuardDuty. Al usar las integraciones de Detective con GuardDuty y AWS Security Hub, puede pasar de un resultado de GuardDuty 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 se utiliza Amazon Detective con fines de investigación en la Guía del usuario de Detective.

# Términos y conceptos de Amazon Detective

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

Cuenta de administrador

Cuenta de AWS propietaria de un gráfico de comportamiento y que lo usa con fines de investigación.

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 “Invitación de cuentas de miembros a un gráfico de comportamiento”.

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 de 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 vinculado de datos generado a partir de datos de origen entrantes que está asociado a una o varias 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:

- Registros de servicios de AWS, como registros de AWS CloudTrail y registros de flujo de Amazon VPC
- Resultados de GuardDuty

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 entidad son las direcciones IP, las instancias de Amazon EC2 y los usuarios de AWS.

Las entidades pueden ser recursos de AWS que usted administra, o 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

En el contexto de Amazon GuardDuty, designa a un problema de seguridad detectado por el servicio.

Grupo de resultados

Conjunto de resultados, entidades y pruebas 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.

Pruebas 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 pruebas se presentan como un resultado con valor de gravedad Informativo. Las pruebas 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 llamadas a la API observadas durante el tiempo de alcance de un resultado. En este momento, estos resultados solo se pueden ver en Detective y no se envían a Security Hub.

Descripción general del resultado

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 instancia EC2 puede tener conexiones desde millones de direcciones IP. El número de conexiones supera el umbral que Detective puede admitir.

Cuando el tiempo de alcance 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

Cuenta de AWS a la que una cuenta de administrador ha invitado a contribuir a un gráfico de comportamiento con datos. 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 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 tipo de relación es una dirección IP que se conecta a una instancia de Amazon EC2.

Tiempo de alcance

Horquilla de tiempo que se utiliza para delimitar los datos que se muestran en los perfiles.

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

El tiempo de alcance predeterminado de un perfil de entidad son las 24 horas anteriores.

# 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 en las que Detective está disponible, consulte Puntos de conexión 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.<br><br>Para volver a habilitar la ingesta de datos, debe ponerse en contacto con AWS Support. |

## Internet Explorer 11 no compatible

No puede utilizar Detective con Internet Explorer 11.

# Configuración de Amazon Detective

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 puede 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 período 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 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 período 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”.

Contenido



## Requisitos previos y recomendaciones de Amazon Detective

Para habilitar Amazon Detective, necesita tener una Cuenta de AWS.

### Inscríbase en una Cuenta de AWS

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

Para suscribirte a una Cuenta de AWS

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

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

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 administrativo 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. Puede ver la actividad de la cuenta y administrar la cuenta en cualquier momento entrando en https://aws.amazon.com/ y seleccionando Mi cuenta.

## Crear un usuario 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 Signing in as the root user 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 administrativo

1. Activar IAM Identity Center

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

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.

Cómo iniciar sesión como usuario administrativo

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

También debe conocer los siguientes requisitos y recomendaciones.

## Versión compatible AWS Command Line Interface

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

## Alineación recomendada con y GuardDuty 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.

## 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.

## Actualización recomendada de la frecuencia de las 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 Amazon Detective

Al activar Detective, designa una cuenta de administrador de Detective e invita a otras cuentas a convertirse en cuentas de miembros. La relación entre administrador y miembros se establece cuando una potencial cuenta de miembro acepta la invitación. Para obtener más información, consulte Administrar cuentas.

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. Para obtener más información sobre cómo se administra la cuenta de administrador de Detective, consulte Designación de la cuenta de administrador de Detective para una organización.

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.

## Habilitación de Detective (consola)

Puede habilitar Amazon Detective desde la AWS Management Console.

Habilitación de Detective (consola)

1. Inicie sesión en. AWS Management Console A continuación, abra la consola de Detective 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 y GuardDuty AWS Security Hub”.

4. El botón Asociar política de IAM le lleva directamente a la consola de IAM y abre la política recomendada. Puede asociar esta política recomendada a la entidad principal que utiliza para 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 “Invitación de cuentas de miembros a un gráfico de comportamiento”.

## Habilitación de Detective (API de Detective, 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"}'
```

## Activación de Detective en todas las regiones (secuencia de comandos de Python activada 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, consulteUso de los scripts de Python de Amazon Detective.

## Comprobación de la extracción de datos

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.

# 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 período. Cuando finaliza el período 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 Hacer el seguimiento de las acciones y el uso en Amazon Detective. Para obtener más información acerca de los precios, consulte Precios de Detective.

Se utiliza el mismo período 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 período 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.

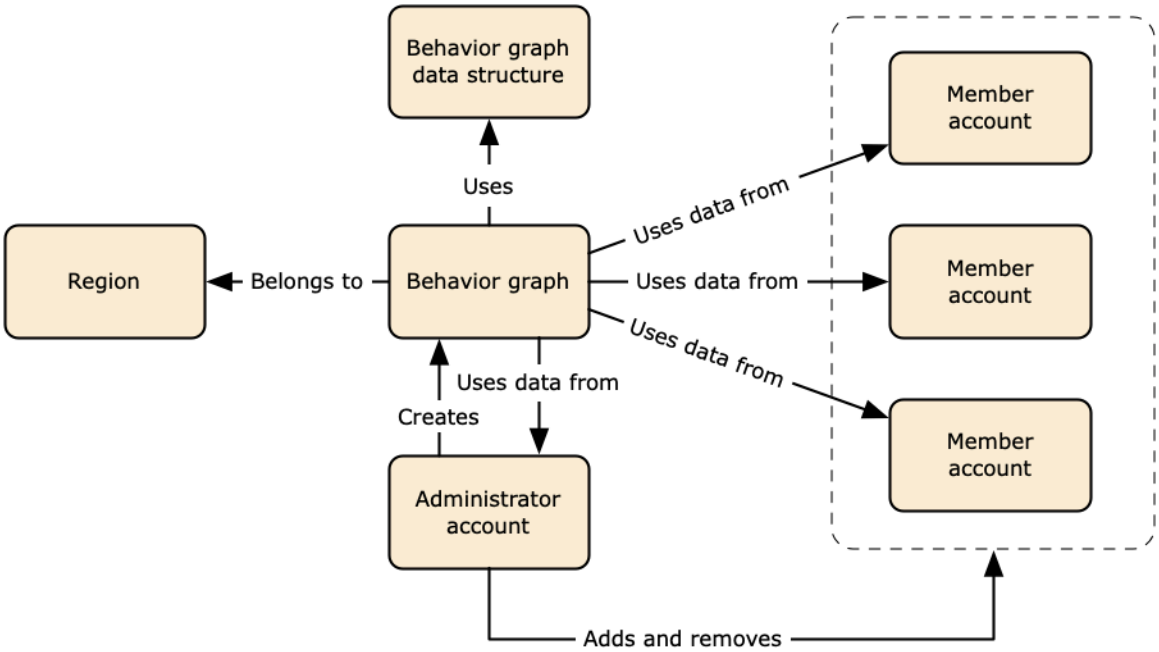
> **Note**
>
> Si un cliente deshabilita un paquete de origen de datos opcional en el plazo de 7 días después de habilitarlo, Detective puede reiniciar una sola vez y de forma automática la versión de prueba gratuita para ese paquete de origen de datos si se habilita de nuevo.

Para habilitar o deshabilitar un origen de datos opcional, consulte Tipos de orígenes de datos opcionales en Detective.

# Datos de origen usados en un gráfico de comportamiento

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 una horquilla de tiempo seleccionada. Detective relaciona estos cambios con los resultados de GuardDuty.




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

Detective ingiere datos de estos tipos de registros de AWS:

- Registros de AWS CloudTrail
- Registros de flujo de Amazon Virtual Private Cloud (Amazon VPC)
- En el caso de las cuentas que están inscritas en GuardDuty, Detective también ingiere los resultados de GuardDuty.

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

## Tipos de orígenes de datos opcionales en Detective

Detective ofrece paquetes de origen opcionales, además de los tres orígenes de datos que se ofrecen en el paquete básico de Detective (el paquete básico incluye registros de AWS CloudTrail, registros de flujo de VPC y resultados de GuardDuty). 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 orígenes de datos opcionales permite a Detective ingerir información detallada sobre los clústeres de EKS de su entorno, y añade esos datos a su gráfico de comportamiento. Para obtener más información, consulte Registros de auditoría de Amazon EKS para Detective.
- Resultados de seguridad de AWS

  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 Resultados de seguridad de AWS.

Iniciar o detener un origen de datos opcional:

1. Abra la consola de Detective 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 período 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 de auditoría de Amazon EKS para Detective

Los registros de auditoría de Amazon EKS son un paquete de orígenes de datos opcionales que se puede agregar a su gráfico de comportamiento de Detective. Puede ver los paquetes de orígenes opcionales disponibles y su estado en su cuenta desde la página Configuración de la consola o a través de la API de Detective.

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 auditoría de Amazon EKS, Detective puede añadir información detallada sobre los recursos creados con Amazon EKS a su gráfico de comportamiento. Este origen de datos mejora la información proporcionada sobre los siguientes tipos de entidades: clústeres de EKS, pods de Kubernetes, imágenes de contenedor y sujetos de Kubernetes.

Además, si ha habilitado los registros de auditoría de EKS como origen de datos en Amazon GuardDuty, podrá ver los detalles de los resultados de Kubernetes en GuardDuty. Para obtener más información sobre cómo habilitar este origen de datos en 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 registros de auditoría de Amazon EKS como orígenes de datos opcionales:

1. Abra la consola de Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, en Configuración, elija General.
3. En Paquetes de origen, seleccione Registros de auditoría de EKS para habilitar este origen de datos. Si ya está habilitada, selecciónela de nuevo para detener la ingesta de Registros de auditoría de EKS en su gráfico de comportamiento.

## Resultados de seguridad de AWS

Resultados de seguridad de AWS es un paquete de orígenes de datos opcionales que se puede añadir a su gráfico de comportamiento de Detective.

Puede ver los paquetes de orígenes opcionales disponibles y su estado en su cuenta desde la página Configuración de la consola o a través de la API de Detective.

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 Resultados de seguridad de AWS, Detective puede usar los resultados de Security Hub agregados por Security Hub desde los servicios previos en un formato de resultado estándar denominado AWS Security Format (ASFF), lo que elimina la engorrosa tarea de conversión. A continuación, correlaciona los resultados ingeridos en los distintos productos para priorizar los más importantes.

Añadir o eliminar resultados de seguridad de AWS como origen de datos opcional:

> **Note**
>
> El origen de datos de resultados de seguridad de AWS está habilitado de forma predeterminada en los gráficos de comportamiento nuevos, 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. Abra la consola de Detective en https://console.aws.amazon.com/detective/.
2. En el panel de navegación, en Configuración, elija General.

3. En Paquetes de origen, seleccione los resultados de seguridad de AWS para habilitar este origen de datos. Si ya está habilitado, selecciónelo de nuevo para detener la ingesta de resultados en AWS Security Finding Format (ASFF) en su gráfico de comportamiento.

### Resultados admitidos actualmente

Detective ingiere todos los resultados ASFF en Security Hub desde los servicios propiedad de Amazon o AWS.

- Para ver la lista de integraciones de servicios admitidas, consulte Integraciones de servicios de AWS disponibles en la Guía del usuario de AWS Security Hub.
- Para ver la lista de recursos admitidos, consulte Recursos en la Guía del usuario de AWS Security Hub.
- No se incluyen en la ingesta los resultados de servicios de AWS cuyo estado de conformidad no esté establecido en `FAILED` ni los resultados agregados 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 con AWS Support para volver a habilitarla. Si es posible, antes de contactar con AWS Support, intente eliminar las cuentas de miembro 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.

# Administración de cuentas

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.

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.

Una cuenta de administrador también puede invitar a cuentas para que se unan 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.

Detective cobra a todas las cuentas por los datos que aportan a cada gráfico de comportamiento. Para obtener información sobre cómo llevar un seguimiento del volumen de datos de cada cuenta en un gráfico de comportamiento, consulte the section called “Uso y costo de la cuenta de administrador”.

Contenido

- 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

# 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.

## Cuentas y regiones

Si utiliza 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 AWS Security Hub y Amazon GuardDuty funcionen sin problemas, se recomienda que la cuenta de administrador sea la misma para todos estos servicios.

Consulte the section called “Alineación recomendada con y GuardDuty AWS Security Hub”.

## Concesión de los permisos necesarios para cuentas de administrador

Para garantizar que una cuenta de administrador disponga de todos los permisos necesarios para administrar su gráfico de comportamiento, asocie la política administrada de `AmazonDetectiveFullAccess` a la entidad principal de IAM.

## 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.

# Transición de Organizations a la administración de cuentas en gráficos de comportamientos

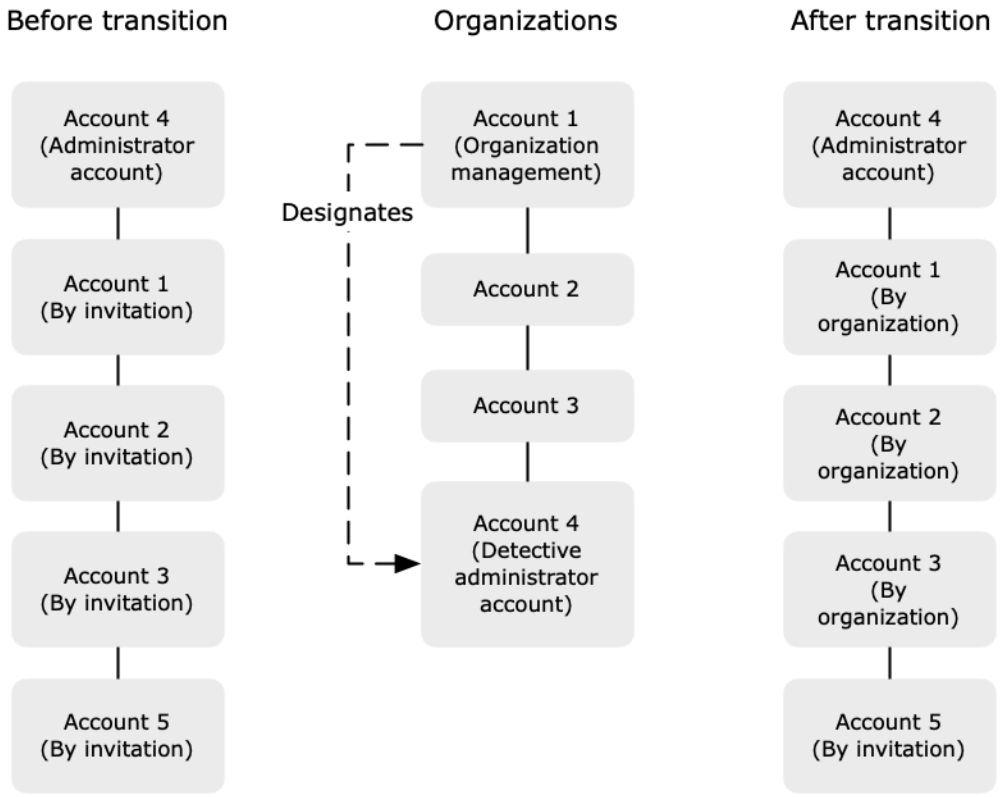
Es posible que ya disponga de un gráfico de comportamiento con cuentas de miembros que aceptaron una invitación manual. Si está inscrito en AWS Organizations, dé los siguientes pasos para usar Organizations para habilitar y administrar cuentas miembro en lugar de utilizar el proceso de invitación manual:

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 “Habilitación automática de nuevas cuentas de la 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.

# 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.

La siguiente tabla refleja los permisos predeterminados para las cuentas de administrador y de miembros. Puede usar políticas de IAM 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<br><br>Se eliminan las cuentas de invitados<br><br>Las cuentas de la organización están desvinculadas | Cualquiera | – | Auto |
| Agregar o eliminar paquetes de | Cualquiera (la configuración se aplica a todas | Cualquiera (la configuración se aplica a todas | – | – |

| Acción | Cuenta de administrador (organización) | Cuenta de administrador (invitación) | Miembro (organización) | Miembro (invitación) |
|---|---|---|---|---|
| origen de datos opcionales | las cuentas de los miembros) | las cuentas de los miembros) | | |
| Deshabilitar Detective | Auto | Auto | – | – |
| Ver los datos del gráfico de comportamiento | Cualquiera | Cualquiera | – | – |
| Habilitar o deshabilitar paquetes de origen de datos opcionales | Todos | Todos | – | – |

# Designación de la cuenta de administrador de Detective para 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 Detective

La cuenta de administración de la organización designa la cuenta de administrador de Detective en cada Región de AWS.

### Configuración de la cuenta de administrador de Detective como 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 como la cuenta de administrador de Detective. La cuenta de administración de la organización no puede ser un administrador delegado en Organizations.

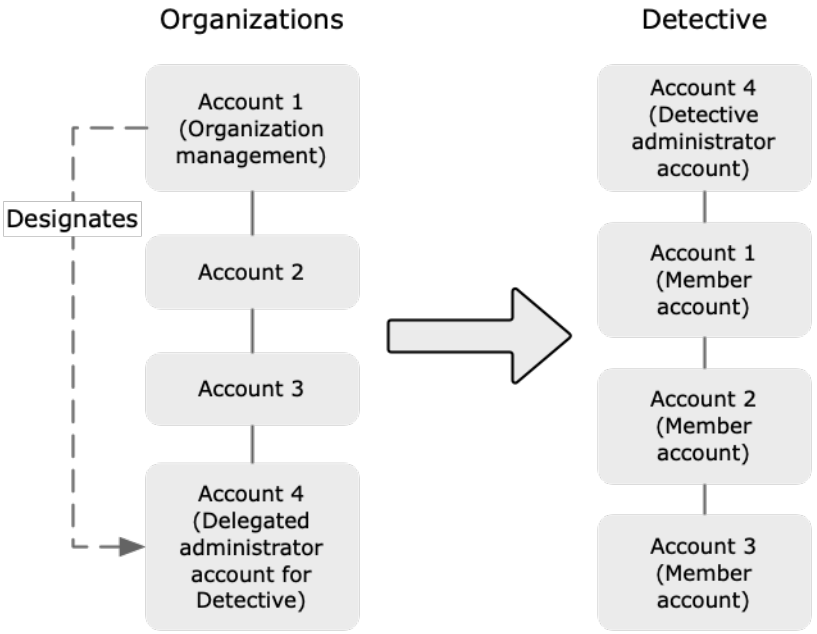
Una vez configurada la cuenta de administrador delegado en Organizations, la cuenta de administración de la organización solo puede elegir la cuenta de administrador delegado o su propia cuenta como cuenta de administrador de Detective. Le recomendamos que elija la cuenta de administrador delegado en 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 Detective, 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 invitadas”.

### 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 la API de Organizations. 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.

## 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 asociar la política administrada `AmazonDetectiveOrganizationsAccess` a las entidades de AWS Identity and Access Management (IAM).

## Designación de una cuenta de administrador de Detective (consola)

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.

Designación de una 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 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. Elija Adjuntar política de IAM para ver la política recomendada directamente en la consola de IAM.
5. En función de si tiene permisos en la consola de IAM o no, continúe de la siguiente forma:

   - Si tiene permisos para trabajar con la consola de IAM, asocie la política recomendada a la entidad principal que utiliza para Detective.
   - Si no tiene permisos para trabajar con la consola de IAM, copie 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.
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 tiene una cuenta de administrador delegado en Organizations para Amazon GuardDuty, AWS Security Hub o Amazon Macie, Detective le solicita que selecciona 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.

Designación 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 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 consola de IAM o no, continúe de la siguiente forma:

   - Si tiene permisos para trabajar con la consola de IAM, asocie la política recomendada a la entidad principal que utiliza para Detective.
   - Si no tiene permisos para trabajar con la consola de IAM, copie 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.

   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 tiene una cuenta de administrador delegado en Organizations para Amazon GuardDuty, AWS Security Hub o Amazon Macie, Detective le solicita que selecciona 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.

## Designación de una cuenta de administrador de Detective (API de Detective y AWS CLI)

Para designar la cuenta de administrador de Detective, puede utilizar una llamada a la API o la AWS Command Line Interface. Debe utilizar 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.

Designación de una cuenta de administrador de Detective (API de Detective y AWS CLI)

- API de Detective: utilice la operación `EnableOrganizationAdminAccount`. Debe proporcionar el identificador de la cuenta de AWS para la cuenta de administrador de Detective. Para obtener el identificador de la cuenta, utilice la operación `ListOrganizationAdminAccounts`.
- AWS CLI: en la línea de comandos, ejecute el comando `enable-organization-admin-account`.

  ```
  aws detective enable-organization-admin-account --account-id <admin account ID>
  ```

  Ejemplo

  ```
  aws detective enable-organization-admin-account --account-id 777788889999
  ```

## Eliminación de una cuenta de administrador de Detective (consola)

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.

## Eliminación de la cuenta de administrador de Detective (API de Detective y AWS CLI)

Para eliminar la cuenta de administrador de Detective, puede utilizar una llamada a la API o la AWS CLI. Debe utilizar 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.

Eliminación de la cuenta de administrador de Detective (API de Detective y AWS CLI)

- API de Detective: utilice la operación `DisableOrganizationAdminAccount`.

  Si se utiliza la API de Detective para eliminar la cuenta de administrador de Detective, solo se elimina en la región en la que se emitió la llamada a la API o el comando.

- AWS CLI: en la línea de comandos, ejecute el comando disable-organization-admin-account.

```
aws detective disable-organization-admin-account
```

## Cómo eliminar la cuenta de administrador delegado (API de Organizations y AWS CLI)

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 actual de Detective, puede utilizar la API de Organizations.

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.

Eliminación de la cuenta de administrador delegado (API de Organizations y AWS CLI)

- API de Organizations: utilice la operación DeregisterDelegatedAdministrator. 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 comando deregister-delegated-administrator.

```
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
```

# Visualización de la lista de cuentas

La cuenta de administrador puede utilizar la consola o la API de Detective para 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 Detective 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 tus cuentas de miembros (API de Detective, AWS CLI)

Puedes usar una llamada a la API o la AWS Command Line Interface para ver una lista de cuentas de miembros en tu gráfico de comportamiento.

Para obtener el ARN del gráfico de comportamiento que se utilizará en la solicitud, utilice la operación `ListGraphs`.

Para recuperar una lista de cuentas de miembros (API de Detective AWS CLI),

- API de Detective: utilice la operación `ListMembers`. Especifique el ARN del gráfico de comportamiento para identificarlo.

  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
  ```

Obtención de detalles sobre cuentas de miembros específicas de un gráfico de comportamiento (API de Detective y AWS CLI)

- API de Detective: utilice la operación `GetMembers`. Especifique el ARN del gráfico de comportamiento y la lista de identificadores de las cuentas de 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
  ```

# Administración de cuentas de la organización como cuentas de miembros

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.

La cuenta de administrador de Detective también puede desasociar cuentas de la organización del gráfico de comportamiento de la organización.

Contenido



## Habilitación automática de nuevas cuentas de la organización como cuentas de 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.

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.

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.

## Habilitación automática de nuevas cuentas de la organización (consola)

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.

## Habilitar automáticamente las nuevas cuentas de la organización (API de Detective AWS CLI)

Para determinar si se deben habilitar automáticamente las nuevas cuentas de la organización como cuentas de miembros, la cuenta de administrador puede utilizar la API de Detective o la AWS Command Line Interface.

Para ver y administración, debe proporcionar el ARN del gráfico de comportamiento. Para obtenerlo, utilice la operación `ListGraphs`.

Visualización de la configuración actual para habilitar automáticamente cuentas de la organización

- API de Detective: utilice la operación `DescribeOrganizationConfiguration`.

  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

- API de Detective: utilice la operación `UpdateOrganizationConfiguration`. 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
```

## Habilitación de cuentas de la organización como cuentas de miembros

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.

## Habilitación de cuentas de la organización como cuentas de miembros (consola)

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.

## Habilitar las cuentas de la organización como cuentas de miembros (API de Detective AWS CLI)

Puede utilizar la API Detective o la 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 el ARN del gráfico de comportamiento que se utilizará en la solicitud, utilice la operación `ListGraphs`.

Para habilitar las cuentas de la organización como cuentas de miembros (API de Detective AWS CLI),

- API de Detective: utilice la operación `CreateMembers`. Debe proporcionar el ARN del gráfico.

  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
```

## Desasociación de cuentas de la organización como cuentas de miembros

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

### Desasociación de cuentas de la organización (consola)

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 Acciones. A continuación, elija Desactivar cuentas.

   El estado de las cuentas desasociadas cambia a No es miembro.

### Disociar las cuentas de la organización (API de Detective,) AWS CLI

Puedes usar la API Detective o la AWS Command Line Interface para desasociar las cuentas de la organización como cuentas de miembros en tu gráfico de comportamiento.

Para obtener el ARN del gráfico de comportamiento que se utilizará en la solicitud, utilice la operación `ListGraphs`.

Desasociación de cuentas de la organización del gráfico de comportamiento de la organización (API de Detective y AWS CLI)

- API de Detective: utilice la operación `DeleteMembers`. Especifique el ARN del gráfico y la lista de identificadores de las cuentas de miembros que desea 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
```

# Administración de cuentas de miembros invitadas

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 cuenta de administrador de Detective también puede invitar a cuentas que no sean de una organización al gráfico de comportamiento de la organización.

La cuenta de administrador puede eliminar cuentas de miembros invitadas del gráfico de comportamiento.

Contenido

# Invitación de cuentas de miembros a un gráfico de comportamiento

La cuenta de administrador puede invitar a cuentas para que proporcionen datos a un gráfico de comportamiento. Un gráfico de comportamiento puede contener hasta 1200 cuentas de miembros.

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 (EE. UU.-Oeste)

   Para otras regiones, puede `DisableEmailNotification` utilizar el CreateMembersfuncionamiento de la API Detective. 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. Consulte the 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.

## Invitación de cuentas a un gráfico de comportamiento (consola)

Puede especificar manualmente las cuentas de miembros que desea invitar para que aporten datos a un gráfico de comportamiento.

Selección manual de cuentas de miembros para invitaciones (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 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 para recordar a la cuenta de miembro que debe asociar la política de IAM necesaria a su usuario o rol antes de aceptar la invitación.
8. La política de IAM de la cuenta miembro contiene el texto de la política de IAM necesaria para cuentas de miembros. El correo electrónico de invitación incluye este texto de política. Para copiarlo, elija Copiar.

9. Elija Invitar.

## Invitación de una lista de cuentas de miembros a un gráfico de comportamiento (consola)

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 de miembro que debe asociar la política de IAM necesaria.

9. La política de IAM de la cuenta miembro contiene el texto de la política de IAM necesaria para cuentas de miembros. El correo electrónico de invitación incluye este texto de política. Para copiarlo, elija Copiar.

10. Elija Invitar.

## Invitar a las cuentas de los miembros a un gráfico de comportamiento (API de Detective AWS CLI)

Puede usar la API Detective o AWS Command Line Interface para invitar a las cuentas de los miembros a contribuir con sus datos a un gráfico de comportamiento. Para obtener el ARN del gráfico de comportamiento que se utilizará en la solicitud, utilice la operación `ListGraphs`.

Para invitar a las cuentas de los miembros a un gráfico de comportamiento (API de Detective AWS CLI),

- API de Detective: utilice la operación `CreateMembers`. Debe proporcionar el ARN del gráfico. 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
```

## Añadir una lista de cuentas de miembros en todas las regiones (secuencia de comandos de Python activada GitHub)

Detective proporciona un script 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, consulteUso de los scripts de 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.

## Habilitación de una cuenta de miembro con el estado No habilitado (consola)

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.

## Habilitar una cuenta de miembro que no está habilitada (API de Detective, AWS CLI)

Puede utilizar una llamada AWS Command Line Interface a la API o para habilitar una cuenta de un solo miembro que no esté habilitada. Para obtener el ARN del gráfico de comportamiento que se utilizará en la solicitud, utilice la operación `ListGraphs`.

Habilitación de una cuenta de miembro con el estado No habilitado

- API de Detective: utilice la operación de la API `StartMonitoringMember`. Debe proporcionar el ARN del gráfico de comportamiento. Para identificar la cuenta del miembro, utilice el identificador de la AWS cuenta.
- AWS CLI: en la línea de comandos, ejecute el comando `start-monitoring-member`:

```
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
```

## Eliminación de cuentas de miembros invitadas de un gráfico de comportamiento

La cuenta de administrador puede eliminar cuentas de miembros 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.

## Eliminación de cuentas de miembros invitadas de un gráfico de comportamiento (consola)

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 Acciones. A continuación, elija Desactivar cuentas.

## Eliminar las cuentas de los miembros invitados de un gráfico de comportamiento (API de Detective AWS CLI)

Puedes usar la API de Detective o AWS Command Line Interface para eliminar las cuentas de los miembros invitados de tu gráfico de comportamiento. Para obtener el ARN del gráfico de comportamiento que se utilizará en la solicitud, utilice la operación `ListGraphs`.

Para eliminar las cuentas de los miembros invitados de tu gráfico de comportamiento (API de Detective, AWS CLI)

- API de Detective: utilice la operación `DeleteMembers`. Especifique el ARN del gráfico y la lista de identificadores de las cuentas de miembros que desea 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
```

### Eliminar una lista de cuentas de miembros invitados en todas las regiones (secuencia de comandos de Python activada GitHub)

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, consulteUso de los scripts de 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



### Política de IAM necesaria para una cuenta de miembro

Para que la cuenta de miembro pueda ver y administrar invitaciones, la política de IAM necesaria debe estar asociada a la entidad principal de la cuenta. 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 la cuenta de administrador solicite al administrador de IAM que asocie la política necesaria.

La política de IAM para cuentas de miembros concede acceso a las acciones de las cuentas de miembros en Amazon Detective. El correo electrónico de invitación para aportar datos a un gráfico de comportamiento incluye el texto de dicha política de IAM.

Para utilizar esta política, sustituya *<behavior graph ARN>* por el ARN del gráfico.

```
{
  "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 Detective, la API Detective o la cuenta de un miembro AWS Command Line Interface, puedes ver sus invitaciones con gráficos de comportamiento.

## Visualización de invitaciones a gráficos de comportamiento (consola)

Puede ver las invitaciones con gráficos de comportamiento en AWS Management Console.

Visualización de invitaciones a gráficos de comportamiento (consola)

1. Inicie sesión en AWS Management Console. A continuación, abra la consola de Detective 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.

  Si su cuenta no provoca que el gráfico de comportamiento supere la cuota de Detectives, Detective actualiza el estado de su cuenta a Habilitada. 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 a gráficos de comportamiento (API de Detective y AWS CLI)

Puede incluir invitaciones a un gráfico de comportamiento en una lista desde la API de Detective o la AWS Command Line Interface.

Obtención de una lista de invitaciones abiertas y aceptadas a gráficos de comportamiento (API de Detective y AWS CLI)

- API de Detective: utilice la operación `ListInvitations`.
- 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 (API de Detective AWS CLI)

Puede responder a invitaciones de gráficos de comportamiento desde la API de Detective o la AWS Command Line Interface.

Para aceptar una invitación con un gráfico de comportamiento (API de Detective AWS CLI),

- API de Detective: utilice la operación `AcceptInvitation`. Debe especificar el ARN del gráfico.
- 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
```

Para rechazar una invitación con un gráfico de comportamiento (API de Detective AWS CLI),

- API de Detective: utilice la operación `RejectInvitation`. Debe especificar el ARN del gráfico.
- 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 (API de Detective, AWS CLI)

Puedes usar la API de Detective o la AWS Command Line Interface para eliminar tu cuenta de un gráfico de comportamiento.

Para eliminar tu cuenta de un gráfico de comportamiento (API de Detective AWS CLI),

- API de Detective: utilice la operación `DisassociateMembership`. Debe especificar el ARN del gráfico.
- 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.

## Suspensión de una cuenta de AWS

Cuando se suspende una cuenta de administrador en 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 una cuenta de miembro en AWS, Detective deja de ingerir 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.

## Cierre de una cuenta de AWS

Cuando se cierra una cuenta de AWS, Detective responde al cierre de la siguiente forma:

- 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 de administrador. Al final del periodo de 90 días, AWS eliminará de forma permanente todos los datos de la política de la cuenta.

- Si desea conservar los resultados por más de 90 días, puede archivar las políticas. También puede utilizar una acción personalizada con una regla de EventBridge para almacenar los resultados en un bucket de S3.

- Mientras AWS conserva los datos de la política, cuando vuelva a abrir la cuenta cerrada, AWS reasignará la cuenta como administrador del servicio y recuperará 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.

# Hacer el seguimiento de las acciones y el uso en Amazon Detective

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 registro de AWS CloudTrail.

Contenido



## Monitorizar el uso y el costo de un gráfico de comportamiento (cuenta de administrador)

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. Luego abra la consola de Detective 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 cuenta de AWS 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 Detective básico muestran el volumen de ingesta de datos de los orígenes básicos de Detective (registros de CloudTrail, registros de flujo de VPC y resultados de GuardDuty) de los últimos 30 días.

Registros de auditoría de EKS

Los paneles Registros de auditoría de EKS muestran el volumen de ingesta de datos de los orígenes de registros de auditoría de EKS durante los últimos 30 días. Los paneles de este paquete de origen solo están disponibles si los registros de auditoría de EKS están habilitados para el gráfico de comportamiento.

# Monitorización del uso y el costo en gráficos de comportamiento (cuenta de miembro)

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. Abra la consola de Detective 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. También 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 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.

# Registro de llamadas a la API de Amazon Detective con AWS CloudTrail

Detective está integrado con AWS CloudTrail, un servicio que proporciona un registro de las acciones de un usuario, rol o servicio de AWS en Detective. CloudTrail recopila las llamadas a la API de Detective como eventos. Entre las llamadas recopiladas, se incluyen las llamadas realizadas desde la consola de Detective y las llamadas de código a las operaciones de la API de Detective.

- Si crea un registro de seguimiento, puede habilitar la entrega continua de eventos de CloudTrail a un bucket de Amazon S3, incluidos los eventos de Detective.
- Si no configura un registro de seguimiento, puede ver los eventos más recientes de la consola de CloudTrail en el Historial de eventos.

Con la información recopilada por CloudTrail, puede determinar la siguiente información:

- 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 acerca de CloudTrail, consulte la Guía del usuario de AWS CloudTrail.

# Información de Detective en CloudTrail

CloudTrail se habilita en su cuenta de AWS cuando la crea. Cuando se produce una actividad en Detective, dicha actividad se registra en un evento de CloudTrail junto con los eventos de los demás servicios de AWS en Historial de eventos. Puede ver, buscar y descargar los últimos eventos de la cuenta de AWS. Para obtener más información, consulte Ver eventos con el historial de eventos de CloudTrail.

Para mantener un registro continuo de eventos de la cuenta de AWS, incluidos los eventos de Detective, cree un registro de seguimiento. Un registro de seguimiento permite a CloudTrail enviar 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. El registro de seguimiento registra los eventos de todas las regiones de la partición de AWS y envía los archivos de registro al bucket de Amazon S3 especificado. Puede configurar otros servicios de AWS para analizar los datos de eventos recopilados en los registros de CloudTrail y tomar medidas al respecto.

Para obtener más información, consulte lo siguiente:

- Introducción a la creación de registros de seguimiento
- Servicios e integraciones compatibles con CloudTrail
- Configuración de notificaciones de Amazon SNS para CloudTrail
- Recibir archivos de registro de CloudTrail de varias regiones y Recibir archivos de registro de CloudTrail de varias cuentas

CloudTrail registra todas las operaciones de Detective, que se documentan en la Referencia de la API de Detective.

Por ejemplo, las llamadas a las operaciones `CreateMembers`, `AcceptInvitation` y `DeleteMembers` generan entradas en los archivos de registro de CloudTrail.

Cada entrada de registro o evento contiene información sobre quién generó la solicitud. La información de identidad del usuario le ayuda a determinar lo siguiente:

- Si la solicitud se realizó con las credenciales raíz o del usuario de 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 servicio de AWS.

Para obtener más información, consulte el Elemento userIdentity de CloudTrail.

## Comprensión de las entradas del archivo de registro de Detective

Un registro de seguimiento es una configuración que permite la entrega de eventos como archivos de registros en un bucket de Amazon S3 que especifique. Los archivos log de CloudTrail pueden contener una o varias entradas de log.

Un evento representa una única solicitud desde cualquier origen. Los eventos incluyen información sobre la acción solicitada, la fecha y hora de la acción, los parámetros de la solicitud, etc. Los archivos de registro de CloudTrail no rastrean el orden en la pila de las llamadas públicas a la API, por lo que las entradas no aparecen en ningún orden específico.

En el siguiente ejemplo, se muestra una entrada de registro de CloudTrail que ilustra la acción `AcceptInvitation`.


```
      {
            "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": []
        },
```

# Administrar etiquetas de un gráfico de comportamiento

Puede asignar etiquetas a su gráfico de comportamiento. A continuación, puede usar los valores de etiqueta de las políticas de IAM para administrar 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 costos asociados a la seguridad, puede asignar la misma etiqueta al gráfico de comportamiento de Detective, al recurso Hub AWS Security Hub y a los detectores de Amazon GuardDuty. En AWS Cost Explorer, puede buscar esa etiqueta para obtener una vista consolidada de los costos de todos esos recursos.

## Visualizar las etiquetas de un gráfico de comportamiento (consola)

Puede administrar las etiquetas de su gráfico de comportamiento desde la página General.

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.

## Obtener la lista de etiquetas de un gráfico de comportamiento (API de Detective, AWS CLI)

Puede usar la API de Detective o la AWS Command Line Interface para obtener la lista de etiquetas de su gráfico de comportamiento.

Para obtener la lista de etiquetas de un gráfico de comportamiento (API de Detective, AWS CLI)

- API de Detective: use la operación `ListTagsForResource`. Debe proporcionar el ARN de su gráfico de 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 (consola)

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, ingrese el nombre de la etiqueta.
3. En Valor, ingrese el valor de la etiqueta.

## Añadir etiquetas a un gráfico de comportamiento (API de DetectiveAWS CLI)

Puede usar la API de Detective o AWS CLI para añadir valores de etiquetas a su gráfico de comportamiento.

Para añadir etiquetas a un gráfico de comportamiento (API de Detective, AWS CLI)

- API de Detective: use la operación `TagResource`. Debe proporcionar el ARN del gráfico de comportamiento y los valores de etiqueta 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 (consola)

Para eliminar una etiqueta de la lista de la página General, elija la opción Eliminar para esa etiqueta.

## Eliminar etiquetas de un gráfico de comportamiento (API de Detective, AWS CLI)

Puede usar la API de Detective o la AWS CLI para eliminar valores de etiquetas de su gráfico de comportamiento.

Para eliminar etiquetas de un gráfico de comportamiento (API de Detective, AWS CLI)

- API de Detective: use la operación `UntagResource`. Proporciona el ARN del gráfico 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"
```

# Seguridad en Amazon Detective

La seguridad en la nube de AWS es la máxima prioridad. Como cliente de AWS, se beneficia de una arquitectura de red y un centro de datos diseñados para satisfacer los requisitos de seguridad de las organizaciones más exigentes.

La seguridad es una responsabilidad compartida entre AWS y el usuario. 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 los servicios de AWS en la nube de AWS. AWS también 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 servicio de AWS que utilice. También es responsable de otros factores, incluida la confidencialidad de los datos, los requisitos de la empresa y la legislación y la normativa aplicables.

Esta documentación le ayuda a comprender cómo aplicar el modelo de responsabilidad compartida cuando se utiliza Detective. En los siguientes temas, se le mostrará cómo configurar Detective para satisfacer sus objetivos de seguridad y conformidad. También puede aprender a utilizar otros servicios de AWS que lo ayuden a supervisar y proteger los recursos de Detective.

Contenido

- Seguridad de la infraestructura en Amazon Detective
- Prácticas recomendadas de seguridad para Amazon Detective

# Protección de datos en Amazon Detective

El modelo de responsabilidad compartida de AWS se aplica a la protección de datos en Amazon Detective. Como se describe en este modelo, AWS es responsable de proteger la infraestructura global que ejecuta la totalidad de Nube de AWS. Usted es responsable de mantener el control sobre el contenido alojado en esta infraestructura. Usted también es responsable de las tareas de administración y configuración de seguridad para los Servicios de AWS que utiliza. Para obtener más información sobre la privacidad de los datos, consulte las Preguntas frecuentes sobre la privacidad de datos. Para obtener información sobre la protección de datos en Europa, consulte la publicación de blog Modelo de responsabilidad compartida y GDPR de AWS en el Blog de seguridad de AWS.

Con fines de protección de datos, recomendamos proteger las credenciales de la cuenta de Cuenta de AWS y configurar cuentas de usuario individuales con AWS IAM Identity Center o AWS Identity and Access Management (IAM). De esta manera, solo se conceden a cada usuario los permisos necesarios para cumplir con sus obligaciones laborales. También recomendamos proteger sus datos de la siguiente manera:

- Utilice autenticación multifactor (MFA) en cada cuenta.
- Utilice SSL/TLS para comunicarse con los recursos de AWS. reSe recomienda el uso de TLS 1.2 y recomendamos TLS 1.3.
- Configure la API y el registro de actividad del usuario con AWS CloudTrail.
- Utilice las soluciones de cifrado de AWS, junto con todos los controles de seguridad predeterminados dentro de los Servicios de AWS.
- Utilice servicios de seguridad gestionados avanzados, como Amazon Macie, que lo ayuden a detectar y proteger los datos confidenciales almacenados en Amazon S3.
- Si necesita módulos criptográficos validados FIPS 140-2 al acceder a AWS a través de una interfaz de la línea de comandos o una API, utilice un punto de conexión de FIPS. Para obtener más información sobre los puntos de conexión de FIPS disponibles, consulte Estándar de procesamiento de la información federal (FIPS) 140-2.

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. Incluye las situaciones en las que se trabaja con Detective u otros Servicios de AWS a través de la consola, la API, la AWS CLI o los SDK de AWS. Cualquier dato que introduzca en etiquetas o campos de formato libre utilizados para nombres se pueden emplear para los registros de facturación o diagnóstico. Si proporciona una URL a un servidor externo, recomendamos encarecidamente que no incluya información de credenciales en la URL a fin de validar la solicitud para ese servidor.

Detective cifra todos los datos que procesa y los almacena en reposo y en tránsito.

Contenido



## 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 propiedad de AWS en la Guía del desarrollador de AWS Key Management Service.

Este tipo de clave KMS rota automáticamente cada año (aproximadamente cada 365 días). Consulte la descripción de la rotación de claves en la Guía del desarrollador de AWS Key Management Service.

# Identity and Access Management para Amazon Detective

AWS Identity and Access Management (IAM) es un Servicio de AWS que ayuda a los administradores a controlar de forma segura el acceso a los recursos de AWS. Los administradores de IAM controlan quién puede estar autenticado (ha iniciado sesión) y autorizado (tiene permisos) para utilizar recursos de Detective. IAM es un servicio de Servicio de AWS que se puede utilizar sin cargo adicional.

Contenido

- Ejemplos de políticas de basadas en identidades de Amazon Detective
- Solución de problemas de identidad y acceso de Amazon Detective

## Público

La forma en que utilice AWS Identity and Access Management (IAM) difiere en función del trabajo que lleve a cabo 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 ayudarlo 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. Luego, debe enviar solicitudes a su administrador de IAM para cambiar los permisos de los usuarios de su servicio. Revise la información de esta página para conocer los conceptos básicos de IAM. Para obtener más información sobre cómo su empresa puede utilizar IAM con Detective, consulte Cómo funciona Amazon Detective con IAM.

Administrador de IAM: si es administrador de IAM, es posible que quiera conocer más detalles sobre cómo escribir políticas para administrar el acceso a Detective. Para consultar ejemplos de políticas basadas en identidades que puede utilizar en IAM, consulte Ejemplos de políticas de basadas en identidades de Amazon Detective.

## Autenticación con identidades

La autenticación es la manera de iniciar sesión en AWS mediante credenciales de identidad. Debe estar autenticado (haber iniciado sesión en AWS) como el Usuario raíz de la cuenta de AWS, como un usuario de IAM o asumiendo un rol de IAM.

Puede iniciar sesión en AWS como una identidad federada mediante las credenciales proporcionadas a través de una fuente de identidad de AWS IAM Identity Center. Los usuarios (del Centro de identidades de IAM), la autenticación de inicio de sesión único de su empresa y sus credenciales de Google o Facebook son ejemplos de identidades federadas. Al iniciar sesión como una identidad federada, su administrador habrá configurado previamente la federación de

identidades mediante roles de IAM. Cuando accede a AWS mediante la federación, está asumiendo un rol de forma indirecta.

Según el tipo de usuario que sea, puede iniciar sesión en la AWS Management Console o en el portal de acceso a AWS. Para obtener más información sobre el inicio de sesión en AWS, consulte Cómo iniciar sesión en su Cuenta de AWS en la Guía del usuario de AWS Sign-In.

Si accede a AWS mediante programación, AWS proporciona un kit de desarrollo de software (SDK) y una interfaz de la línea de comandos (CLI) para firmar criptográficamente las solicitudes mediante el uso de las credenciales. Si no usa las herramientas de AWS, debe firmar usted mismo las solicitudes. Para obtener más información sobre la firma de solicitudes, consulte Firma de solicitudes API de AWS en la Guía del usuario de IAM.

Independientemente del método de autenticación que utilice, es posible que deba proporcionar información de seguridad adicional. Por ejemplo, AWS le recomienda el uso de la autenticación multifactor (MFA) para aumentar la seguridad de su cuenta. Para obtener más información, consulte Autenticación multifactor en la Guía del usuario de AWS Single Sign-On y Uso de la autenticación multifactor (MFA) en AWS en la Guía del usuario de IAM.

### Usuario raíz de cuenta de AWS

Cuando se crea una cuenta de AWS, se comienza con una identidad de inicio de sesión que tiene acceso completo a todos los servicios y recursos de AWS de la cuenta. Esta identidad recibe el nombre de usuario raíz de la Cuenta de AWS y se accede a ella iniciando sesión con la dirección de correo electrónico y la contraseña que utilizó para crear la cuenta. Recomendamos encarecidamente que no utilice el usuario raíz para sus tareas diarias. Proteja las credenciales del usuario raíz y utilícelas solo para las tareas que solo el usuario raíz pueda realizar. Para ver la lista completa de las tareas que requieren que inicie sesión como usuario raíz, consulte Tareas que requieren credenciales de usuario raíz en la Guía del usuario de IAM.

### Usuarios y grupos de IAM

Un usuario de IAM es una identidad en su Cuenta de AWS que dispone de permisos específicos para una sola persona o aplicación. Siempre que sea posible, recomendamos emplear credenciales temporales, en lugar de crear usuarios de IAM que tengan credenciales de larga duración como contraseñas y claves de acceso. No obstante, si tiene casos de uso específicos que requieran credenciales de larga duración con usuarios de IAM, recomendamos rotar las claves de acceso. Para más información, consulte Rotar las claves de acceso periódicamente para casos de uso que requieran credenciales de larga duración en la Guía del Usuario de IAM.

Un grupo de IAM es una identidad que especifica un conjunto de usuarios de IAM. No 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 de grandes conjuntos de usuarios. Por ejemplo, podría tener un grupo cuyo nombre fuese IAMAdmins y conceder permisos a dicho grupo para administrar los recursos de IAM.

Los usuarios son diferentes de los roles. Un usuario se asocia exclusivamente a una persona o aplicación, pero la intención es que cualquier usuario pueda asumir un rol que necesite. Los usuarios tienen credenciales permanentes a largo plazo y los roles proporcionan credenciales temporales. Para más información, consulte Cuándo crear un usuario de IAM (en lugar de un rol) en la Guía del Usuario de IAM.

## Roles de IAM

Un rol de IAM es una identidad de tu cuenta de AWS que dispone de permisos específicos. Es similar a un usuario de IAM, pero no está asociado a una determinada persona. Puede asumir temporalmente un rol de IAM en la AWS Management Consolecambiando de roles. Puede asumir un rol llamando a una operación de AWS CLI o de la API de AWS, o utilizando una URL personalizada. Para más información sobre los métodos para el uso de roles, consulte Uso de roles de IAM en la Guía del Usuario de IAM.

Los roles de IAM con credenciales temporales son útiles en las siguientes situaciones:

- Acceso de usuario federado: para asignar permisos a una identidad federada, 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 acerca de roles para federación, consulte Creación de un rol para un proveedor de identidades de terceros en la Guía del Usuario de IAM. Si utiliza el IAM Identity Center, debe configurar un conjunto de permisos. El IAM Identity Center correlaciona el conjunto de permisos con un rol en IAM para controlar a qué pueden acceder las identidades después de autenticarse. Para obtener información acerca de los conjuntos de permisos, consulte Conjuntos de permisos en la Guía del usuario de AWS IAM Identity Center.
- Permisos de usuario de IAM temporales: un usuario de IAM puede asumir un rol de IAM para recibir temporalmente permisos distintos que le permitan realizar una tarea concreta.
- Acceso entre cuentas: puede utilizar un rol de IAM para permitir que alguien (una entidad principal de confianza) de otra cuenta acceda a los recursos de la cuenta. Los roles son la forma principal de conceder acceso entre cuentas. No obstante, con algunos Servicios de AWS se puede asociar una política directamente a un recurso (en lugar de utilizar un rol como representante). Para

obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del usuario de IAM.

- Acceso entre servicios: algunos servicios de AWS utilizan características de otros Servicios de AWS. Por ejemplo, cuando realiza una llamada en un servicio, es común que ese servicio ejecute aplicaciones en Amazon EC2 o almacene objetos en Amazon S3. Es posible que un servicio haga esto usando los permisos de la entidad principal, usando un rol de servicio o usando un rol vinculado a servicios.
  - Reenviar sesiones de acceso (FAS): cuando utiliza un rol o un usuario de IAM para llevar a cabo acciones en AWS, se le considera una entidad principal. Cuando utiliza algunos servicios, es posible que realice una acción que desencadene otra acción en un servicio diferente. FAS utiliza los permisos de la entidad principal para llamar a un Servicio de AWS, combinados con el Servicio de AWS solicitante para realizar solicitudes a servicios posteriores. Las solicitudes de FAS solo se realizan cuando un servicio recibe una solicitud que requiere interacciones con otros Servicios de AWS o recursos para completarse. En este caso, debe tener permisos para realizar ambas acciones. Para obtener información sobre las políticas a la hora de realizar solicitudes de FAS, consulte Reenviar sesiones de acceso.
  - Rol de servicio: un rol de servicio es un rol de IAM que adopta un servicio para realizar acciones en su nombre. Un administrador de IAM puede crear, modificar y eliminar un rol de servicio desde IAM. Para obtener más información, consulte Creación de un rol para delegar permisos a un Servicio de AWS en la Guía del usuario de IAM.
  - Rol vinculado a servicios: un rol vinculado a servicios es un tipo de rol de servicio que está vinculado a un Servicio de AWS. El servicio puede asumir el rol para realizar una acción en su nombre. Los roles vinculados a servicios aparecen en su Cuenta de AWS y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.
- Aplicaciones que se ejecutan en Amazon EC2: puede utilizar un rol de IAM que le permita administrar credenciales temporales para las aplicaciones que se ejecutan en una instancia de EC2 y realizan solicitudes a la AWS CLI o a la API de AWS. Es preferible hacerlo de este modo a almacenar claves de acceso en la instancia EC2. Para asignar un rol de AWS a una instancia de EC2 y ponerla a disposición de todas las aplicaciones, cree un perfil de instancia asociado a la instancia. Un perfil de instancia contiene el rol y permite a los programas que se ejecutan en la instancia EC2 obtener credenciales temporales. Para obtener más información, consulte Uso de un rol de IAM para conceder permisos a aplicaciones que se ejecutan en instancias de Amazon EC2 en la Guía del usuario de IAM.

Para obtener información sobre el uso de los roles de IAM, consulte Cuándo crear un rol de IAM (en lugar de un usuario) en la Guía del Usuario de IAM.

## Administración de acceso mediante políticas

Para controlar el acceso en AWS, se crean políticas y se adjuntan a identidades o recursos de AWS. Una política es un objeto de AWS que, cuando se asocia a una identidad o un recurso, define sus permisos. AWS evalúa estas políticas cuando una entidad principal (sesión de rol, usuario o usuario raíz) realiza una solicitud. Los permisos en las políticas determinan si la solicitud se permite o se deniega. La mayoría de las políticas se almacenan en AWS como documentos JSON. Para obtener más información sobre la estructura y el contenido de los documentos de política JSON, consulte Información general de las políticas JSON en la Guía del Usuario de IAM.

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

De forma predeterminada, los usuarios y los roles no tienen permisos. Para conceder permiso a los usuarios para realizar acciones en los recursos que necesiten, un administrador de IAM puede crear políticas de IAM. A continuación, el administrador puede añadir las políticas de IAM a roles y los usuarios pueden asumirlos.

Las políticas de IAM definen permisos para una acción independientemente del método que se utilice para realizar la operación. Por ejemplo, suponga que dispone de una política que permite la acción `iam:GetRole`. Un usuario con dicha política puede obtener información del usuario de la consola, AWS CLI o la API de AWS.

### Políticas basadas en identidad

Las políticas basadas en identidad son documentos de políticas de permisos JSON que puede adjuntar a una identidad, como un usuario, un grupo de usuarios o un rol de IAM. Estas políticas controlan qué acciones pueden realizar los usuarios y los roles, en qué recursos y en qué condiciones. Para obtener más información sobre cómo crear una política en función de identidad, consulte Creación de políticas de IAM en la Guía del usuario de IAM.

Las políticas basadas en identidad pueden clasificarse además como políticas insertadas o políticas administradas. Las políticas insertadas se integran directamente en un único usuario, grupo o rol. Las políticas administradas son políticas independientes que puede asociar a varios usuarios, grupos y roles de su Cuenta de AWS. Las políticas administradas incluyen las políticas administradas de AWS y las políticas administradas por el cliente. Para obtener más información sobre cómo elegir una

política administrada o una política insertada, consulte Elegir entre políticas administradas y políticas insertadas en la Guía del usuario de IAM.

### Políticas basadas en recursos

Las políticas basadas en recursos son documentos de política JSON que se asocian a un recurso. Los ejemplos de políticas basadas en recursos son las políticas de confianza de roles de IAM y las políticas de bucket de Amazon S3. En los servicios que admiten políticas basadas en recursos, los administradores 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 puede realizar una entidad principal especificada en ese recurso y en qué condiciones. Debe especificar una entidad principal en una política en función de recursos. Las entidades principales 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 se puede utilizar políticas de IAM administradas por AWS en una política basada en recursos.

### Listas de control de acceso (ACL)

Las listas de control de acceso (ACL) controlan qué entidades principales (miembros de cuentas, usuarios o roles) tienen permisos para acceder a un recurso. Las ACL son similares a las políticas basadas en recursos, aunque no utilizan el formato de documento de política JSON.

Amazon S3, AWS WAF y Amazon VPC son ejemplos de servicios que admiten las ACL. Para obtener más información sobre las ACL, consulte Información general de Lista de control de acceso (ACL) en la Guía para Desarrolladores de Amazon Simple Storage Service.

### Otros tipos de políticas

AWS admite otros tipos de políticas adicionales menos frecuentes. Estos tipos de políticas pueden establecer el máximo de permisos que los tipos de políticas más frecuentes le conceden.

- Límites de permisos: un límite de permisos es una característica avanzada que le permite establecer los permisos máximos que una política en función de identidad puede conceder a una entidad de IAM (usuario o rol de IAM). Puede 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 Límites de permisos para las entidades de IAM en la Guía del Usuario de IAM.

- Políticas de control de servicio (SCP): las SCP son políticas de JSON que especifican los permisos máximos de una organización o una unidad organizativa en AWS Organizations. AWS Organizations es un servicio que le permite agrupar y administrar de manera centralizada varias cuentas de AWS que posea su empresa. Si habilita todas las características en una empresa, entonces podrá aplicar políticas de control de servicio (SCP) a una o todas sus cuentas. Una SCP limita los permisos para las entidades de las cuentas de miembros, incluido cada rootlong. Para más información sobre organizaciones y las SCP, consulte Funcionamiento de las SCP en la Guía del Usuario de AWS Organizations.
- Políticas de sesión: las políticas de sesión son políticas avanzadas que se pasan como parámetro cuando se crea una sesión temporal mediante programación para un rol o un usuario federado. Los permisos de la sesión resultantes son la intersección de las políticas basadas en identidad del rol y las políticas de la sesión. Los permisos también pueden proceder de una política en función de recursos. Una denegación explícita en cualquiera de estas políticas anulará el permiso. Para más información, consulte Políticas de sesión en la Guía del Usuario de IAM.

### Varios tipos de políticas

Cuando se aplican varios tipos de políticas a una solicitud, los permisos resultantes son más complicados de entender. Para obtener información sobre cómo AWS decide si permite o no una solicitud cuando hay varios tipos de políticas implicados, consulte Lógica de evaluación de políticas en la Guía del usuario de IAM.

## Cómo 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 mediante la AWS Management Console, la AWS CLI o la API de AWS. Un administrador de Detective debe contar con políticas de AWS Identity and Access Management (IAM) que concedan a los usuarios de y roles de IAM permiso para realizar operaciones específicas de la API en los recursos especificados que necesiten. El administrador debe asociar esas políticas a la entidad principal que necesite esos permisos.

Detective utiliza políticas de IAM basadas en identidades para conceder permisos relacionados con 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. El gráfico de comportamiento permite clasificar e investigar los resultados y los recursos asociados a dichas 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 conocer al detalle cómo Detective y otros Servicios de AWS funcionan con IAM, consulte Creación de políticas mediante el editor JSON en la Guía del usuario de IAM.

## Políticas basadas en identidades de Detective

Con las políticas basadas en identidad de IAM, puede especificar las acciones y recursos permitidos o denegados. Detective admite acciones, claves de condición y recursos específicos.

Para obtener información sobre todos los elementos que utiliza en una política JSON, consulte Referencia de los elementos de las políticas JSON de IAM en la Guía del usuario de IAM.

Acciones

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Action` de una política JSON describe las acciones que puede utilizar para permitir o denegar el acceso en una política. Las acciones de la política generalmente tienen el mismo nombre que la operación de API de AWS asociada. Hay algunas excepciones, como acciones de solo permiso que no tienen una operación de API coincidente. También hay algunas operaciones que requieren varias acciones en una política. Estas acciones adicionales se denominan acciones dependientes.

Incluya acciones en una política para conceder permisos y así llevar a cabo la operación asociada.

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, si desea conceder permiso para utilizar la operación de la API `CreateMembers` e invitar cuentas de miembros a un gráfico de comportamiento, debe incluir la acción `detective:CreateMembers` 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 utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede realizar acciones en qué recursos y en qué condiciones.

El elemento `Resource` de la política JSON especifica el objeto u objetos a los que se aplica la acción. Las instrucciones deben contener un elemento `Resource` o `NotResource`. Como práctica recomendada, especifique un recurso utilizando el Nombre de recurso de Amazon (ARN). Puede 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, utilice un carácter comodín (*) para indicar que la instrucción se aplica a todos los recursos.

```
"Resource": "*"
```

Para obtener más información acerca del formato de los ARN, consulte Nombres de recursos de Amazon (ARN) y espacios de nombres de servicios de AWS.

En el caso de Detective, el único tipo de recurso disponible es el gráfico de comportamiento. El recurso del gráfico de comportamiento de Detective tiene el siguiente ARN:

```
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`.

Si quisiera identificar este gráfico de comportamiento en una instrucción `Resource`, tendría que utilizar el siguiente ARN:

```
"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"
]
```

También puede invitar a la misma cuenta de AWS para que sea miembro de 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 política de IAM concede acceso a un gráfico de comportamiento, si el usuario no pertenece a la cuenta correcta, no podrá realizar la acción.

La política de IAM debe incluir el ARN del gráfico en todas las acciones que se lleven a cabo para un gráfico de comportamiento específico. El ARN del gráfico se puede agregar más adelante. Por ejemplo, cuando una cuenta habilita Detective por primera vez, la política de IAM inicial proporciona acceso a todas las acciones de Detective, ya que se utiliza el carácter comodín para el ARN del gráfico. 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 que se ha creado el gráfico de comportamiento, puede agregar el ARN del gráfico a la política y actualizarla.

Claves de condición

Los administradores pueden utilizar las políticas JSON de AWS para especificar quién tiene acceso a qué. Es decir, qué entidad principal puede 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. Puede crear expresiones condicionales que utilicen 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 lógica `AND`. Si especifica varios valores para una única clave de condición, AWS evalúa la condición con una operación `OR` lógica. Se deben cumplir todas las condiciones antes de que se concedan los permisos de la instrucción.

También puede utilizar variables de marcador de posición al especificar condiciones. Por ejemplo, puede conceder un permiso de usuario de IAM para acceder a un recurso solo si está etiquetado con su nombre de usuario de IAM. Para más información, consulte Elementos de la política de IAM: variables y etiquetas en la Guía del usuario de IAM.

AWS admite claves de condición globales y claves de condición específicas del servicio. Para ver todas las claves de condición globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del Usuario de IAM.

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 globales de AWS, consulte Claves de contexto de condición globales de AWS en la Guía del usuario de IAM.

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”.

## Roles de IAM en Detective

Un rol de IAM es una entidad de la cuenta de AWS que dispone de permisos específicos.

### Uso de credenciales temporales con Detective

Puede utilizar credenciales temporales para iniciar sesión con federación, asumir un rol de IAM o asumir un rol de acceso entre cuentas. Las credenciales de seguridad temporales se obtienen mediante una llamada a operaciones de la API de AWS STS, como AssumeRole o GetFederationToken.

Detective admite el uso de credenciales temporales.

### Roles vinculados al servicio

Los roles vinculados a servicios permiten a los servicios de AWS obtener acceso a los recursos de otros servicios para completar una acción en su nombre. Los roles vinculados a servicios aparecen en la cuenta de IAM y son propiedad del servicio. Un administrador de IAM puede ver, pero no editar, los permisos de los roles vinculados a servicios.

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 su cuenta de IAM y son propiedad de la cuenta. Esto significa que un administrador de IAM 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, los usuarios y los roles de IAM no tienen permiso para crear o modificar recursos de Detective. Tampoco pueden realizar tareas mediante la AWS Management Console, la AWS CLI, o la API de AWS.

Un administrador de IAM debe crear políticas de IAM que concedan permisos a los usuarios y a los roles para realizar operaciones de la API concretas en los recursos especificados que necesiten. En ese caso, el administrador debe asociar esas políticas a los usuarios o grupos de IAM que necesiten esos permisos.

Para obtener información acerca de cómo crear una política basada en identidad de IAM con estos documentos de políticas JSON de ejemplo, consulte Creación de políticas en la pestaña JSON en la Guía del usuario de IAM.

Temas

- Prácticas recomendadas relativas a políticas
- Uso de la consola de Detective
- 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 relativas a 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 costes adicionales para su Cuenta de AWS. Siga estas directrices y recomendaciones al crear o editar políticas basadas en identidades:

- Comience con las políticas administradas de AWS y continúe con los permisos de privilegio mínimo: a fin de comenzar a conceder permisos a los usuarios y las cargas de trabajo, utilice las políticas administradas de AWS, que conceden permisos para muchos casos de uso comunes. Están disponibles en su Cuenta de AWS. Se recomienda definir políticas administradas por el cliente de AWS específicas para los casos de uso a fin de reducir aún más los permisos. Con el fin de obtener más información, consulte las políticas administradas por AWS o las políticas administradas por AWS para funciones de trabajo en la Guía del usuario de IAM.
- Aplique permisos de privilegio mínimo: cuando establezca permisos con políticas de IAM, conceda solo los permisos necesarios para realizar una tarea. Para ello, debe definir las acciones que se pueden llevar a cabo en determinados recursos en condiciones específicas, también conocidos como permisos de privilegios mínimos. Con el fin de obtener más información sobre el uso de IAM para aplicar permisos, consulte Políticas y permisos en IAM en la Guía de usuario de IAM.
- Utilice condiciones en las políticas de IAM para restringir aún más el acceso: puede agregar 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 utilizando SSL. También puede usar condiciones para conceder acceso a acciones de servicios si se emplean a través de un Servicio de AWS determinado, como por ejemplo AWS CloudFormation. Para obtener más información, consulte Elementos de la política de JSON de IAM: Condición en la Guía del usuario de IAM.
- Utilice el analizador de acceso de IAM para validar las políticas de IAM con el fin de garantizar la seguridad y funcionalidad de los permisos: el analizador de acceso de IAM valida políticas nuevas y existentes para que respeten el lenguaje (JSON) de las políticas de IAM y las prácticas recomendadas de IAM. El analizador de acceso de IAM proporciona más de 100 verificaciones de políticas y recomendaciones procesables para ayudar a crear políticas seguras y funcionales. Para más información, consulte la Política de validación del analizador de acceso de IAM en la Guía de usuario de IAM.
- Solicite la autenticación multifactor (MFA): si se encuentra en una situación en la que necesita usuarios raíz o de IAM en su Cuenta de AWS, active la MFA para mayor seguridad. Para solicitar la MFA cuando se invocan las operaciones de la API, agregue las condiciones de la MFA a sus

políticas. Para obtener más información, consulte Configuración de acceso a una API protegida por MFA en la Guía del usuario de IAM.

Para obtener más información sobre las prácticas recomendadas de IAM, consulte las Prácticas recomendadas de seguridad en IAM en la Guía del usuario de IAM.

## Uso de la consola de Detective

Para utilizar la consola de Amazon Detective, el usuario o el rol deben poder acceder a las acciones pertinentes, que deben coincidir con las acciones correspondientes de la API.

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.

## Permitir a los usuarios que vean sus propios permisos

En este ejemplo, se muestra cómo podría crear una política que permita a los usuarios de IAM ver las políticas administradas e insertadas que se asocian a la identidad de sus usuarios. Esta política incluye permisos para realizar esta acción en la consola o mediante programación con la AWS CLI o la API de AWS.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

## 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"}
        }
    } ]
}
```

## Solución de problemas de identidad y acceso de Amazon Detective

Utilice la siguiente información para diagnosticar y solucionar los problemas comunes que puedan surgir cuando trabaje con Detective e IAM. Si tiene problemas de acceso denegado o dificultados similares al trabajar con AWS Identity and Access Management (IAM), consulte los temas de solución de problemas de IAM de la Guía del usuario de IAM.

### No tengo autorización para realizar una acción en Detective

Si la AWS Management Console le indica que no está autorizado para llevar a cabo una acción, debe ponerse en contacto con su administrador para recibir ayuda. Su administrador es la persona que le facilitó su nombre de usuario y contraseña.

El siguiente ejemplo de error ocurre cuando el usuario de IAM `mateojackson` intenta utilizar la consola para aceptar una invitación y ser cuenta de miembro de un gráfico de rendimiento, pero no cuenta con permisos `detective:AcceptInvitation`.

```
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 tengo autorización para realizar la operación iam:PassRole

Si recibe un error que indica que no tiene autorización para realizar la acción `iam:PassRole`, se deben actualizar las políticas a fin de permitirle pasar un rol a Detective.

Algunos Servicios de AWS le permiten transferir un rol existente a dicho servicio en lugar de crear un nuevo rol de servicio o uno vinculado a servicios. Para ello, debe tener permisos para transferir el rol al servicio.

En el siguiente ejemplo, el error se produce cuando un usuario de IAM denominado `marymajor` intenta utilizar la consola para realizar una acción en Detective. Sin embargo, la acción requiere que el servicio cuente con permisos que concede 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 administrador de AWS. El administrador es la persona que le proporcionó las credenciales de inicio de sesión.

## Quiero permitir que personas ajenas a mi cuenta de AWS puedan acceder a mis recursos de Detective

Puede crear un rol que los usuarios de otras cuentas o las personas externas a la organización puedan utilizar para acceder a sus recursos. Puede especificar una persona de confianza para que

asuma el rol. En el caso de los servicios que admitan las políticas basadas en recursos o las listas de control de acceso (ACL), puede utilizar dichas políticas para conceder a las personas acceso a sus recursos.

Para 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 acerca de cómo proporcionar acceso a los recursos de las Cuentas de AWS de su propiedad, consulte Cómo proporcionar acceso a un usuario de IAM a otra Cuenta de AWS de la que es propietario en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso a los recursos a Cuentas de AWS de terceros, consulte Proporcionar acceso a Cuentas de AWS que son propiedad de terceros en la Guía del usuario de IAM.
- Para obtener información sobre cómo proporcionar acceso mediante federación de identidades, consulte Proporcionar acceso a usuarios autenticados externamente (federación de identidades) en la Guía del usuario de IAM.
- Para obtener información sobre la diferencia entre los roles y las políticas basadas en recursos para el acceso entre cuentas, consulte Cómo los roles de IAM difieren de las políticas basadas en recursos en la Guía del Usuario de IAM.

## Usar roles vinculados a servicios para Detective

Amazon Detective usa roles vinculados a servicios de AWS Identity and Access Management (IAM). Un rol vinculado a un servicio es un tipo único de rol de IAM que está vinculado directamente a Detective. Los roles vinculados a servicios están predefinidos por Detective e incluyen todos los permisos que el servicio requiere para llamar a otros servicios de AWS 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 utiliza el rol vinculado a servicio denominado AWSServiceRoleForDetective: permite a Detective acceder a información de AWS Organizations en su nombre.

El rol vinculado al servicio AWSServiceRoleForDetective confía en los siguientes servicios para que asuman el rol:

- `detective.amazonaws.com`

El rol vinculado a servicio AWSServiceRoleForDetective utiliza la política administrada `AmazonDetectiveServiceLinkedRolePolicy`.

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. Al designar la cuenta de administrador de Detective de una organización en la AWS Management Console, en la AWS CLI o en la API de AWS, Detective crea el rol vinculado al servicio en su nombre.

Si elimina este rol vinculado al servicio 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 vinculado al servicio AWSServiceRoleForDetective. 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, puede editar la descripción del rol mediante 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 recursos de Detective utilizados por el rol 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, la AWS CLI o la API de AWS para eliminar el rol vinculado al servicio AWSServiceRoleForDetective. 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.

# Políticas administradas de AWS para Amazon Detective

Una política administrada de AWS es una política independiente que AWS crea y administra. Las políticas administradas de AWS se diseñan para ofrecer permisos para muchos casos de uso comunes, por lo que puede empezar a asignar permisos a los usuarios, grupos y roles.

Considere que es posible que las políticas administradas por AWS no concedan permisos de privilegio mínimo para los casos de uso concretos, ya que están disponibles para que las utilicen

todos los clientes de AWS. Se recomienda definir políticas administradas por el cliente para los casos de uso a fin de reducir aún más los permisos.

No puede cambiar los permisos definidos en las políticas administradas de AWS. Si AWS actualiza los permisos definidos en una política administrada de AWS, la actualización afecta a todas las identidades de entidades principales (usuarios, grupos y roles) a las que está adjunta la política. Lo más probable es que AWS actualice una política administrada de AWS cuando se lance un nuevo Servicio de AWS o las operaciones de la API nuevas estén disponibles para los servicios existentes.

Para obtener más información, consulte Políticas administradas por AWS en la Guía del usuario de IAM.

## Política administrada de AWS: 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, añadir etiquetas a su gráfico de comportamiento y usar Detective con fines de investigación. También pueden archivar resultados de GuardDuty. La política proporciona los permisos que la consola de Detective necesita para mostrar los nombres de las cuentas que figuran en 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 las entidades principales obtener y archivar resultados de GuardDuty 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": "*"
         }
    ]
```

```
}
```

## Política administrada de AWS: 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 las entidades principales obtener y archivar resultados de GuardDuty desde Detective.
- `securityhub`: permite a las entidades principales obtener resultados de Security Hub desde Detective.
- `organizations`: permite a las entidades principales 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": "*"
    }
  ]
}
```

## Política administrada de AWS: 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 las entidades principales 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 servicio de AWS, permite registrar y

anular el registro de la cuenta de miembro especificada como administrador delegado, y permite a las entidades principales recuperar cuentas de administrador delegado en otros servicios de seguridad, como Amazon Detective, Amazon GuardDuty, Amazon 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 Detective a las políticas administradas de AWS

Consulte detalles sobre las actualizaciones de las políticas administradas de AWS para Detective desde que el servicio comenzó a hacer el seguimiento de 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.

| 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.<br><br>Estas acciones permiten iniciar, recuperar y actualizar las investigaciones de Detective y obtener un | 26 de noviembre de 2023 |

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| | resumen de grupo de resultados desde Detective. | |
| AmazonDetectiveFullAccess y AmazonDetectiveInvestigatorAccess: actualizaciones de las políticas existentes | Detective añadió las acciones `GetFindings` de Security Hub a las políticas `AmazonDetectiveFullAccess` y `AmazonDetectiveInvestigatorAccess`.<br><br>Estas acciones permiten obtener los resultados de Security Hub desde Detective. | 16 de mayo de 2023 |
| AmazonDetectiveOrganizationsAccess: política nueva | Detective añadió la política `AmazonDetectiveOrganizationsAccess`.<br><br>Esta política otorga permiso para habilitar y administrar Detective dentro de una organización. | 2 de marzo de 2023 |
| AmazonDetectiveMemberAccess: política nueva | Detective añadió la política `AmazonDetectiveMemberAccess`.<br><br>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 | Detective añadió las acciones `GetFindings` de GuardDuty a la política `AmazonDetectiveFullAccess`.<br><br>Estas acciones permiten obtener los resultados de GuardDuty desde Detective. | 17 de enero de 2023 |
| AmazonDetectiveInvestigatorAccess: política nueva | Detective añadió la política `AmazonDetectiveInvestigatorAccess`.<br><br>Esta política permite a la entidad principal realizar investigaciones en Detective. | 17 de enero de 2023 |
| AmazonDetectiveServiceLinkedRole: política nueva | Detective añadió una nueva política para su rol vinculado al servicio.<br><br>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 hacer el seguimiento de los cambios de sus políticas administradas de AWS. | 10 de mayo de 2021 |

# Registro y monitorización en Amazon Detective

Amazon Detective está integrado en AWS CloudTrail. CloudTrail captura todas las llamadas a la API de Detective como eventos.

Para obtener más información sobre el uso del registro de CloudTrail para Detective, consulte the section called “Registro de llamadas a la API de Detective con CloudTrail”.

# Validación de conformidad para Amazon Detective

Amazon Detective forma parte del ámbito del programa de garantía de AWS. Para obtener más información, consulte Marco de seguridad común (CSF) de Health Information Trust Alliance (HITRUST).

Para obtener una lista de servicios de AWS en el ámbito de programas de conformidad específicos, consulte Servicios de AWS en el ámbito del programa de conformidad. Para obtener información general, consulte Programas de conformidad de AWS.

Puede descargar los 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 con la conformidad:

- Security and Compliance Quick Start Guides (Guías de inicio rápido de seguridad y conformidad) (Guías de inicio rápido de seguridad y conformidad): Estas guías de implementación analizan consideraciones sobre arquitectura y proporcionan los pasos para implementar los entornos de referencia centrados en la seguridad y la conformidad en AWS.
- Evaluación de recursos con reglas en la Guía para desarrolladores de AWS Config: el servicio AWS Config evalúa en qué medida las configuraciones de sus recursos cumplen las prácticas internas, las directrices del sector y las normativas.
- AWS Security Hub: este servicio de AWS proporciona una vista integral de su estado de seguridad en AWS que lo ayuda a verificar la conformidad con los estándares y las prácticas recomendadas del sector de seguridad.

# Resiliencia de Amazon Detective

La infraestructura global de AWS se compone de regiones y zonas de disponibilidad de AWS. AWS Las regiones proporcionan varias zonas de disponibilidad físicamente independientes y aisladas que se encuentran conectadas mediante redes con un alto nivel de rendimiento y redundancia, además de baja latencia. Con las zonas de disponibilidad, puede diseñar y utilizar aplicaciones y bases de datos que 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 centros de datos únicos o múltiples.

Para obtener más información sobre las regiones y zonas de disponibilidad de AWS, consulte Infraestructura global de AWS.

Además de la infraestructura global de AWS, Detective utiliza la resiliencia integrada de Amazon DynamoDB y Amazon Simple Storage Service (Amazon S3).

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 administrado, Amazon Detective se encuentra protegido por la seguridad de red global de AWS. Para obtener información sobre los servicios de seguridad de AWS y sobre cómo AWS protege la infraestructura, consulte Seguridad en la nube de AWS. Para diseñar su entorno de AWS conforme a las prácticas recomendadas de seguridad de la infraestructura, consulte Protección de la infraestructura en Pilar de seguridad del Marco de AWS Well-Architected.

Utilice llamadas a la API publicadas en AWS para acceder a Detective a través de la red. Los clientes deben admitir lo siguiente:

- Seguridad de la capa de transporte (TLS). Nosotros exigimos TLS 1.2 y recomendamos TLS 1.3.
- Conjuntos de cifrado con confidencialidad directa total (PFS) tales como DHE (Ephemeral Diffie-Hellman) o 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 estar firmadas mediante un ID de clave de acceso y una clave de acceso secreta que esté asociada a una entidad principal de IAM. También puede utilizar AWS Security Token Service (AWS STS) para generar credenciales de seguridad temporales para firmar solicitudes.

## Prácticas recomendadas de seguridad para Amazon Detective

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 suponen 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.

## Prácticas recomendadas para cuentas de administrador

Invite al gráfico de comportamiento solo cuentas de miembros que pueda supervisar.

Limite el acceso al gráfico de comportamiento. 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 que sea el identificador de la cuenta de AWS de la cuenta de administrador que ha enviado 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.

# 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)

Puede deshabilitar Amazon Detective desde la AWS Management Console.

Deshabilitación de 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, vaya a Deshabilitar Detective y elija Deshabilitar detective.
4. Cuando se le pida confirmación, escriba **`disable`**.
5. Elija Deshabilitar Detective.

## Deshabilitación de Detective (API de Detective y 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`.

Deshabilitación de Detective (API de Detective y 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
```

## Deshabilitación de Detective en varias regiones (script de Python de GitHub)

Detective proporciona un script de código abierto disponible en GitHub que le permite deshabilitar Detective de una cuenta de administrador en una lista especificada de regiones.

Para obtener información sobre cómo configurar y utilizar scripts de GitHub, consulte Uso de los scripts de Python de Amazon Detective.

# Uso de los scripts de Python de Amazon Detective

Amazon Detective proporciona un conjunto de scripts de Python de código abierto en el repositorio de GitHub 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 que haya un rol de AWS preexistente en la cuenta del administrador y en todas las cuentas de miembros que quiera agregar o eliminar.

> **Note**
>
> El nombre del rol debe ser el mismo en todas las cuentas.

Según las prácticas recomendadas para políticas de IAM, lo mejor es utilizar los roles menos limitados. 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.
- Agregue los permisos necesarios que se indican más arriba (recomendado) o seleccione la política administrada AmazonDetectiveFullAccess.
- Agregue el bloque de relaciones de confianza del rol, tal como se indica más arriba.

Para automatizar este proceso, puede la plantilla `EnableDetective.yaml` de AWS CloudFormation. 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 instancia de EC2 o desde una máquina local.

## Lanzamiento y configuración de una instancia de EC2

Tiene la opción de ejecutar scripts desde una instancia de EC2.

Lanzamiento y configuración de una instancia de EC2

1. Lance una instancia de EC2 en la cuenta de administrador. Para obtener información sobre cómo lanzar una instancia de EC2, consulte Introducción a las instancias Linux de Amazon EC2 en la Guía del usuario de Amazon EC2 para instancias Linux.
2. Adjunte a la instancia un rol de IAM que tenga permisos que permitan a la instancia llamar a `AssumeRole` en la cuenta de administrador.

   Si ha utilizado la plantilla `EnableDetective.yaml` de AWS CloudFormation, se crea un rol de instancia con un perfil denominado `EnableDetective`.

   Si, por contra, no ha utilizado una plantilla, consulte la entrada del blog Sustitución y adición de un rol de IAM a una instancia de EC2 existente con la consola de EC2 (en inglés) para obtener información sobre cómo crear un rol de instancia.
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. Clone el repositorio en la instancia de EC2.

   ```
   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)
   - Scripts de GitHub

| Plataforma | Instrucciones de configuración |
| --- | --- |
| Windows | 1. Instale Python 3 (https://www.python.org/downloads/windows/).<br>2. Abra un símbolo del sistema.<br>3. Ejecute `pip install boto3` para instalar Boto.<br>4. Descargue el código fuente del script de GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts). |
| Mac | 1. Instale Python 3 (https://www.python.org/downloads/mac-osx/).<br>2. Abra un símbolo del sistema.<br>3. Ejecute `pip install boto3` para instalar Boto.<br>4. Descargue el código fuente del script de GitHub (https://github.com/aws-samples/amazon-detective-multiaccount-scripts). |
| Linux | 1. Para instalar Python 3, ejecute uno de los siguientes comandos:<br>• `sudo apt-get -y install install python3-pip python3 git`<br>• `sudo yum install git python`<br>2. Ejecute `sudo pip install boto3` para instalar Boto.<br>3. Clone el código fuente del script de 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 una cuenta de miembro contiene el ID de la cuenta de AWS 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 script `enableDetective.py` desde una instancia de EC2 o desde una máquina local.

Para ejecutar **enableDetective.py**

1. Copie el archivo `.csv` en el directorio `amazon-detective-multiaccount-scripts` de la instancia de EC2 o la 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 la cuenta de administrador de AWS.

*roleName*

El nombre del rol de AWS que se asume en la cuenta de administrador y cada cuenta de 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 script `disableDetective.py` desde una instancia de EC2 o desde una 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 la cuenta de administrador de AWS.

*roleName*

El nombre del rol de AWS que se asume en la cuenta de administrador y cada cuenta de 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.

# Historial de documentos de la Guía de administración 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: 15 de abril de 2024

| Cambio | Descripción | Fecha |
| --- | --- | --- |
| 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 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 |
| Cambios en la forma en que Detective lee el tráfico de flujo de las VPC compartidas | 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 | 20 de diciembre de 2023 |

| | | |
|---|---|---|
| | 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. | |
| 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 |
| Puntos de conexión y cuotas de Amazon Detective | Detective ya está disponible en la región de Israel (Tel Aviv). | 25 de agosto de 2023 |
| Se agregaron hallazgos de AWS seguridad como un nuevo paquete de fuentes de datos opcional. | Detective ahora proporciona 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 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 |

| | | |
|---|---|---|
| Información sobre políticas administradas agregada al capítulo de seguridad | El Detective ahora apoya las acciones de GuardDuty obtención de hallazgos a través de la AmazonDet ectiveFullAccess política. El capítulo de seguridad ahora proporciona detalles sobre las siguientes nuevas políticas gestionadas para Detective : AmazonDetectiveMem berAccess y AmazonDet ectiveInvestigatorAccess. | 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 |
| 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 |

| | | |
|---|---|---|
| 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 |
| 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 (Habilitado). Tenga en cuenta que las cuentas de miembros cuyo estado sea Aceptado (No habilitado) en este momento no se habilitarán automáticamente. | 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, `AmazonDetectiveFullAccess`. | 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 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 desactiva n 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 |
| 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 |
| Opción agregada a la API para no enviar correos electrónicos 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 electrónicos de invitación a cuentas de miembros. | 25 de febrero de 2021 |
| 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 |

| | | |
|---|---|---|
| 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 |

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.

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.